Acronis

acronis.com

Console cloud Cyber Protect

26.01

Guide de l'utilisateur

RÉVISION : MARDI 3 FÉVRIER 2026

Table des matières

Prise en main de Cyber Protection **21**
Activation du compte 21
Exigences relatives au mot de passe 21
Authentification à deux facteurs 21
Paramètres de confidentialité 24
Accès au service Cyber Protection 24
Navigateurs Web pris en charge 25
Ma boîte de réception 26
Vue d'ensemble 26
Vérification de vos notifications 26
Recherche dans Ma boîte de réception 26
Fonctionnalités de protection prises en charge par système d'exploitation 27
Systèmes d'exploitation et versions pris en charge 27
Installation et déploiement d'agents Cyber Protection **37**
Avant de commencer 37
Préparation 37
Sauvegarde avec et sans agent 40
De quel agent ai-je besoin ? 41
Configuration système requise pour les agents 45
Téléchargement d'agents de protection 47
Packages Linux requis pour l'installation d'agents dans Linux 48
Configuration des paramètres de serveur proxy 52
Installation dynamique des composants 56
Attribution des autorisations système requises à Agent Connect 57
Mode compatible FIPS 59
Installation de l'agent pour Windows en mode compatible FIPS 60
Installation de l'agent pour Linux en mode compatible FIPS 63
Activation du mode compatible FIPS pour une appliance virtuelle 64
Installation des agents de protection à l'aide de l'interface utilisateur graphique 64
Installation des agents de protection sous Windows 64
Installation des agents de protection sous Linux 69
Installation des agents de protection sous macOS 71
Désinstallation d'agents 72
Installation et désinstallation d'agents de protection à l'aide de l'interface de ligne de commande 74

© Acronis International GmbH, 2003-2026

Installation et désinstallation d'agents de protection sous Windows ... 74
Exemples ... 75
Exemple ... 76
Exemples ... 77
Exemples ... 85
Exemple ... 86
Exemples ... 87
Installation et désinstallation d'agents de protection sous Linux ... 92
Installation et désinstallation d'agents de protection dans macOS ... 99
Enregistrement des ressources ... 110
Enregistrement des ressources à l'aide de l'interface utilisateur graphique ... 110
Enregistrement et désenregistrement de ressources à l'aide de l'interface de ligne de commande ... 115
Modification de l'inscription d'une ressource ... 120
Déplacement des ressources vers un autre tenant ... 121
Mise à jour des agents de protection ... 121
Espace disque libre nécessaire pour la mise à jour ... 122
Configuration de la méthode par défaut pour mettre à jour les agents ... 122
Mise à jour manuelle des agents de protection ... 129
Mise à jour automatique des agents de protection ... 131
Mise à jour des agents de protection sur les ressources chiffrées par BitLocker ... 134
Déploiement d'agents de protection via la stratégie de groupe ... 135
Prérequis ... 135
Création du fichier de transformation et extraction des packages d'installation ... 136
Configuration de l'objet de stratégie de groupe ... 137
Déploiement d'appliances virtuelles ... 138
Déploiement de l'agent pour VMware (appliance virtuelle) ... 138
Déploiement de l'agent pour Scale Computing HC3 (appliance virtuelle) ... 141
Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) ... 145
Exemples ... 149
Exemples ... 153
Déploiement de l'agent pour oVirt (appliance virtuelle) ... 157
Déploiement de l'agent pour Azure ... 162
Déploiement de l'agent pour Nutanix AHV ... 167
Déploiement de l'agent pour Synology ... 171
Connexions SSH à une appliance virtuelle ... 180
Détection des terminaux ... 182

© Acronis International GmbH, 2003-2026

Découverte de plusieurs terminaux ... 182
Découverte de terminaux à l'aide de Device Sense ™ ... 189
Affichage des informations sur les terminaux découverts ... 195
Installation à distance des agents ... 196
Exclusion des terminaux de la découverte ... 205
Connexion aux terminaux découverts à distance ... 205
Dépannage de la découverte de terminaux ... 206
Empêcher la désinstallation ou la modification non autorisée d'agents ... 207
Modifier le quota du service pour les ressources ... 209
Paramètres de protection ... 210
Mises à jour automatiques pour les composants ... 211
Collecte automatique de données de performances ... 212
Mise à jour des définitions de Cyber Protection de façon planifiée ... 213
Mise à jour des définitions de Cyber Protection à la demande ... 213
Mémoire en cache ... 213
Services Cyber Protection installés dans votre environnement ... 214
Services installés sous Windows ... 214
Services installés sous macOS ... 214
Collecte des informations système ... 215
Gestion des licences pour les serveurs de gestion sur site ... 215
Utilisation de plans ... 216
Présentation des plans ... 216
Plans intégrés ... 219
Plans par défaut ... 231
Plans favoris ... 234
Plans préselectionnés ... 238
Plans à différents niveaux d'administration ... 240
État du plan ... 242
Plans et modules de protection ... 243
Création d'un plan de protection ... 244
Actions avec plans de protection ... 245
Plans de protection individuels pour l'hébergement des intégrations du panneau de configuration ... 251
Problèmes de compatibilité avec les plans ... 251
Résolution des problèmes de compatibilité ... 253
Plans de protection des données hors hôte ... 255
Réplication de sauvegarde ... 255

© Acronis International GmbH, 2003-2026

Validation ... 259
Nettoyage ... 266
Conversion en une machine virtuelle ... 267
Plan d'analyse des sauvegardes ... 272
Plans de sauvegarde pour les applications dans le Cloud ... 273
Protection des applications de collaboration et de communication ... 273
Plans de transfert SIEM ... 274
Installation de la fonctionnalité SIEM ... 275
Listes de plans de transfert SIEM ... 279
Créer un plan de transfert SIEM pour plusieurs clients ... 280
Création d'un plan SIEM pour un client individuel ... 282
Renommer un plan de transfert SIEM ... 285
Modification d'un plan de transfert SIEM ... 285
Suppression du plan SIEM ... 285
Méthodes de transfert SIEM ... 286
Format et exemples de données SIEM ... 286
Présentation de votre niveau de protection actuel ... 298
Surveillance ... 298
Tableau de bord Vue d'ensemble ... 298
Le tableau de bord Activités ... 299
Le tableau de bord des alertes ... 300
Cyber Protection ... 339
État de protection ... 340
Widgets de Endpoint Detection and Response (EDR) ... 341
Score #CyberFit par machine ... 345
Surveillance de l'intégrité du disque ... 346
Widgets de protection de l'intelligence artificielle générative ... 350
Widget de carte de protection des données ... 352
Widget Terminaux découverts ... 353
Widgets d'évaluation des vulnérabilités ... 354
Widgets d'installation des correctifs ... 355
Détails de l'analyse de la sauvegarde ... 357
Affectés récemment ... 357
Applications dans le Cloud ... 358
Widgets de logiciels ... 359
Widgets d'inventaire du matériel ... 362
Widget Sessions distantes ... 363

© Acronis International GmbH, 2003-2026

Protection intelligente ... 364
Onglet Activités ... 371
Cyber Protect Monitor ... 372
Configuration des paramètres de serveur proxy dans Cyber Protect Monitor ... 375
Chats dans Monitor ... 375
Rapports ... 378
Actions relatives aux rapports ... 379
Données rapportées en fonction du type de widget ... 382
Gestion des ressources dans la console Cyber Protect ... 385
La console Cyber Protect ... 385
Nouveautés de la console Cyber Protect ... 386
Niveaux d'administration dans la console Cyber Protect ... 387
Prérequis ... 391
Utilisation de caractères génériques pour définir des exclusions ... 395
Utilisation de variables pour définir des exclusions ... 396
Ressources ... 396
Ajout de ressources à la console Cyber Protect ... 398
Suppression de ressources de la console Cyber Protect ... 403
Types de ressources ... 407
Groupes du terminal ... 419
Groupes par défaut et groupes personnalisés ... 419
Groupes statiques et dynamiques ... 420
Groupes de cloud à cloud et groupes autres que de cloud à cloud ... 421
Création d'un groupe statique ... 422
Ajout de ressources à un groupe statique ... 423
Création d'un groupe dynamique ... 424
Modification d'un groupe dynamique ... 445
Suppression d'un groupe ... 446
Application d'un plan à un groupe ... 446
Révocation d'un plan à partir d'un groupe ... 447
Utilisation du module de contrôle des terminaux ... 448
Utilisation du contrôle des terminaux ... 451
Paramètres d'accès ... 459
Liste d'autorisation des types de terminaux ... 464
Liste d'autorisation des périphériques USB ... 466
Exclusion de processus du contrôle d'accès ... 471
Alertes de contrôle des terminaux ... 473

© Acronis International GmbH, 2003-2026

Effacement des données d'une ressource gérée ... 476
Affichage des ressources gérées par les intégrations RMM ... 478
Ressources CyberApp ... 479
Ressources agrégées ... 479
Utilisation de ressources CyberApp ... 479
Utilisation de ressources agrégées ... 480
Association de ressources à des utilisateurs spécifiques ... 481
Consultation du dernier utilisateur connecté ... 482
Score #CyberFit pour les machines ... 483
Fonctionnement ... 483
Lancer une analyse du Score #CyberFit ... 487
Création de cyber-scripts ... 489
Prérequis ... 489
Limites ... 490
Plates-formes prises en charge ... 490
Rôles d'utilisateur et droits de création de cyber-scripts ... 491
Scripts ... 493
Référentiel de scripts ... 502
Plans de création de scripts ... 503
Exécution rapide du script ... 510
Gestion de la sauvegarde et de la restauration des ressources et fichiers ... 513
Systèmes d'exploitation et environnements pris en charge pour la sauvegarde et la restauration ... 513
Agent pour Windows ... 513
Agent pour Windows (hérité) ... 514
Agent pour SQL, agent pour Active Directory, agent pour Exchange (pour la sauvegarde de bases de données et la sauvegarde reconnaissant les applications) ... 516
Agent pour empêcher les pertes de données ... 516
Agent pour File Sync & Share ... 517
Agent pour Exchange (pour la sauvegarde de boîte aux lettres) ... 517
Agent pour Microsoft 365 ... 518
Agent pour Oracle ... 518
Agent pour MySQL/MariaDB ... 518
Agent pour Linux ... 518
Agent pour Mac ... 520
Agent pour VMware (appliance virtuelle) ... 521
Agent pour VMware (Windows) ... 521

© Acronis International GmbH, 2003-2026

Agent pour Hyper-V ... 522
Agent pour Virtuozzo ... 522
Agent pour Virtuozzo Hybrid Infrastructure ... 523
Agent pour Scale Computing HC3 ... 523
Agent pour oVirt ... 523
Agent pour Synology ... 523
Agent pour Azure ... 523
Agent pour Nutanix ... 523
Cyber Protect Monitor ... 524
Versions de Microsoft SQL Server prises en charge ... 524
Versions Microsoft Exchange Server compatibles ... 524
Versions de Microsoft SharePoint prises en charge ... 525
Versions Oracle Database prises en charge ... 525
Versions SAP HANA prises en charge ... 525
Versions de MySQL prises en charge ... 526
Versions de MariaDB prises en charge ... 526
Plates-formes de virtualisation prises en charge ... 526
Compatibilité avec les stockages Data Domain Dell EMC ... 538
Systèmes de fichiers pris en charge ... 539
Opérations prises en charge pour les volumes logiques ... 543
Compatibilité avec le logiciel de chiffrage ... 545
Compatibilité avec les disques durs Advanced Format (secteurs 4 K) ... 546
Sauvegarde ... 547
Aide-mémoire pour la sauvegarde ... 549
Durée de conservation des sauvegardes ... 552
Sélection des données à sauvegarder ... 552
Sélection d'un ordinateur complet ... 552
Sélection de disques ou de volumes ... 553
Sélection de fichiers ou de dossiers ... 556
Sélection de l'état du système ... 559
Sélection de la configuration ESXi ... 560
Sélection d'une destination ... 560
Option de stockage avancée ... 562
À propos de Secure Zone ... 563
Protection continue des données (CDP) ... 566
Fonctionnement ... 566
Sources de données prises en charge ... 568

© Acronis International GmbH, 2003-2026

Destinations prises en charge ... 569
Configuration d'une sauvegarde CDP ... 569
Planification de sauvegarde ... 570
Modèles de sauvegarde ... 571
Types de sauvegarde ... 573
Exécution d'une sauvegarde à partir d'une planification ... 574
Exécution manuelle d'une sauvegarde ... 588
Règles de rétention ... 589
Conseils importants ... 589
Règles de rétention en fonction du modèle de sauvegarde ... 590
Configuration des règles de rétention ... 593
Réplication ... 594
Exemples d'utilisation ... 594
Emplacements pris en charge ... 595
Chiffrement ... 596
Configuration du chiffrement dans le plan de protection ... 597
Configuration du chiffrement en tant que propriété de l'ordinateur ... 598
Notarisation ... 601
Comment utiliser la notarisation ... 601
Fonctionnement ... 601
Options de sauvegarde par défaut ... 602
Options de sauvegarde ... 602
Disponibilité des options de sauvegarde ... 602
Alertes ... 606
Points de restauration Azure ... 606
Consolidation de sauvegarde ... 608
Nom de fichier de sauvegarde ... 609
Format de sauvegarde ... 614
Validation de la sauvegarde ... 615
Suivi des blocs modifiés (CBT) ... 616
Mode de sauvegarde de cluster ... 616
Niveau de compression ... 618
Gestion erreurs ... 618
Sauvegarde incrémentielle/différentielle rapide ... 620
Filtres de fichiers (Inclusions/Exclusions) ... 620
Instantané de sauvegarde de niveau fichier ... 627
Données d'investigation ... 628

© Acronis International GmbH, 2003-2026

Troncation de journal ... 638
Prise d'instantanés LVM ... 638
Points de montage ... 639
Snapshot Multi-volume ... 640
Restauration en un seul clic ... 640
Performance et créneau de sauvegarde ... 645
Envoi de données physiques ... 649
Commandes Pré/Post ... 651
Commandes de capture de données Pré/Post ... 653
Planification ... 657
Sauvegarde secteur par secteur ... 657
Fractionnement ... 658
Traitement de l'échec de tâche ... 658
Conditions de démarrage de tâche ... 659
Service de cliché instantané des volumes ... 660
Service de cliché instantané des volumes (VSS) pour les machines virtuelles ... 662
Sauvegarde hebdomadaire ... 664
Journal des événements Windows ... 664
Restauration ... 664
Restauration de l'aide-mémoire ... 664
Restauration interplate-forme ... 667
Restauration de machines physiques ... 674
Restauration de machines virtuelles ... 689
Restauration de disques via un support de démarrage ... 704
Restauration des fichiers ... 707
Restauration de l'état du système ... 714
Restauration d'une configuration ESXi ... 715
Restauration avec redémarrage ... 716
En utilisant Universal Restore ... 718
Options de restauration ... 721
Restauration sûre ... 730
Opérations avec des sauvegardes ... 731
Stockage de sauvegarde ... 731
Montage de volumes à partir d'une sauvegarde ... 734
Validation des sauvegardes ... 736
Exportation de sauvegardes ... 736
Suppression de sauvegardes ... 737

© Acronis International GmbH, 2003-2026

Compréhension de la détection des goulots d'étranglement ... 740
Sauvegarde de ressources dans des clouds publics ... 745
Définition d'un emplacement de sauvegarde dans Microsoft Azure ... 745
Définir un emplacement de sauvegarde dans Amazon S3 ... 748
Définir un emplacement de sauvegarde dans IONOS Cloud, Impossible Cloud ou un stockage compatible S3 ... 752
Affichage et mise à jour des emplacements de sauvegarde dans le cloud public ... 756
Gestion de l'accès du compte dans le cloud public ... 757
Archivage d'e-mails ... 771
Limites ... 772
Configuration de l'archivage des e-mails ... 772
Plans d'archivage ... 775
Importation des e-mails à partir de fichiers PST ... 778
Requêtes de recherche ... 781
Règles de rétention ... 790
Règles de conservation légale ... 794
Restauration de données à partir d'une archive d'e-mails ... 798
Stockage immuable pour l'archivage des e-mails ... 802
Protection d'applications Microsoft ... 803
Protection des serveurs Microsoft SQL Server et Microsoft Exchange Server ... 803
Protection de Microsoft SharePoint ... 804
Protection d'un contrôleur de domaine ... 804
Restauration d'applications ... 804
Exigences supplémentaires pour les sauvegardes reconnaissant les applications ... 805
Sauvegarde de base de données ... 808
Sauvegarde reconnaissant les applications ... 814
Sauvegarde de boîte de réception ... 817
Restauration de bases de données SQL ... 819
Restauration de bases de données Exchange ... 828
Restauration de boîtes aux lettres et éléments de boîtes aux lettres Exchange ... 831
Modification des informations d'identification de SQL Server ou d'Exchange Server ... 839
Protection des terminaux mobiles ... 840
Terminaux mobiles pris en charge ... 840
Ce que vous pouvez sauvegarder ... 840
Ce que vous devez savoir ... 841
Où trouver l'application Acronis Cyber Protect ... 842
Comment commencer à sauvegarde vos données ... 842

© Acronis International GmbH, 2003-2026

Comment restaurer les données vers un terminal mobile ... 842
Comment examiner des données à partir de la console Cyber Protect ... 843
Protection des données Microsoft 365 ... 844
Comparaison des solutions de sauvegarde pour les données Microsoft 365 ... 845
Droits utilisateurs requis ... 851
Ajout d'une organisation Microsoft 365 ... 853
Administration d'organisations Microsoft 365 organisations ajoutées à différents niveaux ... 854
Découverte de ressources Microsoft 365 ... 855
Suppression d'une organisation Microsoft 365 ... 856
Révocation des droits d'accès de l'application de service de sauvegarde ... 857
Rapport des licences de poste Microsoft 365 ... 857
Configuration de la fréquence des sauvegardes Microsoft 365 ... 858
Microsoft 365 Business – Sauvegarde ... 859
Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365 ... 902
Agent pour Office 365 installé localement ... 912
Protection des données Google Workspace ... 917
Que signifie la protection Google Workspace ? ... 917
Droits utilisateurs requis ... 918
À propos de la planification de sauvegarde ... 918
Limites ... 919
Ajouter une organisation Google Workspace ... 919
Création d'un projet Google Cloud personnel ... 921
Découverte des ressources Google Workspace ... 924
Configuration de la fréquence des sauvegardes Google Workspace ... 925
Protéger des données Gmail ... 926
Protéger des fichiers Google Drive ... 930
Protection des fichiers de Drive partagés ... 935
Notarisation ... 939
Recherche dans les sauvegardes cloud à cloud ... 941
Recherche en texte intégral ... 942
Index de recherche ... 942
Vérification de la taille d'un index de recherche ... 943
Mise à jour, reconstruction ou suppression des index ... 943
Activation de la recherche améliorée dans les sauvegardes chiffrées ... 944
Désactivation de la recherche en texte intégral pour les sauvegardes Gmail ... 945
Sauvegarde d'Oracle Database ... 946
Protection de SAP HANA ... 946

© Acronis International GmbH, 2003-2026

Protection des données MySQL et MariaDB ... 946
Configuration d'une sauvegarde reconnaissant les applications ... 947
Restauration à partir d'une sauvegarde reconnaissant les applications ... 948
Protection des machines virtuelles et des conteneurs Proxmox ... 953
Limitations pour les ressources Proxmox ... 954
Installation de l'agent pour Proxmox ... 955
Sauvegarde des ressources Proxmox ... 955
Restaurer des ressources Proxmox ... 955
Protéger les serveurs d'hébergement Web ... 956
Quotas ... 956
Intégration de DirectAdmin, de cPanel et de Plesk ... 956
Opérations spéciales avec les machines virtuelles ... 957
Exécution d'une machine virtuelle à partir d'une sauvegarde (restauration instantanée) ... 957
Fonctionnement dans VMware vSphere ... 961
Sauvegarde de machines Hyper-V en cluster. ... 985
Limite le nombre total de machines virtuelles sauvegardées simultanément. ... 986
Sauvegarde avec agent de machines virtuelles Microsoft Azure et Amazon EC2 ... 988
Création d'un support de démarrage afin de restaurer des systèmes d'exploitation ... 989
Support de démarrage personnalisé ou tout prêt ? ... 990
Support de démarrage basé sur Linux ou sur WinPE/WinRE ? ... 990
Création d'un support de démarrage physique ... 991
Bootable Media Builder ... 992
Restauration du stockage Cloud ... 996
Restauration depuis un partage réseau ... 996
Fichiers d'un script ... 997
Structure d'autostart.json ... 998
Objet Toplevel ... 998
Objet de variable ... 998
Type de contrôle ... 999
Connexion à un ordinateur démarré à partir d'un support de démarrage ... 1007
Opérations locales avec support de démarrage ... 1007
Opérations à distance avec un support de démarrage ... 1009
Prise en charge de l'agrégation de cartes réseau ... 1011
Startup Recovery Manager ... 1012
Implémentation de la reprise d'activité après sinistre ... 1016
À propos d'Acronis Disaster Recovery ... 1016
Disaster Recovery vers Cyber Protect Cloud ... 1016

© Acronis International GmbH, 2003-2026

Les fonctionnalités clés ... 1016
Exigences logicielles pour Disaster Recovery vers Cyber Protect Cloud ... 1017
Version d'évaluation Disaster Recovery ... 1020
Opérations réalisées avec les machines virtuelles Microsoft Azure ... 1020
Limites d'utilisation du stockage géoredondant dans le cloud ... 1021
Suppression automatique des environnements clients non utilisés sur un site dans le Cloud 1021
Travail avec Disaster Recovery vers Cyber Protect Cloud ... 1022
Création d'un plan de protection de reprise d'activité après sinistre ... 1022
Connectivité et réseaux ... 1026
Prérequis ... 1029
Configuration requise ... 1032
Ports ... 1033
Prérequis ... 1051
Prérequis ... 1054
Serveurs Cloud ... 1066
Points de calcul ... 1082
Basculement test ... 1083
Basculement test automatisé ... 1085
Basculement de la production ... 1087
Restauration automatique ... 1091
Orchestration (runbooks) ... 1104
Suppression du site de reprise d'activité après sinistre ... 1110
Disaster Recovery vers Microsoft Azure ... 1111
Exigences logicielles pour Disaster Recovery vers Microsoft Azure ... 1112
Licence de Disaster Recovery pour Microsoft Azure ... 1114
Travailler avec Disaster Recovery vers Microsoft Azure ... 1114
Gestion de l'accès à votre abonnement Microsoft Azure ... 1115
Problèmes de configuration inter-abonnements dans Microsoft Azure ... 1115
Création d'un plan de protection de reprise d'activité après sinistre avec Microsoft Azure ... 1116
Gestion du site de reprise d'activité après sinistre dans Microsoft Azure ... 1117
Connectivité et réseaux dans Microsoft Azure ... 1120
Serveurs de restauration dans Microsoft Azure ... 1126
Basculement dans Microsoft Azure ... 1131
Restauration automatique dans Microsoft Azure ... 1139
Runbooks dans Microsoft Azure ... 1153
Ressources Azure créées lors de la configuration du site DR et du basculement ... 1158

© Acronis International GmbH, 2003-2026

Suppression douce des tenants disposant d'un site de reprise d'activité après sinistre dans Microsoft Azure ... 1158
Agents dans Microsoft Azure ... 1159
Tableau de bord Reprise d'activité après sinistre ... 1159
Terminaux éligibles à la reprise d'activité après sinistre ... 1159
Vérification de l'intégrité ... 1160
Basculement test automatisé ... 1160
Serveurs de restauration en basculement ... 1161
Serveurs primaires ... 1161
Alertes du serveur dans le cloud ... 1162
Utilisation des points de calcul ... 1162
Compatibilité de Disaster Recovery avec le logiciel de chiffrement ... 1162
Configuration de la protection antivirus et antimalware ... 1164
Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware ... 1164
Fonctionnalités prises en charge par plate-forme ... 1165
Protection contre les virus et les malwares ... 1168
Fonctionnalités antimalware ... 1168
Types d'analyses ... 1168
Paramètres de protection contre les virus et les malwares ... 1170
Active Protection dans l'édition Cyber Backup Standard ... 1188
Paramètres d'Active Protection dans Cyber Backup Standard ... 1188
Filtrage d'URL ... 1197
Comment fonctionne le filtrage d'URL ... 1197
Configurer le filtrage d'URL ... 1199
Paramètres du filtrage d'URL ... 1199
Antivirus Microsoft Defender et Microsoft Security Essentials ... 1208
Planifier l'analyse ... 1209
Actions par défaut ... 1210
Protection en temps réel ... 1210
Advanced ... 1211
Exclusions ... 1212
Gestion du pare-feu ... 1212
Quarantaine ... 1213
Comment les fichiers arrivent-ils dans le dossier de quarantaine ? ... 1213
Gestion des fichiers mis en quarantaine ... 1214
Emplacement de quarantaine sur les machines ... 1215
Dossier personnalisé en libre-service et à la demande ... 1215

© Acronis International GmbH, 2003-2026

Liste blanche d'entreprise ... 1215
Ajout automatique à la liste blanche ... 1216
Ajout manuel à la liste blanche ... 1216
Ajout de fichiers mis en quarantaine à la liste blanche ... 1216
Paramètres de liste blanche ... 1216
Afficher les détails à propos des éléments de la liste blanche ... 1217
Analyse antimalware des sauvegardes ... 1217
Limites ... 1218
Configuration de la sécurité de votre intelligence artificielle générative ... 1220
Paramètres de sécurité de l'intelligence artificielle générative ... 1220
Surveillance de l'utilisation ... 1220
Champ d'application de la protection ... 1221
Prévention des pertes de données GenAI ... 1221
Protection contre l'injection de prompt ... 1222
Gestion et affectation des workflows d'automatisation ... 1223
Comment créer, configurer et activer un workflow ... 1223
Affichage des workflows actuels ... 1226
Création d'un workflow ... 1227
Composants et modèles de workflow ... 1231
Gestion de vos workflows ... 1233
Activation d'un workflow ... 1234
Affectation des workflows ... 1235
Visualisation de l'historique d'exécution d'un workflow ... 1236
Clonage d'un workflow ... 1236
Mise à jour d'un workflow ... 1237
Suppression d'un workflow ... 1237
Versions de workflow ... 1237
Visualisation d'une version de workflow ... 1238
Créer une nouvelle version d'un workflow ... 1239
Définir la version par défaut d'un workflow ... 1240
Clonage d'une version de workflow ... 1240
Suppression d'une version de workflow ... 1241
XDR (Extended Detection and Response) ... 1242
Utilité de la fonctionnalité XDR (Extended Detection and Response) ... 1242
Activation de la fonctionnalité XDR (Extended Detection and Response) ... 1243
Utilisation du graphique XDR ... 1244
Procédure d'analyse du graphique XDR ... 1245

© Acronis International GmbH, 2003-2026

Recherche de nœuds individuels ... 1247
Application des mesures d'intervention ... 1248
Affichage des erreurs d'intégration XDR ... 1249
Icônes du graphique XDR ... 1249
Endpoint Detection and Response (EDR) ... **1251**
Utilité de la fonctionnalité EDR (Endpoint Detection and Response) ... 1251
Fonctionnalités EDR ... 1252
Exigences logicielles pour Endpoint Detection and Response ... 1255
Activation de la fonctionnalité EDR (Endpoint Detection and Response) ... 1255
Méthode d'utilisation de la fonctionnalité EDR (Endpoint Detection and Response) ... 1258
Examen des incidents ... 1259
Exemples de requêtes ... 1275
Types d'événements ... 1276
Exemples de types de données ... 1277
Champs d'événements ... 1278
Enquête sur les incidents ... 1286
Atténuation d'incidents ... 1304
Activation du mode de surveillance pour EDR (Endpoint Detection and Response) ... 1339
Test du fonctionnement de la fonctionnalité EDR (Endpoint Detection and Response) ... 1341
RMM ... **1344**
Gestion et surveillance de l'environnement Microsoft 365 ... 1345
Configuration des connexions Microsoft 365 ... 1345
Examen du niveau de sécurité ... 1349
Travail avec les références ... 1351
Gestion des modèles de référence du tenant ... 1368
Gestion des utilisateurs Microsoft 365 ... 1375
Gestion de votre inventaire matériel ... 1379
Activation ou désactivation de l'analyse de l'inventaire matériel ... 1380
Démarrage manuel d'une analyse de l'inventaire matériel ... 1381
Navigation dans l'inventaire du matériel ... 1381
Affichage du matériel d'un seul terminal ... 1384
Gestion de logiciels ... 1385
Gestion de votre inventaire de logiciels ... 1386
Évaluation des vulnérabilités et gestion des correctifs ... 1390
Configuration du plan de protection Correctifs Test ... **1415**
Configuration du plan de protection Correctifs Production ... **1416**
Exécution du plan de protection Correctifs Test et refus des correctifs non sécurisés ... **1417**

© Acronis International GmbH, 2003-2026

Utilisation des référentiels de logiciels et des packages logiciels ... 1429
Arguments de commande ... 1437
Chemin de désinstallation ... 1437
Arguments de commande ... 1437
Installation du logiciel ... 1438
Désinstallation du logiciel ... 1442
Plans de déploiement de logiciels ... 1446
Connexion à des ressources de type Bureau ou assistance à distance ... 1459
Fonctionnalités prises en charge de bureau et assistance à distance ... 1460
Systèmes d'exploitation pris en charge pour le bureau à distance et l'assistance ... 1463
Protocoles de connexion à distance ... 1464
Redirection du son à distance ... 1465
Connexions à des ressources distantes de type bureau ou assistance à distance ... 1466
Plans de gestion à distance ... 1467
Identifiants de la ressource ... 1481
Utilisation des ressources gérées ... 1484
Utilisation des ressources non gérées ... 1502
Utilisation de la barre d'outils dans la fenêtre de la visionneuse ... 1505
Enregistrement et lecture de sessions à distance ... 1508
Configuration des paramètres Connect Client ... 1509
Notificateurs de Bureau à distance ... 1510
Suivi de la géolocalisation ... 1512
Chat d'assistance ... 1515
Surveillance de l'intégrité et des performances de la ressource ... 1523
Surveillance basée sur une anomalie ... 1524
Plates-formes prises en charge pour la surveillance ... 1524
Moniteurs configurables ... 1525
Plans de surveillance ... 1561
Alertes de surveillance ... 1571
Configuration des stratégies de notification par e-mail ... 1579
Visualisation des données des moniteurs ... 1580
Prévention des pertes de données ... 1583
Création des règles et des règles de flux de données ... 1583
Structure de la règle de flux de données ... 1585
Structure de règle ... 1586
Ajustement des autorisations dans les règles de flux de données ... 1588
Combinaison de règles de flux de données ... 1589

© Acronis International GmbH, 2003-2026

Examen et gestion des stratégies ... 1590
Renouvellement de la règle de flux de données ... 1590
Activation de Data Loss Prevention dans les plans de protection ... 1593
Paramètres avancés ... 1595
Détection automatique de la destination ... 1596
Définitions des données sensibles ... 1597
Informations de santé protégées (PHI) ... 1597
Informations personnelles identifiables (PII) ... 1599
Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) ... 1601
Marqué confidentiel ... 1602
Événements de prévention des pertes de données ... 1604
Widgets Data Loss Prevention dans le tableau de bord Vue d'ensemble ... 1605
Catégories personnalisées de sensibilité ... 1606
Détecteurs de contenu personnalisés ... 1607
Carte de l'organisation ... 1610
Comment cela fonctionne-t-il ? ... 1611
Problèmes connus et limites ... 1613
Autres outils Cyber Protection ... 1615
Mode de conformité ... 1615
Limites ... 1615
Fonctionnalités non prises en charge ... 1615
Définition du mot de passe de chiffrement ... 1616
Modification du mot de passe de chiffrement ... 1616
Restauration de sauvegardes dans les tenants en mode de conformité ... 1617
Stockage immuable ... 1617
Modes de stockage immuable ... 1618
Stockages et agents pris en charge ... 1618
Activation du stockage immuable ... 1619
Désactivation du stockage immuable ... 1620
Accès aux sauvegardes supprimées dans le stockage immuable ... 1621
Affichage de l'utilisation du stockage immuable ... 1621
Stockage géoredondant ... 1622
Limites ... 1622
Activation du stockage géoredondant ... 1622
Désactivation du stockage géoredondant ... 1623
Affichage du statut de la géoréplication ... 1624
Stockage d'archives ... 1624

© Acronis International GmbH, 2003-2026

Fonctionnalités compatibles avec S3 1625
Gestion des compartiments dans le stockage d'archive 1627
Accéder au stockage d'archive via des clients tiers 1631
Tableau de bord de sensibilisation 1633
Utilisation du service de formation et de sensibilisation à la sécurité 1633
OpenVPN de site à site – Informations complémentaires 1634
Glossaire 1641
Index 1646

© Acronis International GmbH, 2003-2026

Prise en main de Cyber Protection

Activation du compte

Lorsqu'un administrateur vous crée un compte, un e-mail vous est envoyé. Le message contient les informations suivantes :

- **Votre identifiant.** Nom d'utilisateur que vous utilisez pour vous connecter. Votre identifiant figure également sur la page d'activation du compte.
- Bouton **Activer le compte**. Cliquez sur le bouton et définissez le mot de passe de votre compte. Assurez-vous que votre mot de passe comporte au moins neuf caractères. Pour en savoir plus sur le mot de passe, consultez "Exigences relatives au mot de passe" (p. 21).

Si votre administrateur a activé l'authentification à deux facteurs, vous serez invité à la configurer pour votre compte. Pour plus d'informations à ce sujet, reportez-vous à "Authentification à deux facteurs" (p. 21).

Exigences relatives au mot de passe

La complexité des mots de passe est vérifiée lors de l'inscription de l'utilisateur et les mots de passe sont classés dans l'une des catégories suivantes :

- Faible
- Moyenne
- Fort

Vous ne pouvez pas enregistrer un mot de passe faible, même s'il contient 9 caractères ou plus. Les mots de passe qui contiennent le nom de l'utilisateur, l'identifiant, l'adresse e-mail de l'utilisateur ou le nom du tenant auquel le compte utilisateur appartient sont toujours considérés comme étant faibles. La plupart des mots de passe courants sont également considérés comme faibles.

Remarque
Les exigences en matière de mot de passe sont susceptibles de changer.

Pour renforcer un mot de passe, ajoutez-lui des caractères. L'utilisation de différents types de caractères (chiffres, majuscules, minuscules et caractères spéciaux) n'est pas obligatoire, mais permet d'obtenir des mots de passe plus forts, mais aussi plus courts.

Authentification à deux facteurs

L'authentification à deux facteurs vous protège davantage contre l'accès non autorisé à votre compte. Lorsque l'authentification à deux facteurs est configurée, vous devez saisir votre mot de passe (premier facteur) et un code unique (second facteur) pour vous connecter à la console Cyber Protect. Le code unique est généré par une application spéciale qui doit être installée sur votre téléphone mobile ou un autre terminal vous appartenant. Même si quelqu'un découvre votre

© Acronis International GmbH, 2003-2026

identifiant et votre mot de passe, il ne pourra pas se connecter à votre compte sans avoir accès à le terminal qui applique le second facteur.

Configuration de l'authentification à deux facteurs pour votre compte

Vous devez configurer l'authentification à deux facteurs pour votre compte si l'administrateur l'a activée pour votre organisation. Si l'administrateur active l'authentification à deux facteurs alors que vous êtes connecté à la console Cyber Protect, vous devrez la configurer à l'expiration de votre session actuelle.

Prérequis

- L'authentification à deux facteurs est activée pour votre organisation par un administrateur.

Pour configurer l'authentification à deux facteurs pour votre compte

1. Choisissez un terminal pour le second facteur.
   C'est souvent un téléphone portable, mais vous pouvez également utiliser une tablette, un ordinateur portable, ou un ordinateur de bureau.
2. Installez une application d'authentification sur votre terminal servant à l'authentification à deux facteurs.
   Exemples d'applications d'authentification :
   - Microsoft Authenticator
   - Google Authenticator
   - Twilio Authy
3. Scannez le QR code à l'aide de votre application d'authentification, puis saisissez le code à 6 chiffres affiché dans l'application d'authentification, dans la fenêtre **Configurer l'authentification à deux facteurs**.
4. Cliquez sur **Suivant**.
   Les instructions qui concernent la restauration de votre accès à votre compte (si vous perdez votre terminal avec authentification à deux facteurs ou désinstallez l'application d'authentification) s'affichent.
5. Enregistrez ou imprimez le fichier PDF.

   Remarque
   Veillez à enregistrer le fichier PDF dans un endroit sûr ou à l'imprimer pour vous y reporter ultérieurement. C'est la meilleure façon de restaurer l'accès.

6. Retournez à la page de connexion de la console Cyber Protect et saisissez le code généré.
   Un code unique est valable 30 secondes. Si vous attendez plus de 30 secondes, utilisez le code généré juste après.

Remarque
Si votre application d'authentification prend en charge la sauvegarde, nous vous recommandons de sauvegarder votre configuration dans le cloud.

© Acronis International GmbH, 2003-2026

Lors de votre prochaine connexion, vous pourrez cocher la case **Faire confiance à ce navigateur**. Dans ce cas, le code ne sera pas requis lors des connexions suivantes avec ce navigateur sur cet ordinateur.

Remarque
Nous vous recommandons de ne pas cocher cette case. Sinon, vous perdrez l'accès aux paramètres d'authentification à deux facteurs pour votre compte.

Pour configurer l'authentification à deux facteurs sur un nouveau terminal

Cette procédure est applicable si vous avez accès à l'application d'authentification configurée précédemment.

1. Installez une application d'authentification sur votre nouveau terminal.
2. Utilisez le fichier PDF que vous avez enregistré lorsque vous avez configuré l'authentification à deux facteurs sur votre terminal.
   Ce fichier contient le code à 32 chiffres que vous devez saisir dans l'application d'authentification pour réassocier cette application à votre compte Acronis.

   Important
   Si le code ne fonctionne pas, veillez à ce que l'heure dans l'application d'authentification pour mobile soit synchronisée avec votre terminal.

Si vous n'avez pas enregistré le fichier PDF pendant l'installation :

1. Cliquez sur **Réinitialiser l'authentification à deux facteurs**, puis saisissez le mot de passe à usage unique dans l'application d'authentification sur mobile.
2. Suivez les instructions affichées à l'écran.

Pour restaurer l'accès à votre compte lorsque l'authentification à deux facteurs est activée

Ces options s'appliquent lorsque vous n'avez pas accès à l'application d'authentification configurée précédemment, dans le cas, par exemple, où le terminal aurait été perdu, volé ou effacé.

- Pour reconfigurer l'application d'authentification TOTP, utilisez le code de l'authentification à deux facteurs fourni lors de la configuration initiale de cette authentification. Le nom de fichier par défaut est `cyberprotect-2fa-backupcode.pdf`.
- Si vous avez une sauvegarde dans l'application d'authentification, restaurez la configuration de l'authentification à deux facteurs à partir de la sauvegarde.
- Pour réinitialiser la configuration de l'authentification à deux facteurs, contactez l'administrateur de votre compte qui a accès au portail de gestion dans le cloud.
- Demandez à votre fournisseur de services de réinitialiser la configuration d'authentification à deux facteurs.
- Contactez l'équipe de support du fournisseur pour obtenir de l'aide.

© Acronis International GmbH, 2003-2026

Paramètres de confidentialité

Les paramètres de confidentialité vous aident à indiquer si vous donnez ou non votre consentement pour la collecte, l'utilisation et la divulgation de vos informations personnelles.

En fonction du pays dans lequel vous utilisez Cyber Protect Cloud et du centre de données Cyber Protect Cloud qui vous fournit des services, lors du lancement initial de Cyber Protect Cloud vous serez peut-être invité à confirmer si vous acceptez ou non d'utiliser Google Analytics dans Cyber Protect Cloud.

Google Analytics nous aide à mieux comprendre le comportement des utilisateurs et à leur offrir une meilleure expérience dans Cyber Protect Cloud en collectant des données avec pseudonyme.

Si vous avez activé ou refusé d'activer Google Analytics lors du lancement initial de Cyber Protect Cloud, vous pouvez changer d'avis ultérieurement.

Activer ou désactiver Google Analytics

1. Dans la console Cyber Protect, cliquez sur **Gérer les comptes**.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit.
3. Sélectionnez **Mes paramètres de confidentialité**. La fenêtre **Mes paramètres de confidentialité** s'affiche.
4. Dans la section **Collecte de données Google Analytics**, cliquez sur l'un des boutons suivants :
   - **Activé** pour activer Google Analytics
   - **Désactivé** pour désactiver Google Analytics

Dans la section **Comment supprimer les cookies**, vous pouvez contrôler et gérer les cookies directement dans votre navigateur.

Remarque
Si la section Google Analytics n'apparaît pas, cela signifie que Google Analytics n'est pas utilisé dans votre pays.

Dans la section **Intégration au produit et aide interactive** (affichée initialement pendant la période d'évaluation) vous pouvez choisir d'arrêter ou de continuer de recevoir les informations sur les améliorations et nouvelles fonctionnalités du programme. La fonctionnalité est activée par défaut, mais vous pouvez la désactiver en paramétrant le commutateur sur **Désactiver**.

Accès au service Cyber Protection

Une fois que vous avez activé votre compte, vous pouvez accéder au service Cyber Protection en vous connectant à la console Cyber Protect ou via Portail de gestion.

Vous connecter à la console Cyber Protect

© Acronis International GmbH, 2003-2026

1. Allez à la page de connexion de Cyber Protection.
2. Saisissez votre identifiant, puis cliquez sur **Suivant**.
3. Saisissez votre mot de passe, puis cliquez sur **Suivant**.
4. [Si vous utilisez plusieurs services Cyber Protect Cloud] Cliquez sur **Cyberprotection**.

   Vous pouvez basculer entre les services disponibles et Portail de gestion en utilisant l'icône  dans le coin supérieur droit.

Le délai d'expiration pour la console Cyber Protect est de 24 heures pour les sessions actives et d'une heure pour les sessions inactives.

Vous pouvez modifier la langue de l'interface Web en cliquant sur l'icône de compte dans l'angle supérieur droit.

Pour accéder à la console Cyber Protect via Portail de gestion

1. Dans le portail de gestion, accédez à **Surveillance** > **Utilisation**.
2. Sous **Cyber Protect**, sélectionnez **Protection**, puis cliquez sur **Gérer le service**.
   Vous pouvez aussi sélectionner un client sous **Clients**, puis cliquer sur **Gérer le service**.

Vous serez alors redirigé vers la console Cyber Protect.

Important
Si le client est en mode de gestion **Libre-service**, vous ne pouvez pas gérer les services à sa place. Seuls les administrateurs clients peuvent modifier le mode client et sélectionner **Géré par le fournisseur de services**, puis gérer les services.

Pour réinitialiser votre mot de passe

1. Allez à la page de connexion de Cyber Protection.
2. Saisissez votre identifiant, puis cliquez sur **Suivant**.
3. Cliquez sur **Mot de passe oublié ?**
4. Cliquez sur **Envoyer** pour recevoir des instructions supplémentaires par e-mail.
5. Suivez les instructions dans le message e-mail pour créer un nouveau mot de passe.

Navigateurs Web pris en charge

La console Cyber Protect utilise le protocole TLS 1.2 et prend en charge les navigateurs Web suivants :

- Google Chrome 109 ou version ultérieure
- Mozilla Firefox 115 ou version ultérieure
- Opera 95 ou version ultérieure (Chromium 109)
- Microsoft Edge 109 ou version ultérieure

© Acronis International GmbH, 2003-2026

- Apple Safari (pour Mac OS X) 16 ou version ultérieure, exécuté dans les systèmes d'exploitation macOS et iOS

Il est possible que les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) n'affichent pas correctement l'interface utilisateur ou ne proposent pas certaines fonctions.

Les navigateurs mobiles ne sont pas pris en charge.

Ma boîte de réception

La page Ma boîte de réception est conçue pour rationaliser votre communication au sein de l'application. En suivant ce guide, vous pouvez gérer efficacement vos messages, rester organisé et améliorer votre productivité. La boîte de réception de la solution est le centre névralgique dans lequel vous recevez et gérez les communications au sein de l'application. Elle vous permet de rester informé des mises à jour, des messages et des alertes importants dans votre workflow.

Vue d'ensemble

L'onglet **Ma boîte de réception** comporte un compteur de notifications qui affiche le nombre de notifications non lues. En cliquant sur ce compteur, vous pouvez afficher les notifications non lues et suivre facilement les éléments en attente. En outre, les compteurs situés à côté de chacun des filtres (catégorie, importance, action) permettent de connaître la répartition des notifications dans les différentes catégories.

Vous recevrez dans votre boîte de réception des notifications de différents types correspondant au contexte et aux objectifs spécifiques définis dans les paramètres de compte : annonces de fonctionnalités, nouveaux programmes de formation disponibles, invitations à des événements et des webinaires, rappels d'expiration de certificat, promotions, avis de maintenance, enquêtes, etc.

Vérification de vos notifications

Vérification de votre section de notification

1. Connectez-vous à la console Cyber Protect Cloud.
2. Dans le volet de navigation, sélectionnez l'option de menu **Ma boîte de réception**.

Recherche dans Ma boîte de réception

Pour rechercher des messages non lus

1. Cliquez sur l'option de menu **Ma boîte de réception**.
2. Dans l'angle supérieur droit, activez le bouton **Afficher uniquement les éléments non lus**.

Pour rechercher des informations importantes dans votre boîte de réception

© Acronis International GmbH, 2003-2026

1. Accédez à **Ma boîte de réception** depuis le tableau de bord Cyber Protect Cloud.
2. Dans la vue de la boîte de réception, localisez la **barre de recherche**, en haut.
3. Saisissez les mots-clés ou les noms d'expéditeur pertinents pour filtrer les messages.
4. Appuyez sur la touche **Entrée** pour afficher les résultats de la recherche.

Les résultats affichent toutes les notifications correspondant à vos critères de recherche.

Fonctionnalités de protection prises en charge par système d'exploitation

Cette rubrique contient des informations sur les fonctionnalités de protection de Cyber Protect Cloud. Pour consulter la liste des systèmes d'exploitation et des environnements pris en charge par la sauvegarde et la restauration, voir "Systèmes d'exploitation et environnements pris en charge pour la sauvegarde et la restauration" (p. 513).

Les fonctionnalités de protection ne sont prises en charge que sur les ordinateurs sur lesquels un agent de protection est installé. Elles ne sont pas disponibles pour les machines virtuelles sauvegardées en mode sans agent, par exemple par l'agent pour Hyper-V, l'agent pour VMware, l'agent pour Virtuozzo Hybrid Infrastructure, l'agent pour Scale Computing ou l'agent pour oVirt.

Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Systèmes d'exploitation et versions pris en charge

Windows

Sauf indication contraire pour un ensemble spécifique de fonctionnalités, les versions Windows suivantes sont prises en charge :

- Windows 7 Service Pack 1 et versions ultérieures
- Windows Server 2008 R2 Service Pack 1 et versions ultérieures

Remarque
Pour Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft avant d'installer l'agent de protection :

- Mises à jour de sécurité étendues (ESU) pour Windows 7
- KB4474419
- KB4490628

Pour plus d'informations sur les mises à jour requises, voir cet article de la base de connaissances.

Linux

© Acronis International GmbH, 2003-2026

Les distributions Linux et leurs versions prises en charge dépendent des ensembles de fonctionnalités et sont affichées au bas de chaque tableau.

macOS

Les versions macOS prises en charge dépendent des ensembles de fonctionnalités et sont affichées au bas de chaque tableau.

Fonctionnalité	Windows	Linux	macOS
Plans de protection par défaut			
Employés en télétravail	Oui	Non	Non
Employés de bureau (Antivirus tiers)	Oui	Non	Non
Employés de bureau (Antivirus Cyber Protect)	Oui	Non	Non
Cyber Protect Essentials (uniquement pour l'édition Cyber Protect Essentials)	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Sauvegarde de données d'investigation			
Collecter le vidage mémoire	Oui	Non	Non
Instantané des processus en cours d'exécution	Oui	Non	Non
Notarisation de la sauvegarde de données d'investigation de l'image locale	Oui	Non	Non
Notarisation de la sauvegarde de données d'investigation de l'image Cloud	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Protection continue des données (CDP)			
Protection continue des données pour les fichiers et dossiers	Oui	Non	Non
Protection continue des données pour les fichiers modifiés via le suivi de l'application	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Découverte automatique et installation à distance			
Découverte basée sur le réseau	Oui	Non	Non
Découverte basée sur Active Directory*	Oui	Non	Non
Découverte basée sur le modèle (importer les machines depuis un fichier)	Oui	Non	Non
Ajout manuel de terminaux	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

*La découverte basée sur Active Directory ne fonctionne pas comme prévu avec la configuration par défaut de Windows Server 2025 car elle applique le chiffrement LDAP par défaut. Voir cet article de la base de connaissances.

Active Protection

Fonctionnalité	Windows	Linux	macOS
Détection d'un processus d'injection	Oui	Non	Non
Restauration automatique de fichiers affectés depuis le cache local	Oui	Oui	Oui
Auto-défense pour les fichiers de sauvegarde Acronis	Oui	Non	Non
Auto-défense pour le logiciel Acronis	Oui	Non	Oui (Uniquement les composants Active Protection et Antimalware)
Gestion des processus fiables/bloqués	Oui	Non	Oui
Exclusions des processus/dossiers	Oui	Oui	Oui
Détection des ransomware basée sur un comportement de processus (basé sur l'IA)	Oui	Oui	Oui
Détection du cryptominage basée sur un comportement de processus	Oui	Non	Non
Protection des lecteurs externes (HDD, lecteurs flash, cartes SD)	Oui	Non	Oui

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Protection du dossier réseau	Oui	Non*	Oui
Protection côté serveur	Oui	Non	Non
Protection Zoom, Cisco Webex, Citrix Workspace et Microsoft Teams	Oui	Non	Non

*Les dossiers réseau sous Linux sont traités comme des dossiers locaux ; ainsi, Active Protection protégera automatiquement les dossiers réseau dans le système d'exploitation Linux, comme s'il s'agissait de dossiers locaux.

Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Protection contre les virus et les malwares

Fonctionnalité	Windows	Linux	macOS
Fonctionnalité Active Protection totalement intégrée	Oui	Non	Non
Protection antimalware en temps réel	Oui	Oui	Oui
Fonctionnalité avancée de protection antimalware en temps réel avec détection basée sur la signature locale	Oui	Oui	Oui
Analyse statique pour les fichiers exécutables portables	Oui	Non	Oui[1]
Analyse antimalware à la demande	Oui	Oui[2]	Oui
Protection du dossier réseau	Oui	Non[3]	Non
Protection côté serveur	Oui	Non	Non
Analyse des fichiers d'archive	Oui	Non	Oui
Analyse des lecteurs amovibles	Oui	Non	Oui
Analyse des fichiers nouveaux et modifiés uniquement	Oui	Non	Oui
Exclusions de fichier/dossier	Oui	Oui	Oui[4]
Exclusions des processus	Oui	Non	Oui
Moteur d'analyse du comportement	Oui	Oui[5]	Oui
Prévention des failles	Oui	Non	Non
Quarantaine	Oui	Oui	Oui

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Nettoyage automatique de la zone de quarantaine	Oui	Oui	Oui
Filtrage d'URL (http/https)	Oui	Non	Non
Liste blanche à l'échelle de l'entreprise	Oui	Non	Oui
Gestion du pare-feu[6]	Oui	Non	Non
Gestion de Microsoft Defender Antivirus[7]	Oui	Non	Non
Gestion de Microsoft Security Essentials	Oui	Non	Non
Inscription et gestion de la protection contre les virus et les malwares via le centre de sécurité Windows	Oui	Non	Non

[1] L'analyse statique pour les fichiers exécutables portables est prise en charge uniquement pour les analyses planifiées sur macOS.

[2] Les conditions de démarrage ne sont pas prises en charge pour l'analyse à la demande sous Linux.

[3] Les dossiers réseau dans Linux sont traités comme des dossiers locaux, c'est pourquoi Active Protection protégera automatiquement les dossiers réseau dans le système d'exploitation Linux, comme s'il s'agissait de dossiers locaux.

[4] Les exclusions de fichier/dossier sont prises en charge uniquement lorsque vous spécifiez les fichiers et les dossiers qui ne seront pas analysés par la protection en temps réel ni par les analyses planifiées sur macOS.

[5] Le moteur d'analyse comportementale prend en charge les versions Linux suivantes :

- CentOS 7.x
- Debian 10.x, 11.x
- CloudLinux 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.04, et 22.04

[6] La gestion du pare-feu est prise en charge sur Windows 8 et versions ultérieures. Windows Server n'est pas pris en charge.

[7] La gestion de l'Antivirus Microsoft Defender est prise en charge sur Windows 8.1 et versions ultérieures.

Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Fonctionnalité	Windows	Linux	macOS
Endpoint detection and response			
Endpoint detection and response[1]	Oui	Oui	Oui
Surveillance étendue	Oui	Oui	Non

[1]Voir "Fonctionnalités EDR" (p. 1252).

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Endpoint detection and response			
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Exigences logicielles pour Endpoint Detection and Response" (p. 1255).			

Fonctionnalité	Windows	Linux	macOS
Évaluation des vulnérabilités			
Évaluation des vulnérabilités du système d'exploitation et de ses applications natives	Oui	Oui*	Oui
Évaluation des vulnérabilités pour les applications tierces	Oui	Non	Oui
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Solutions Microsoft et tiers prises en charge pour l'évaluation des vulnérabilités" (p. 1391), "Solutions Linux prises en charge pour l'évaluation des vulnérabilités" (p. 1394) et "Solutions Apple et tiers prises en charge pour l'évaluation des vulnérabilités" (p. 1393).			

L'évaluation des vulnérabilités dépend de la disponibilité des alertes de sécurité officielles pour une distribution spécifique, par exemple https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce et d'autres.

Fonctionnalité	Windows	Linux	macOS
Gestion des correctifs			
Approbation manuelle des correctifs	Oui	Non	Non
Installation automatique des correctifs	Oui	Non	Non
Test des correctifs	Oui	Non	Non
Installation manuelle des correctifs	Oui	Non	Non
Programmation des correctifs	Oui	Non	Non
Mise à jour corrective sans échec : sauvegarde de machine avant l'installation de correctifs dans le cadre d'un plan de protection	Oui	Non	Non
Annulation du redémarrage d'une machine si une sauvegarde est en cours d'exécution	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Carte de la protection des données			
Définition ajustable des fichiers importants	Oui	Non	Non
Analyse des machines pour trouver des fichiers non protégés	Oui	Non	Non
Aperçu des emplacements non protégés	Oui	Non	Non
Capacité à démarrer l'action de protection depuis le widget de carte de protection des données (action **Protéger tous les fichiers**)	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
État de santé du disque			
Contrôle de l'état de santé des HDD et SSD basés sur l'IA	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Plans de protection intelligente basés sur les alertes du centre opérationnel de cyberprotection (CPOC) Acronis			
Flux de menaces	Oui	Non	Non
Assistant de réparation	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Analyse de la sauvegarde			
Analyse antimalware des sauvegardes d'images dans le cadre du plan de sauvegarde	Oui	Non	Non
Analyse des sauvegardes d'images pour détecter des malwares dans le Cloud	Oui	Non	Non
Analyse des sauvegardes chiffrées pour détecter des malware	Oui	Non	Non

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Analyse de la sauvegarde			
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Restauration sûre			
Analyse antimalware avec protection contre les virus et les malwares lors du processus de restauration	Oui	Non	Non
Restauration sûre pour les sauvegardes chiffrées	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Connexion à distance au bureau			
Connexion par NEAR	Oui	Oui	Oui
Connexion par RDP	Oui	Non	Non
Connexion via le Partage d'écran Apple	Non	Non	Oui
Connexion par client Web	Oui	Non	Non
Connexion par Assistance rapide	Oui	Oui	Oui
Assistance à distance	Oui	Oui	Oui
Transfert de fichiers	Oui	Oui	Oui
Transmission de captures d'écran	Oui	Oui	Oui
Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Systèmes d'exploitation pris en charge pour le bureau à distance et l'assistance" (p. 1463).			

Fonctionnalité	Windows	Linux	macOS
Score #CyberFit			
Statut de score #CyberFit	Oui	Non	Non
Outil autonome de score #CyberFit	Oui	Non	Non
Recommandations du Score #CyberFit	Oui	Non	Non

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Score #CyberFit			
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Prévention des pertes de données			
Contrôle des terminaux	Oui	Non	Pris en charge sur les Mac dotés de processeurs Intel et fonctionnant sous macOS 10.15 et versions ultérieures ou macOS 11.2.3 et versions ultérieures. Non supporté par les processeurs Apple Silicon basés sur l'ARM, tels que les Apple M1 / M2.
Prévention des pertes de données	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)).			

Fonctionnalité	Windows	Linux	macOS
Options de gestion			
Scénarios de vente incitative pour promouvoir les éditions Cyber Protect	Oui	Oui	Oui
Console d'administration centralisée et à distance basée sur le Web	Oui	Oui	Oui
Systèmes d'exploitation et versions pris en charge : Indépendance par rapport à la plate-forme.			

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Options de protection			
Effacement à distance	Oui	Non	Non
Pris en charge pour Windows 10 et les versions ultérieures.			

Fonctionnalité	Windows	Linux	macOS
Cyber Protect Monitor			
Application Cyber Protect	Oui	Non	Oui
Statut de protection pour Zoom	Oui	Non	Non
Statut de protection pour Cisco Webex	Oui	Non	Non
Statut de protection pour Citrix Workspace	Oui	Non	Non
Statut de protection pour Microsoft Teams	Oui	Non	Non
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)). Sur macOS, Cyber Protect Monitor est pris en charge pour toutes les versions sur lesquelles vous pouvez installer l'agent pour Mac, excepté macOS 10.x. Pour plus d'informations, voir "Agent pour Mac" (p. 520).			

Fonctionnalité	Windows	Linux	macOS
Inventaire du logiciel			
Analyse de l'inventaire du logiciel	Oui	Non	Oui
Surveillance de l'inventaire du logiciel	Oui	Non	Oui
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)). Sur macOS, l'inventaire du logiciel est pris en charge pour les versions 10.13.x à 13.x.			

Fonctionnalité	Windows	Linux	macOS
Inventaire du matériel			
Analyse Inventaire matériel	Oui	Non	Oui
Surveillance de l'inventaire matériel	Oui	Non	Oui
Consultez les versions de Windows prises en charge au début de cette section ("Systèmes d'exploitation et versions pris en charge" (p. 27)). Sur macOS, l'inventaire du matériel est pris en charge pour les versions 10.13.x à 13.x.			

© Acronis International GmbH, 2003-2026

Installation et déploiement d'agents Cyber Protection

Avant de commencer

Préparation

Etape 1

Choisissez un agent en fonction de ce que vous allez sauvegarder. Pour plus d'informations sur les choix possibles, consultez De quel agent ai-je besoin ?

Etape 2

Assurez-vous que l'espace disponible sur votre disque dur est suffisant pour installer un agent. Pour des informations détaillées sur l'espace disque requis, consultez "Configuration système requise pour les agents" (p. 45).

Etape 3

Téléchargez le programme d'installation. Pour trouver les liens de téléchargement, cliquez sur **Tous les terminaux** > **Ajouter**.

La page **Ajouter des terminaux** fournit des programmes d'installation Web pour chacun des agents installés sous Windows. Un programme d'installation Web consiste en un petit fichier exécutable qui télécharge sur Internet le programme d'installation principal et le sauvegarde en tant que fichier temporaire. Ce fichier est automatiquement supprimé après l'installation.

Si vous souhaitez enregistrer les programmes d'installation localement, téléchargez un paquet comprenant tous les agents d'installation pour Windows à l'aide du lien au bas de la page **Ajouter des terminaux**. Des paquets 32 bits et 64 bits sont disponibles. Ces paquets vous permettent de personnaliser la liste des composants à installer. Ces paquets permettent également d'effectuer une installation sans assistance, par exemple via la stratégie de groupe. Ce scénario avancé est décrit dans "Déploiement d'agents de protection via la stratégie de groupe" (p. 135).

Pour télécharger le programme d'installation de l'agent pour Microsoft 365, cliquez sur l'icône de compte dans l'angle supérieur droit, puis cliquez sur **Téléchargements** > **Agent pour Microsoft 365**.

L'installation sous Linux et macOS est effectuée depuis les programmes d'installation habituels.

Tous les programmes d'installation requièrent une connexion Internet afin d'enregistrer la machine au sein du service Cyber Protection. Sans connexion Internet, l'installation ne pourra être effectuée.

© Acronis International GmbH, 2003-2026

Etape 4

Les fonctionnalités Cyber Protect nécessitent le package redistribuable Microsoft Visual C++ 2017. Veillez à ce qu'il soit déjà installé sur votre machine, ou installez-le avant d'installer l'agent. Après l'installation de Microsoft Visual C++, il peut être nécessaire de redémarrer l'ordinateur. Le package redistribuable Microsoft Visual C++ est disponible ici https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Etape 5

Assurez-vous que les pare-feu et les autres composants du système de sécurité de votre réseau (comme un serveur proxy) autorisent les connexions sortantes via les ports TCP suivants.

- Ports **443** et **8443**

  Ces ports permettent d'accéder à la console Cyber Protect, d'enregistrer des agents, de télécharger des certificats, d'autoriser des utilisateurs et de télécharger des fichiers depuis le stockage dans le cloud.
- Ports entre **7770** et **7800**

  Ces ports permettent aux agents de communiquer avec le serveur de gestion.
- Port **44445**

  Les agents utilisent ce port pour le transfert des données pendant la sauvegarde et la restauration.

Si un serveur proxy est activé dans votre réseau, consultez "Configuration des paramètres de serveur proxy" (p. 52) pour savoir si vous devez configurer ces paramètres sur chaque ordinateur qui exécute un agent de protection.

La vitesse minimale de connexion Internet requise pour gérer un agent du Cloud est 1 Mbit/s (à ne pas confondre avec le taux de transfert de données acceptable pour la sauvegarde dans le Cloud). Prenez ceci en compte si vous utilisez une technologie de connexion à faible bande passante, comme la technologie ADSL.

Ports TCP requis pour la sauvegarde et la réplication de machines virtuelles VMware

- Port **443**

  L'agent pour VMware (Windows et appliances virtuelles) se connecte à ce port sur l'hôte ESXi ou le serveur vCenter afin d'exécuter des opérations de gestion de machine virtuelle, comme la création, la mise à jour et la suppression de machines virtuelles sur vSphere lors des opérations de sauvegarde, de restauration et de réplication de MV.
- Port **902**

  L'agent pour VMware (Windows et appliances virtuelles) se connecte à ce port sur l'hôte ESXi afin d'établir des connexions NFC pour lire/écrire des données sur des disques de machine virtuelle lors des opérations de sauvegarde, de restauration et de réplication de machine virtuelle.
- Port **2029**

© Acronis International GmbH, 2003-2026

L'agent pour VMware (appliance virtuelle) écoute sur ce port les requêtes entrantes vers le serveur NFS qui est hébergé sur l'agent. Les connexions via ce port sont requises pour exécuter une machine virtuelle à partir d'une sauvegarde (restauration instantanée).

- Port **3333**

  Si l'agent pour VMware (appliances virtuelles) est en cours d'exécution sur le cluster/hôte ESXi qui est la cible de la réplication de machine virtuelle, le trafic de réplication de machine virtuelle ne va pas directement à l'hôte ESXi sur le port **902**. Au lieu de cela, le trafic part de l'agent pour VMware source et va jusqu'au port TCP **3333** de l'agent pour VMware (appliances virtuelles) situé sur le cluster/hôte ESXi cible.

  L'agent pour VMware source qui lit les données à partir des disques de la MV d'origine peut se trouver à n'importe quel autre emplacement et peut être de n'importe quel type : Appliance virtuelle ou Windows.

  Le service chargé d'accepter les données de réplication de MV sur l'agent pour VMware cible (appliance virtuelle) est appelé « serveur de disque de réplica ». Ce service est chargé des techniques d'optimisation WAN, comme la compression et la déduplication du trafic lors de la réplication de MV, notamment l'amorçage du réplica (voir "Amorçage d'un réplica initial" (p. 966)). Lorsqu'aucun agent pour VMware (appliance virtuelle) n'est en cours d'exécution sur l'hôte ESXi, ce service n'est pas disponible. Par conséquent, le scénario d'amorçage de réplica n'est pas pris en charge.

Ports requis par le composant Téléchargeur

Le composant Téléchargeur est chargé de délivrer des mises à jour à un ordinateur et de les distribuer à d'autres instances du Téléchargeur. Il peut s'exécuter en mode agent, qui transforme l'ordinateur en agent Téléchargeur. L'agent Téléchargeur télécharge des mises à jour depuis Internet et sert de source pour la distribution de mises à jour vers d'autres ordinateurs. Le Téléchargeur nécessite les ports suivants pour fonctionner.

- Port TCP et UDP (entrant) **6888**

  Utilisé par le protocole BitTorrent pour les mises à jour BitTorrent de pair-à-pair.
- Port UDP **6771**

  Utilisé comme port de découverte pair local. Joue également un rôle dans les mises à jour de pair-à-pair.
- Port TCP **18018**

  Utilisé pour la communication entre les programmes de mise à jour fonctionnant dans différents modes : Responsable de la mise à jour et Agent responsable de la mise à jour.
- Port TCP **18019**

  Port local, utilisé pour la communication entre le programme de mise à jour et l'agent de protection.

Étape 6

Vérifiez que les ports locaux suivants ne sont pas utilisés par d'autres processus sur l'ordinateur sur lequel vous prévoyez d'installer l'agent de protection.

© Acronis International GmbH, 2003-2026

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

Remarque
Vous n'avez pas à les ouvrir dans le pare-feu.

Modification des ports utilisés par l'agent de protection

Il se peut que certains des ports requis par l'agent de protection soient utilisés par d'autres applications de votre environnement. Afin d'éviter les conflits, vous pouvez modifier les ports par défaut utilisés par l'agent de protection en modifiant les fichiers suivants.

- Sous Linux : `/opt/Acronis/etc/aakore.yaml`
- Sous Windows : `\ProgramData\Acronis\Agent\etc\aakore.yaml`

Sauvegarde avec et sans agent

La sauvegarde avec agent nécessite l'installation d'un agent de protection sur chaque machine protégée. La sauvegarde avec agent est prise en charge sur toutes les machines physiques et virtuelles. Pour plus d'informations sur l'agent nécessaire et sur son emplacement d'installation, voir "De quel agent ai-je besoin ?" (p. 41)

La sauvegarde sans agent est prise en charge par certaines plates-formes de virtualisation et n'est pas disponible pour les machines physiques. La sauvegarde sans agent ne nécessite qu'un seul agent de protection, installé sur un ordinateur dédié dans l'environnement virtuel. Cet agent sauvegarde toutes les autres machines virtuelles de cet environnement. Pour plus d'informations sur les types de sauvegarde pris en charge par plate-forme de virtualisation, voir "Plates-formes de virtualisation prises en charge" (p. 526).

Les appliances virtuelles sont disponibles pour certaines plates-formes de virtualisation. Une appliance virtuelle est une machine virtuelle prête à l'emploi contenant un agent de protection. Les appliances virtuelles sont disponibles dans un format propre à l'hyperviseur, par exemple, .ovf, .ova ou .qcow.

De quel type de sauvegarde ai-je besoin ?

Nous recommandons la sauvegarde basée sur un agent si vous avez besoin des éléments suivants :

- Fonctionnalité de protection supplémentaire, telle qu'un antivirus ou un antimalware, la gestion des correctifs ou la connexion Bureau à distance. Pour plus d'informations sur ces fonctionnalités, voir "Fonctionnalités de protection prises en charge par système d'exploitation" (p. 27).
- Machines virtuelles séparées au niveau du tenant. Par exemple, lorsque vous souhaitez que les utilisateurs du tenant n’aient accès qu’à leurs propres sauvegardes.

© Acronis International GmbH, 2003-2026

- Sauvegardes au niveau des fichiers que vous pouvez restaurer sur les systèmes d'exploitation invités.

Nous recommandons la sauvegarde sans agent si vous avez besoin des éléments suivants :

- Il s'agit uniquement d'une sauvegarde, sans aucun dispositif de protection supplémentaire.
- Gestion simplifiée : vous pouvez sauvegarder plusieurs machines virtuelles en installant et en configurant un seul agent.
- Utilisation minimale des ressources : un agent dédié utilise moins de processeur et de mémoire RAM que plusieurs agents installés sur chaque machine virtuelle de votre environnement.
- Configurations de sauvegarde spécifiques telles que la sauvegarde sans réseau. Pour plus d'informations sur cette fonctionnalité, voir "Agent pour VMware - Sauvegarde sans réseau local" (p. 967).
- Moins de frais généraux de configuration. L'agent dédié sauvegarde les machines virtuelles au niveau de l'hyperviseur, indépendamment des systèmes d'exploitation invités.

De quel agent ai-je besoin ?

La sélection d'un agent dépend de ce que vous allez sauvegarder. Le tableau ci-dessous regroupe les informations qui vous aideront à faire votre choix.

Sous Windows, l'agent pour Exchange, l'agent pour SQL, l'agent pour Active Directory et l'agent pour Oracle nécessitent que l'agent pour Windows soit installé. Ainsi, si vous installez l'agent pour SQL, par exemple, vous pourrez également sauvegarder la totalité de la machine sur laquelle l'agent est installé.

Nous vous recommandons également d'installer l'agent pour Windows lorsque vous installez l'agent pour VMware (Windows) et l'agent pour Hyper-V.

Sous Linux, l'agent pour Oracle, l'agent pour MySQL/MariaDB, l'agent pour Virtuozzo et l'agent pour Proxmox nécessitent que l'agent pour Linux (64 bits) soit également installé. Ces agents sont inclus dans le fichier d'installation de l'agent pour Linux (64 bits).

Qu'allez-vous sauvegarder ?	Quel agent installer ?	Où dois-je l'installer ?
Machines physiques		
Machines physiques fonctionnant sous Windows	Agent pour Windows	Sur la machine qui sera sauvegardée.
Machines physiques fonctionnant sous Linux	Agent pour Linux	
Machines physiques fonctionnant sous macOS	Agent pour Mac	
Bases de données		
Bases de données SQL	Agent pour SQL	Sur une machine fonctionnant sous Microsoft SQL Server.

© Acronis International GmbH, 2003-2026

Bases de données MySQL	Agent pour MySQL/MariaDB (Inclus avec le fichier d'installation de l'agent pour Linux (64 bits))	Sur l'ordinateur exécutant MySQL Server.
Bases de données MariaDB	Agent pour MySQL/MariaDB (Inclus avec le fichier d'installation de l'agent pour Linux (64 bits))	Sur l'ordinateur exécutant MariaDB Server.
Bases de données Exchange	Agent pour Exchange	Sur une machine exécutant le rôle de boîte aux lettres de Microsoft Exchange Server.*
Base de données Oracle	Agent pour Oracle (Sous Linux, inclus avec le fichier d'installation de l'agent pour Linux (64 bits))	Sur la machine sous Oracle Database.
Ressources de cloud à cloud		
Boîtes aux lettres Microsoft 365 (Agent cloud ou agent local)	Agent cloud (Aucune installation n'est requise)	Cette fonctionnalité est disponible avec un agent cloud déployé dans le centre de données. Pour plus d'informations, voir "Comparaison des solutions de sauvegarde pour les données Microsoft 365" (p. 845).
	Agent pour Office 365	Sur un ordinateur Windows connecté à Internet. Pour plus d'informations, voir "Agent pour Office 365 installé localement" (p. 912).
Fichiers OneDrive et sites SharePoint Online Microsoft 365	Agent cloud (Aucune installation n'est requise)	Cette fonctionnalité est disponible avec un agent cloud déployé dans le centre de données. Pour plus d'informations, voir "Comparaison des solutions de sauvegarde pour les données Microsoft 365" (p.

© Acronis International GmbH, 2003-2026

		845).
Boîtes aux lettres Gmail Google Workspace, fichiers Google Drive, et fichiers de Drive partagés	Agent cloud (Aucune installation n'est requise)	Cette fonctionnalité est disponible avec un agent cloud déployé dans le centre de données. Pour plus d'informations, voir "Protection des données Google Workspace" (p. 917).
Active Directory		
Machines fonctionnant sous les services de domaine Active Directory	Agent pour Active Directory	Sur le contrôleur de domaine.
Machines virtuelles		
Machines virtuelles VMware ESXi (Broadcom)	Agent pour VMware (Windows)	Sur une machine sous Windows possédant un accès réseau au vCenter Server et au stockage de la machine virtuelle.**
	Agent pour VMware (appliance virtuelle)	Sur l'hôte ESXi.
Machines virtuelles Microsoft Hyper-V	Agent pour Hyper-V	Sur un hôte Hyper-V.
Machines virtuelles Scale Computing HyperCore	Agent pour Scale Computing HC3 (appliance virtuelle)	Sur l'hôte Scale Computing HyperCore.
Machines virtuelles Nutanix	Agent pour Nutanix AHV (appliance virtuelle)	Sur l'hôte Nutanix AHV.
Machines virtuelles Proxmox	Agent pour Proxmox (Inclus avec le fichier d'installation de l'agent pour Linux (64 bits))	Sur l'hôte Proxmox VE.
Machines virtuelles Red Hat Virtualization (gérées par oVirt)	Agent pour oVirt (appliance virtuelle)	Sur l'hôte Red Hat Virtualization
Machines virtuelles et conteneurs Virtuozzo Hybrid Server***	Agent pour Virtuozzo (Inclus avec le fichier d'installation de l'agent pour Linux (64 bits))	Sur l'hôte Virtuozzo Hybrid Server.
Machines virtuelles Virtuozzo Hybrid	Agent pour Virtuozzo	Sur l'hôte Virtuozzo Hybrid

© Acronis International GmbH, 2003-2026

Infrastructure	Hybrid Infrastructure (Appliance virtuelle)	Infrastructure.
Les machines virtuelles hébergées sur Amazon EC2	Comme pour les machines physiques****	Sur la machine qui sera sauvegardée.
Les machines virtuelles hébergées sur Windows Azure		
Machines virtuelles Citrix Hypervisor / XenServer		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Machines virtuelles basées sur un noyau (KVM), non gérées par oVirt		
Machines virtuelles Oracle, non gérées par oVirt		
Red Hat Virtualization (RHV/RHEV), gérées par oVirt	Agent pour oVirt (appliance virtuelle)	Sur l'hôte de virtualisation.
Machines virtuelles basées sur un noyau (KVM), gérées par oVirt		
Machines virtuelles Oracle, gérées par oVirt		
Stockage en réseau		
Synology	Agent pour Synology (appliance virtuelle)	Sur le terminal NAS.
Terminaux mobiles		
Terminaux mobiles sous Android	Application mobile pour Android	Sur le terminal mobile qui sera sauvegardé.
Terminaux mobiles sous iOS	Application mobile pour iOS	

*Lors de l'installation, l'agent pour Exchange vérifie que la machine sur laquelle il sera exécuté dispose de suffisamment d'espace libre. Lors de la restauration granulaire, un espace libre égal à 15 % de la plus grosse base de données Exchange est nécessaire de manière temporaire.

**Si votre ESXi utilise un stockage rattaché à un SAN, installez l'agent sur une machine connectée au même SAN. L'agent sauvegardera les machines virtuelles directement à partir du stockage plutôt que via l'hôte ESXi et le réseau local. Pour des instructions détaillées, voir "Agent pour VMware - Sauvegarde sans réseau local" (p. 967).

© Acronis International GmbH, 2003-2026

***Pour Virtuozzo 7, seuls les conteneurs ploop sont pris en charge. Les machines virtuelles ne sont pas prises en charge.

****Une machine est considérée comme étant virtuelle si elle est sauvegardée via un agent externe. Si l'agent est installé dans le système invité, les opérations de sauvegarde et de restauration sont les mêmes que pour une machine physique. Cependant, si Cyber Protection peut identifier une machine virtuelle en utilisant l'instruction CPUID, un quota de service de machine virtuelle lui est attribué.Si vous utilisez l'accès direct ou une autre option qui masque l'ID de fabricant du CPU, seuls des quotas de services pour les machines physiques peuvent être attribués.

Configuration système requise pour les agents

Agent	Espace disque requis pour l'installation
Agent pour Windows	1,2 Go
Agent pour Linux	2 Go
Agent pour Mac	1 Go
Agent pour SQL et Agent pour Windows	1,2 Go
Agent pour Exchange et Agent pour Windows	1,3 Go
Agent pour empêcher les pertes de données	500 Mo
Agent pour Microsoft 365	500 Mo
Agent pour Active Directory et Agent pour Windows	2 Go
Agent pour VMware et agent pour Windows	1,5 Go
Agent pour Hyper-V et agent pour Windows	1,5 Go
Agent pour Virtuozzo et agent pour Linux	1 Go
Agent pour Virtuozzo Hybrid Infrastructure	700 Mo
Agent pour Oracle et Agent pour Windows	2,2 Go
Agent pour Oracle et agent pour Linux	2 Go
Agent pour MySQL/MariaDB et agent pour Linux	2 Go

Nous recommandons que les agents de protection utilisent une mise en réseau avec une unité de transmission maximale (MTU) de 1500 octets. Tous les terminaux de cette mise en réseau doivent utiliser les mêmes paramètres de MTU.

© Acronis International GmbH, 2003-2026

Les opérations de sauvegarde, y compris leur suppression, nécessitent environ 1 Go de mémoire RAM par To de taille de sauvegarde. La consommation de mémoire varie en fonction du volume et du type des données traitées par les agents.

Remarque
L'utilisation de la mémoire vive peut augmenter lors de la sauvegarde d'archives de sauvegarde très volumineuses (4 To et plus).

Dans les systèmes x64, les opérations avec un support de démarrage et la restauration de disque avec redémarrage nécessitent au moins 1,5 Go de mémoire.

Sur les ressources dotées de processeurs modernes prenant en charge la technologie CET (tels que les Intel Core de 11e génération ou les AMD Ryzen 7), certaines fonctionnalités de l'agent pour la prévention des pertes de données (Data Loss Prevention) sont désactivées afin d'éviter les conflits. Le tableau suivant indique la disponibilité des fonctionnalités de contrôle des terminaux et de DLP sur les systèmes équipés de tels processeurs.

Fonctionnalités	Contrôle des terminaux	Prévention des pertes de données
Canaux locaux		
Stockage amovible	N/D	Oui
Stockage amovible chiffré	Oui	N/D
Imprimantes	N/D	Non
Lecteurs mappés redirigés	N/D	Oui
Presse-papiers redirigé	N/D	Non
Communications réseau		
E-mails SMTP	N/D	Oui
Microsoft Outlook (MAPI)	N/D	Oui
IBM Notes	N/D	Non
Messageries Web	N/D	Oui
Messagerie instantanée (ICQ)	N/D	Non
Messagerie instantanée (Viber)	N/D	Non
Messagerie instantanée (IRC, Jabber, Skype, Viber)	N/D	Oui
Services de partage de fichiers	N/D	Oui
Réseaux sociaux	N/D	Oui

© Acronis International GmbH, 2003-2026

Partage de fichiers sur réseau local (SMB)	N/D	Oui
Accès Web (HTTP/HTTPS)	N/D	Oui
Transferts de fichiers (FTP/FTPS)	N/D	Oui
Liste d'autorisation de transfert de données		
Liste d'autorisation des types de terminaux	N/D	Oui
Liste d'autorisation des communications réseau	N/D	Oui
Liste d'autorisation des hôtes distants	N/D	Oui
Liste d'autorisation des applications	N/D	Oui
Périphériques		
Stockage amovible	Oui	Oui
Stockage amovible chiffré	Oui	Oui
Imprimantes	Non	Non
Terminaux mobiles connectés par MTP	Non	Non
Adaptateurs Bluetooth	Oui	Oui
Lecteurs optiques	Oui	Oui
Disquettes	Oui	Oui
Presse-papiers Windows	Non	Non
Capture d'écran	Non	Non
Lecteurs mappés redirigés	Oui	Oui
Presse-papiers redirigé	Non	Non
Autoprotection d'agents Cyber Protect		
Protection des utilisateurs finaux standard	Oui	Oui
Protection des administrateurs système locaux	Oui	Oui

Téléchargement d'agents de protection

Avant d'installer un agent, vous devez télécharger son fichier d'installation depuis la console Cyber Protect.

Pour télécharger un agent lors de l'ajout d'une ressource à protéger

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. En haut à droite, cliquez sur **Ajouter un terminal**.
3. Dans le volet **Ajouter des terminaux**, à partir du menu déroulant **Canal de publication**, sélectionnez une version d'agent.
   - **Plus récente** – télécharger la version d'agent la plus récente disponible.
   - **Précédente version stable** – télécharger la version d'agent de la version précédente.
4. Sélectionnez l'agent correspondant au système d'exploitation de la ressource que vous ajoutez.
   La boîte de dialogue **Enregistrer sous** s'affiche.
5. [Uniquement pour les Mac équipés de processeurs Apple Silicon, tels que M1 et M2] Cliquez sur **Annuler**. Dans le panneau **Ajouter un ordinateur Mac** qui s'ouvre, cliquez sur **Télécharger l'installateur ARM**.
6. Sélectionnez un emplacement pour enregistrer le fichier d'agent d'installation et cliquez sur **Enregistrer**.

Pour télécharger un agent pour un usage ultérieur

1. Cliquez sur l'icône **Utilisateur** dans l'angle supérieur droit de la console Cyber Protect.
2. Cliquez sur **Téléchargements**.
3. Dans la boîte de dialogue **Téléchargements**, à partir du menu déroulant **Canal de publication**, sélectionnez une version d'agent.
   - **Plus récente** – télécharger la version d'agent la plus récente disponible.
   - **Précédente version stable** – télécharger la version d'agent de la version précédente.
4. Parcourez la liste des installateurs disponibles pour trouver l'installateur d'agent dont vous avez besoin et cliquez sur l'icône de téléchargement au bout de la ligne correspondante.
   La boîte de dialogue **Enregistrer sous** s'affiche.
5. Sélectionnez un emplacement pour enregistrer le fichier d'agent d'installation et cliquez sur **Enregistrer**.

Packages Linux requis pour l'installation d'agents dans Linux

Pour ajouter les modules nécessaires au noyau Linux, le programme d'installation de l'agent a besoin des paquets Linux suivants :

- Le paquet comprenant les sources et en-têtes du noyau. La version du paquet doit correspondre à celle de la version de noyau.
- Le système de compilation GNU Compiler Collection (GCC). La version du GCC doit être celle avec laquelle le noyau a été compilé.
- L'outil Make.
- L'interpréteur Perl.
- Les bibliothèques `libelf-dev`, `libelf-devel` ou `elfutils-libelf-devel` pour créer des noyaux à partir de 4.15 et configurées avec CONFIG_UNWINDER_ORC=y. Pour certaines distributions, comme Fedora 28, elles doivent être installées séparément des fichiers en-tête du noyau.

© Acronis International GmbH, 2003-2026

Les noms de ces paquets peuvent varier en fonction de votre distribution Linux.

Sous Red Hat Enterprise Linux, CentOS et Fedora, les paquets sont normalement installés par le programme d'installation. Dans d'autres distributions, vous devez installer les paquets s'ils ne sont pas installés ou ne possèdent pas de la version requise.

Est-ce que les paquets requis sont déjà installés ?

Pour vérifier si les paquets sont déjà installés, effectuez les étapes suivantes :

1. Exécutez la commande suivante pour déterminer la version de noyau et la version de GCC requise :

   ```
   cat /proc/version
   ```

   Cette commande renvoie des lignes similaires aux suivantes : `Linux version 2.6.35.6` et `gcc version 4.5.1`
2. Exécutez la commande suivante pour vérifier si l'outil Make et le compilateur GCC sont installés :

   ```
   make -v
   gcc -v
   ```

   Pour **gcc**, assurez-vous que la version renvoyée par la commande est la même que dans `gcc version` à l'étape 1. Pour **make**, assurez-vous simplement que la commande s'exécute.
3. Vérifiez si la version appropriée des paquets pour la génération des modules du noyau est installée :
   - Sous Red Hat Enterprise Linux, CentOS et Fedora, exécutez la commande suivante :

     ```
     yum list installed | grep kernel-devel
     ```
   - Sous Ubuntu, exécutez les commandes suivantes :

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   Dans un cas comme dans l'autre, assurez-vous que les versions des paquets sont les mêmes que dans `Linux version` à l'étape 1.
4. Exécutez les commandes suivantes afin de vérifier que l'interpréteur Perl est bien installé :

   ```
   perl --version
   ```

   Si les informations de la version de Perl s'affichent, cela signifie que l'interpréteur est installé.
5. Sous Red Hat Enterprise Linux, CentOS et Fedora, exécutez la commande suivante pour vérifier si `elfutils-libelf-devel` est installé :

   ```
   yum list installed | grep elfutils-libelf-devel
   ```


© Acronis International GmbH, 2003-2026

Si les informations de la version de la bibliothèque s'affichent, cela signifie que cette dernière est installée.

Installation des paquets à partir de la base de données de référentiel.

Le tableau suivant indique comment installer les paquets requis dans diverses distributions Linux.

Distribution Linux	Noms des paquets	Comment installer
Red Hat Enterprise Linux	**kernel-devel gcc make elfutils-libelf-devel**	Le programme d'installation téléchargera et installera les paquets automatiquement en utilisant votre abonnement Red Hat.
	perl	Exécuter la commande suivante : `yum install perl`
CentOS Fedora	**kernel-devel gcc make elfutils-libelf-devel**	Le programme d'installation téléchargera et installera les paquets automatiquement.
	perl	Exécuter la commande suivante : `yum install perl`

Ubuntu
Debian
	linux-headers linux-image gcc make perl	Exécutez les commandes suivantes :
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source gcc make perl	`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

© Acronis International GmbH, 2003-2026

Les paquets seront téléchargés à partir de la base de données de référentiel de la distribution et installés.

Pour les autres distributions Linux, consultez la documentation de la distribution pour connaître les noms exacts des packages requis et les méthodes d'installation.

Installation manuelle des paquets

Vous devrez peut-être installer les packages **manuellement** dans les cas suivants :

- La machine ne possède pas d'abonnement Red Hat actif ou ne dispose pas d'une connexion Internet.
- Le programme d'installation ne peut pas trouver les versions de **kernel-devel** ou **gcc** correspondant à la version de noyau ; Si la version disponible de **kernel-devel** est plus récente que votre noyau, vous devez soit mettre à jour le noyau ou installer la version correspondante de **kernel-devel** manuellement.
- Vous possédez les paquets requis sur le réseau local et ne voulez pas perdre de temps pour la recherche et le téléchargement automatique.

Obtenez les paquets à partir de votre réseau local ou depuis un site Web tiers auquel vous faites confiance, et installez-les de la façon suivante :

- Sous Red Hat Enterprise Linux, CentOS ou Fedora, exécutez la commande suivante en tant qu'utilisateur racine :

  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- Sous Ubuntu, exécutez la commande suivante :

  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Exemple : Installation manuelle des paquets sous Fedora 14

Suivez ces étapes pour installer les paquets requis dans Fedora 14 sur une machine 32 bits :

1. Exécutez la commande suivante pour déterminer la version de noyau et la version de GCC requise :

   ```
   cat /proc/version
   ```

   Les données de sortie de cette commande incluent les éléments suivants :

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Obtenez les paquets **kernel-devel** et **gcc** qui correspondent à cette version de noyau :

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```


© Acronis International GmbH, 2003-2026

3. Obtenez le paquet **make** pour Fedora 14 :

```
make-3.82-3.fc14.i686
```

4. Installez les paquets en exécutant les commandes suivantes en tant qu'utilisateur racine :

```
rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
rpm -ivh gcc-4.5.1.fc14.i686.rpm
rpm -ivh make-3.82-3.fc14.i686
```

   Vous pouvez spécifier tous ces paquets dans une seule commande `rpm`. L'installation de l'un de ces paquets peut nécessiter l'installation d'autres paquets supplémentaires pour résoudre les dépendances.

Configuration des paramètres de serveur proxy

Les agents de protection peuvent transférer des données via un serveur proxy HTTP/HTTPS. Le serveur doit passer par un tunnel HTTP sans analyser ou interférer avec le trafic HTTP. Les proxys intermédiaires ne sont pas pris en charge.

Puisque l'agent s'enregistre dans le cloud lors de l'installation, vous devez configurer les paramètres du serveur proxy lors de l'installation de l'agent ou à l'avance.

Pour Windows

Si un serveur proxy est configuré dans le **Panneau de configuration** > **Options Internet** > **Connexions**, le programme d'installation lit dans le registre les paramètres de serveur proxy et les utilise automatiquement.

Utilisez cette procédure si vous souhaitez effectuer les tâches suivantes.

- Configurez les paramètres de proxy avant l'installation de l'agent.
- Mettez à jour les paramètres de proxy après l'installation de l'agent.

Pour configurer les paramètres de proxy pendant l'installation de l'agent, voir "Installation des agents de protection sous Windows" (p. 64).

Remarque
Cette procédure n'est valable que lorsque le fichier `http-proxy.yaml` n'existe pas sur l'ordinateur. Si le fichier `http-proxy.yaml` existe sur l'ordinateur, vous devez mettre à jour les paramètres de proxy de ce fichier, car ils remplacent ceux du fichier `aakore.yaml`.

Le fichier `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` est créé lorsque vous configurez les paramètres du serveur proxy à l'aide de Cyber Protection Monitor. Pour plus d'informations, voir "Configuration des paramètres de serveur proxy dans Cyber Protect Monitor" (p. 375).

Pour ouvrir le fichier `http-proxy.yaml`, vous devez être membre du groupe Administrateurs dans Windows.

© Acronis International GmbH, 2003-2026

Pour configurer les paramètres de proxy

1. Créez un nouveau document texte et ouvrez-le dans un éditeur de texte comme le Bloc-notes.
2. Copiez et collez les lignes suivantes dans le fichier.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Remplacez `proxy.company.com` par votre adresse IP/nom d'hôte de serveur proxy et `000001bb` par la valeur hexadécimale du numéro de port. Par exemple, `000001bb` est le port 443.
4. Si votre serveur proxy nécessite une authentification, remplacez `proxy_login` et `proxy_password` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le document sous `proxy.reg`.
6. Exécutez le fichier en tant qu'administrateur.
7. Confirmez que vous souhaitez modifier le registre Windows.
8. Si l'agent n'est pas encore installé sur cette ressource, installez-le maintenant. Si l'agent est déjà installé sur la ressource, passez à l'étape suivante.
9. Ouvrez le fichier `%programdata%\Acronis\Agent\etc\aakore.yaml` dans un éditeur de texte.
   Pour ouvrir ce fichier, vous devez être membre du groupe Administrateurs dans Windows.
10. Localisez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
12. Dans le menu **Démarrer**, cliquez sur **Exécuter**, saisissez : **cmd**, puis cliquez sur **OK**.
13. Redémarrez le service aakore en exécutant les commandes suivantes.

```
net stop aakore
net start aakore
```

14. Redémarrez l'agent exécutant les commandes suivantes.

```
net stop mms
net start mms
```

Pour macOS

© Acronis International GmbH, 2003-2026

Utilisez cette procédure si vous souhaitez effectuer les tâches suivantes.

- Configurez les paramètres de proxy avant l'installation de l'agent.
- Mettez à jour les paramètres de proxy après l'installation de l'agent.

Pour configurer les paramètres de proxy pendant l'installation de l'agent, voir "Installation des agents de protection sous macOS" (p. 71).

Pour configurer les paramètres de proxy

1. Créez le fichier `/Library/Application Support/Acronis/Registry/Global.config` et ouvrez-le dans un éditeur de texte tel que TextEdit.
2. Copiez et collez les lignes suivantes dans le fichier.

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Remplacez `proxy.company.com` par votre adresse IP/nom d'hôte de serveur proxy et `443` par la valeur décimale du numéro de port.
4. Si votre serveur proxy nécessite une authentification, remplacez `proxy_login` et `proxy_password` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le fichier.
6. Si l'agent n'est pas encore installé sur cette ressource, installez-le maintenant. Si l'agent est déjà installé sur la ressource, passez à l'étape suivante.
7. Ouvrez le fichier `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` dans un éditeur de texte.
8. Localisez la section **env** ou créez-la, puis ajoutez-y les lignes suivantes.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
10. Rendez-vous dans **Applications** > **Utilitaires** > **Terminal**.
11. Redémarrez le service aakore en exécutant les commandes suivantes.

© Acronis International GmbH, 2003-2026

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. Redémarrez l'agent exécutant les commandes suivantes.

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

Pour Linux

Exécutez le fichier d'installation avec les paramètres `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD`. Utilisez la procédure suivante pour mettre à jour les paramètres de proxy après l'installation de l'agent de protection.

Pour configurer les paramètres de proxy

1. Ouvrez le fichier `/etc/Acronis/Global.config` dans un éditeur de texte.
2. Effectuez l'une des actions suivantes :
   - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, localisez la section suivante.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - Si les paramètres de proxy n'ont pas été spécifiés pendant l'installation de l'agent, copiez les lignes suivantes et collez-les dans le fichier, entre les balises `<registry name="Global">...</registry>`.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

3. Remplacez `ADDRESS` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.
4. Si votre serveur proxy nécessite une authentification, remplacez `LOGIN` et `PASSWORD` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le fichier.
6. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.

© Acronis International GmbH, 2003-2026

7. Localisez la section **env** ou créez-la et ajoutez les lignes suivantes :

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
9. Redémarrez le service aakore en exécutant la commande suivante.

```
sudo service aakore restart
```

10. Redémarrez l'agent en exécutant la commande d'exécution dans n'importe quel répertoire.

```
sudo service acronis_mms restart
```

Pour un support de démarrage

En cas d'utilisation d'un support de démarrage, vous pourriez avoir besoin d'accéder au stockage dans le cloud via un serveur proxy. Pour configurer les paramètres du serveur proxy, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez le nom d'hôte/l'adresse IP, le port et les identifiants du serveur proxy.

Installation dynamique des composants

Pour les ressources Windows protégées par l'agent version 15.0.26986 (publiée en mai 2021) ou versions ultérieures, les composants suivants sont installés de façon dynamique, c'est-à-dire uniquement lorsqu'ils sont requis par un plan de protection :

- Agent pour la protection contre les virus et les malwares et le Filtrage d'URL – requis pour la protection contre les virus et les malwares, ainsi que le Filtrage d'URL.
- Agent pour la prévention de la perte de données – requis pour le contrôle des terminaux.

Par défaut, ces composants ne sont pas installés. Le composant correspondant est automatiquement installé si une ressource devient protégée par un plan dans lequel le module **Protection contre les virus et les malwares** est activé.

Par défaut, ces composants ne sont pas installés. Le composant correspondant est automatiquement installé si une ressource devient protégée par un plan dans lequel l'un des modules suivants est activé :

- **Protection contre les virus et les malwares**
- **Filtrage d'URL**
- **Contrôle des terminaux**

De même, si aucun plan de protection n'exige la protection antimalware, le Filtrage d'URL ou le contrôle des terminaux, le composant correspondant est automatiquement désinstallé.

© Acronis International GmbH, 2003-2026

De même, si aucun plan de protection n'exige la protection antimalware, le composant correspondant est automatiquement désinstallé.

L'installation ou la désinstallation dynamique des composants peut prendre jusqu'à 10 minutes après l'application, la révocation, la modification ou la suppression d'un plan de protection. Si l'une des opérations suivantes est en cours, l'installation ou la désinstallation dynamique débutera une fois l'opération terminée :

- Sauvegarde
- Restauration
- Réplication de sauvegarde
- Réplication de machine virtuelle
- Test d'un réplica
- Exécution d'une machine virtuelle à partir d'une sauvegarde (y compris finalisation)
- Basculement pour reprise d'activité après sinistre
- Restauration automatique pour reprise d'activité après sinistre
- Exécution d'un script (pour la fonctionnalité de création de cyber-scripts)
- Installation des correctifs
- Sauvegarde de la configuration ESXi

Attribution des autorisations système requises à Agent Connect

Pour activer toutes les caractéristiques de la fonctionnalité Bureau à distance sur les ressources macOS, vous devez autoriser l'accès complet au disque et également affecter les autorisations suivantes à Agent Connect :

- **Enregistrement d'écran** : permet l'enregistrement d'écran de la ressource macOS via NEAR. Jusqu'à ce que cette autorisation soit accordée, toutes les connexions de contrôle à distance seront refusées.
- **Accessibilité** : permet d'établir des connexions à distance en mode de contrôle via NEAR.
- **Microphone** : permet la redirection du son d'une ressource macOS distante vers la ressource locale via NEAR. Pour activer la fonctionnalité de redirection du son, vous devez installer un pilote de capture de son sur la ressource. Pour plus d'informations, voir "Redirection du son à distance" (p. 1465).
- **Automatisation** : active l'action de vidage de la corbeille.
- **Services de localisation** : active les services de localisation sur l'emplacement. Tant que cette autorisation n'est pas accordée, l'agent ne peut pas suivre l'emplacement de la ressource.

Une fois l'agent démarré sur la ressource macOS, le système vérifie si cet agent dispose de ces droits et vous demande d'accorder les autorisations le cas échéant.

Pour accorder l'autorisation d'enregistrement de l'écran

© Acronis International GmbH, 2003-2026

1. Dans la zone **Octroi des autorisations système requises à l'agent Cyber Protect**, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez dans la ligne **Enregistrement d'écran** sur **Acquérir**.
3. Cliquez sur **Ouvrir Réglages système**.
4. Pour **Agent Connect**, activez le bouton bascule.

Si l'agent ne dispose pas de l'autorisation correspondante lorsque vous essayez d'accéder à distance à la ressource, une boîte de dialogue demandant l'autorisation d'enregistrement d'écran s'affiche. Seul l'utilisateur local peut répondre à cette demande.

Pour accorder l'autorisation d'accessibilité

1. Dans la zone **Octroi des autorisations système requises à l'agent Cyber Protect**, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez dans la ligne **Accessibilité** sur **Acquérir**.
3. Cliquez sur **Ouvrir Réglages système**.
4. Cliquez sur l'icône en forme de cadenas, en bas à gauche de la fenêtre, afin qu'elle change et affiche un cadenas déverrouillé. Pour que vous puissiez effectuer les modifications, le système vous demande un mot de passe d'administrateur.
5. Sélectionnez **Agent Connect**.

Pour accorder l'autorisation de microphone

1. Dans la zone **Octroi des autorisations système requises à l'agent Cyber Protect**, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez dans la ligne **Microphone** sur **Acquérir**.
3. Dans la fenêtre de confirmation, cliquez sur **Autoriser**.

Remarque
Pour permettre à l'agent d'utiliser l'autorisation donnée et de rediriger le son de la ressource, vous devez également installer un pilote de capture audio sur la ressource macOS. Pour plus d'informations, voir "Redirection du son à distance" (p. 1465).

Pour accorder l'autorisation d'automatisation

1. Dans la zone **Octroi des autorisations système requises à l'agent Agent Connect**, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez dans la ligne **Automatisation** sur **Acquérir**.
3. Dans la fenêtre de confirmation, cliquez sur **Autoriser**.

Pour accorder l'autorisation des services de localisation

© Acronis International GmbH, 2003-2026

1. Dans la zone **Octroi des autorisations système requises à l'agent Agent Connect**, cliquez sur **Configurer les autorisations système**.
2. Dans la boîte de dialogue **Autorisations système**, cliquez dans la ligne **Services de localisation**, cliquez sur **Acquérir**.
3. Dans la fenêtre de confirmation, cliquez sur **Autoriser**.

Mode compatible FIPS

Pour répondre aux exigences de conformité, vous pouvez installer et utiliser des agents de protection en mode compatible FIPS.

Ce mode utilise uniquement des algorithmes et des bibliothèques de cryptographies certifiés, conformément aux normes de traitement de l'information du Gouvernement fédéral des États-Unis (140-2), comme suit :

- [Windows] API de cryptographie Microsoft certifiée FIPS : Next Generation (CNG).
- [Linux] Bibliothèque BoringCrypto certifiée FIPS.
- [Windows et Linux] Module OpenSSL 3 certifié FIPS.

Le mode compatible FIPS est pris en charge par les agents suivants :

- Agent pour Windows (sur les systèmes d'exploitation 64 bits)
  Pour connaître les versions prises en charge, voir "Agent pour Windows" (p. 513).

  Remarque
  L'agent pour Windows (hérité) ne prend pas en charge le mode compatible FIPS.

- Agent pour Linux
  Pour connaître les versions prises en charge, voir "Agent pour Linux" (p. 518).
- Appliances virtuelles
  - Agent pour VMware (appliance virtuelle)
  - Agent pour Virtuozzo Hybrid Infrastructure
  - Agent pour Scale Computing HC3
  - Agent pour oVirt

Limites

- Les composants ou services suivants ne sont pas conformes à FIPS :
  - File Sync & Share
  - Endpoint Detection and Response (EDR)
  - Reprise d'activité après sinistre
  - Prévention des pertes de données (DLP)

© Acronis International GmbH, 2003-2026

  - Application Acronis Cyber Protect (sauvegarde de terminaux mobiles)
  - Envoi de données physiques
  - Console Web Restore
- Les appliances virtuelles en mode compatible FIPS ne prennent pas en charge les partages SMB.
- Le support de démarrage créé par l'agent pour Windows ou l'agent pour Linux compatible FIPS ne prend pas en charge les partages SMB.
- Vous ne pouvez sélectionner le mode FIPS pour l'agent pour Windows et l'agent pour Linux que pendant l'installation. Pour modifier le mode FIPS ultérieurement, réexécutez le fichier d'installation et modifiez l'installation.

Installation de l'agent pour Windows en mode compatible FIPS

Vous pouvez installer l'agent pour Windows en mode compatible FIPS en utilisant l'interface graphique ou l'interface en ligne de commande.

Prérequis

- Votre ressource dispose d'un système d'exploitation Windows 64 bits.
- Le système d'exploitation de la ressource fonctionne en mode FIPS.
  Pour plus d'informations, voir Cryptographie système : Utiliser des algorithmes conformes à la norme FIPS pour le chiffrement, le hachage et la signature dans la documentation Microsoft.
- Vous avez téléchargé le fichier d'installation pour l'Agent pour Windows.
  Pour plus d'informations, voir "Téléchargement d'agents de protection" (p. 47).

Pour installer l'agent pour Windows en mode compatible FIPS

Interface graphique

1. Sur l'ordinateur sur lequel vous souhaitez installer l'agent, exécutez l'invite de commandes en tant qu'administrateur.
2. Dans l'invite de commandes, accédez au fichier d'installation.
3. Pour exécuter la procédure d'installation en mode compatible FIPS et continuer dans l'interface graphique, exécutez la commande suivante :

   ```
   <file path>/<EXE file> --fips=enabled
   ```

   Par exemple :

   ```
   C:\Users\Administrator\Downloads\AgentForWindows_web.exe --fips=enabled
   ```

4. [Facultatif] Cliquez sur **Personnaliser les paramètres d'installation**, puis configurez les paramètres d'installation.
   Les options suivantes sont disponibles :
   - Modification des composants à installer (par exemple, désactivation de l'installation de Cyber Protect Monitor ou de l'outil de ligne de commande, ou installation de l'agent de protection

© Acronis International GmbH, 2003-2026

antimalware et du filtrage d'URL).

Remarque
Sur les ordinateurs Windows, les fonctionnalités de protection antimalware et de filtrage d'URL nécessitent l'installation de l'agent de protection antimalware et de filtrage d'URL. Cet agent est installé automatiquement pour les ressources protégées si les options **Protection antivirus et antimalware** ou **Filtrage d'URL** sont activées dans leurs plans de protection.

- Modification des composants à installer (par exemple, désactivation de l'installation de Cyber Protect Monitor ou de l'outil de ligne de commande, ou installation de l'agent pour la protection antimalware et du filtrage d'URL ou de la fonctionnalité SIEM Journal Forwarder).

Remarque
Sur les ordinateurs Windows, les fonctionnalités de protection antimalware et de filtrage d'URL nécessitent l'installation de l'agent de protection antimalware et de filtrage d'URL. Cet agent est installé automatiquement pour les ressources protégées si les options **Protection antivirus et antimalware** ou **Filtrage d'URL** sont activées dans leurs plans de protection.

- Modification de la méthode d'enregistrement de la ressource au sein du service Cyber Protection. Vous pouvez passer de l'option **Utiliser la console de service** (par défaut) à **Utiliser les identifiants** ou **Utiliser un jeton d'enregistrement**.
- Modification du chemin d'installation.
- Modification du compte utilisateur sous lequel le service de l'agent sera exécuté. Pour plus d'informations, voir "Changer le compte de connexion sur les machines Windows" (p. 66).
- Vérification ou modification du nom d'hôte ou de l'adresse IP d'un serveur proxy, du port, du nom d'utilisateur et du mot de passe pour y accéder.
  Le mot de passe peut inclure des caractères alphanumériques minuscules et majuscules, ainsi que les caractères spéciaux suivants :

```
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` } | { ~
```

Remarque
Si un serveur proxy est activé dans Windows, il est détecté et utilisé automatiquement.

5. Cliquez sur **Installer**.
6. [Lors de l'installation de l'agent pour VMware uniquement] Indiquez l'adresse et les identifiants de vCenter Server ou de l'hôte ESXi autonome dont vous souhaitez sauvegarder et restaurer les machines virtuelles, puis cliquez sur **Terminé**.
   Nous vous recommandons d'utiliser un compte dédié pour accéder à vCenter Server ou à l'hôte ESXi, plutôt que d'utiliser un compte existant avec le rôle d'administrateur. Pour plus d'informations, voir "Privilèges requis pour l'agent pour VMware" (p. 977).
7. [Lors d'une installation sur un contrôleur de domaine uniquement] Spécifiez le compte d'utilisateur depuis lequel l'agent sera exécuté, puis cliquez sur **Terminé**. Pour des raisons de

© Acronis International GmbH, 2003-2026

sécurité, le programme d'installation ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine.

Remarque
Le compte utilisateur que vous indiquez doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.

Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.

8. [Si vous avez sélectionné la méthode d'inscription par défaut **Utiliser la console de service**] Attendez l'affichage de l'écran d'inscription.
9. Enregistrez l'agent sous un compte utilisateur d'un tenant de client. Pour plus d'informations sur l'inscription, voir "Enregistrement des ressources à l'aide de l'interface utilisateur graphique" (p. 110).
10. [Si vous avez enregistré l'agent dans un tenant qui utilise le mode de conformité] Définissez le mot de passe de chiffrement.

Interface de ligne de commande

1. Sur l'ordinateur sur lequel vous souhaitez installer l'agent, exécutez l'invite de commandes en tant qu'administrateur.
2. Dans l'invite de commandes, accédez au fichier d'installation.
3. Exécuter la commande suivante :

```
<file path>/<EXE file> --fips=enabled <PARAMETER 1>=<value 1>...<PARAMETER N>=<value n>
```

Utilisez des espaces pour séparer les paramètres, ainsi que des virgules sans espace pour séparer les valeurs des paramètres. Par exemple :

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --fips=enabled --add-components=agentForWindows,commandLine --install-dir="C:\Program Files\BackupClient" --reg-address=https://eu2.company.cloud --reg-token=34F6-8C39-4A5C --quiet
```

Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 77).

Remarque
Pour installer les agents compatibles FIPS sur plusieurs ordinateurs, vous pouvez utiliser un fichier MSI créé par un agent compatible FIPS. Pour plus d'informations sur l'installation d'agents avec un fichier MSI, voir "Installation et désinstallation sans assistance à l'aide d'un fichier MSI" (p. 83).

© Acronis International GmbH, 2003-2026

Installation de l'agent pour Linux en mode compatible FIPS

Vous pouvez installer l'agent Linux en mode compatible FIPS en utilisant l'interface de ligne de commande.

Prérequis

- Vous avez téléchargé le package d'installation de l'agent pour Linux.

Pour installer l'agent pour Linux en mode compatible FIPS

1. Ouvrir l'application Terminal.
2. Effectuez l'une des actions suivantes :
   - Pour installer l'agent en précisant les paramètres dans la ligne de commande, exécutez la commande suivante :

     ```
     <package name> -a --fips-mode=1 <parameter 1> ... <parameter N>
     ```

     Ici, `<package name>` est le nom du package d'installation (fichier .i686 ou .x86_64). Tous les paramètres disponibles et leurs valeurs sont décrits dans "Paramètres d'installation ou de désinstallation sans assistance" (p. 95).
   - Pour installer l'agent avec les paramètres indiqués dans un fichier texte séparé, exécutez la commande suivante :

     ```
     <package name> -a --fips-mode=1 --options-file=<path to the file>
     ```

     Cette approche peut s'avérer utile si vous ne souhaitez pas saisir d'informations sensibles sur la ligne de commande. Dans ce cas, vous pouvez spécifier les paramètres de configuration dans un fichier texte séparé et vous assurer que vous êtes le seul à pouvoir y accéder. Placez chaque paramètre sur une nouvelle ligne, suivi de la valeur de ce paramètre. Par exemple :

     ```
     --rain=https://company.cloud
     --login=johndoe
     --password=johnspassword
     --auto
     ```

     ou

     ```
     -C
     https://company.cloud
     -g
     johndoe
     -w
     johnspassword
     -a
     --language
     en
     ```


© Acronis International GmbH, 2003-2026

Si le même paramètre est indiqué dans la ligne de commande et dans le fichier texte, la valeur de la ligne de commande le précède.

3. Si UEFI Secure Boot est activé sur l'ordinateur, vous êtes invité à redémarrer le système après l'installation. Lorsque vous êtes invité à saisir un mot de passe, utilisez le mot de passe de l'utilisateur root. Si ce mot de passe n'est pas accepté, utilisez le mot « acronis » comme mot de passe. Au redémarrage du système, choisissez la gestion MOK (Machine Owner Key), sélectionnez **Enroll MOK**, puis inscrivez la clé en utilisant le mot de passe recommandé.
   Si vous activez UEFI Secure Boot après l'installation de l'agent, répétez l'installation en incluant l'étape 3. Sinon, les sauvegardes échoueront.

Activation du mode compatible FIPS pour une appliance virtuelle

Vous pouvez activer le mode compatible FIPS dans la console de l'appliance.

Prérequis

- Une appliance virtuelle est déployée et configurée.

Pour activer le mode FIPS sur une appliance virtuelle

1. Connectez-vous à l'interface de l'hyperviseur en tant qu'administrateur.
2. Ouvrez la console de l'appliance virtuelle.
3. Dans l'interface de ligne de commande, exécutez la commande suivante :

```
fips-mode-setup --enable
```

L'appliance virtuelle redémarre. Après son redémarrage, elle fonctionne en mode compatible FIPS.

Installation des agents de protection à l'aide de l'interface utilisateur graphique

Installation des agents de protection sous Windows

Prérequis

- Un fichier de programme d'installation de l'agent de protection est téléchargé sur la ressource que vous souhaitez protéger. Voir "Téléchargement d'agents de protection" (p. 47).
- La ressource que vous souhaitez protéger est connectée à Internet.

Pour installer l'agent pour Windows

1. Sur la ressource que vous souhaitez protéger, connectez-vous en tant qu'administrateur, puis ouvrez le fichier du programme d'installation.
2. [Facultatif] Cliquez sur **Personnaliser les paramètres d'installation**, puis configurez les paramètres d'installation.
   Les options suivantes sont disponibles :

© Acronis International GmbH, 2003-2026

- Modification des composants à installer (par exemple, désactivation de l'installation de Cyber Protect Monitor ou de l'outil de ligne de commande, ou installation de l'agent de protection antimalware et du filtrage d'URL).

  Remarque
  Sur les ordinateurs Windows, les fonctionnalités de protection antimalware et de filtrage d'URL nécessitent l'installation de l'agent de protection antimalware et de filtrage d'URL. Cet agent est installé automatiquement pour les ressources protégées si les options **Protection antivirus et antimalware** ou **Filtrage d'URL** sont activées dans leurs plans de protection.

- Modification des composants à installer (par exemple, désactivation de l'installation de Cyber Protect Monitor ou de l'outil de ligne de commande, ou installation de l'agent pour la protection antimalware et du filtrage d'URL ou de la fonctionnalité SIEM Journal Forwarder).

  Remarque
  Sur les ordinateurs Windows, les fonctionnalités de protection antimalware et de filtrage d'URL nécessitent l'installation de l'agent de protection antimalware et de filtrage d'URL. Cet agent est installé automatiquement pour les ressources protégées si les options **Protection antivirus et antimalware** ou **Filtrage d'URL** sont activées dans leurs plans de protection.

- Modification de la méthode d'enregistrement de la ressource au sein du service Cyber Protection. Vous pouvez passer de l'option **Utiliser la console de service** (par défaut) à **Utiliser les identifiants** ou **Utiliser un jeton d'enregistrement**.
- Modification du chemin d'installation.
- Modification du compte utilisateur sous lequel le service de l'agent sera exécuté. Pour plus d'informations, voir "Changer le compte de connexion sur les machines Windows" (p. 66).
- Vérification ou modification du nom d'hôte ou de l'adresse IP d'un serveur proxy, du port, du nom d'utilisateur et du mot de passe pour y accéder.

  Le mot de passe peut inclure des caractères alphanumériques minuscules et majuscules, ainsi que les caractères spéciaux suivants :

  ```
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` } | { ~
  ```

  Remarque
  Si un serveur proxy est activé dans Windows, il est détecté et utilisé automatiquement.

3. Cliquez sur **Installer**.
4. [Lors de l'installation de l'agent pour VMware uniquement] Indiquez l'adresse et les identifiants de vCenter Server ou de l'hôte ESXi autonome dont vous souhaitez sauvegarder et restaurer les machines virtuelles, puis cliquez sur **Terminé**.

   Nous vous recommandons d'utiliser un compte dédié pour accéder à vCenter Server ou à l'hôte ESXi, plutôt que d'utiliser un compte existant avec le rôle d'administrateur. Pour plus d'informations, voir "Privilèges requis pour l'agent pour VMware" (p. 977).

© Acronis International GmbH, 2003-2026

5. [Lors d'une installation sur un contrôleur de domaine uniquement] Spécifiez le compte d'utilisateur depuis lequel l'agent sera exécuté, puis cliquez sur **Terminé**. Pour des raisons de sécurité, le programme d'installation ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine.

   Remarque
   Le compte utilisateur que vous indiquez doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.

   Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.
6. [Si vous avez sélectionné la méthode d'inscription par défaut **Utiliser la console de service**] Attendez l'affichage de l'écran d'inscription.
7. Enregistrez l'agent sous un compte utilisateur d'un tenant de client. Pour plus d'informations sur l'inscription, voir "Enregistrement des ressources à l'aide de l'interface utilisateur graphique" (p. 110).
8. [Si vous avez enregistré l'agent dans un tenant qui utilise le mode de conformité] Définissez le mot de passe de chiffrement.

Changer le compte de connexion sur les machines Windows

Dans l'onglet **Sélectionner des composants de l'agent**, définissez le compte sous lequel les services seront exécutés en indiquant **Compte de connexion pour le service de l'agent**. Vous pouvez sélectionner l'une des options suivantes :

- **Utiliser des comptes d'utilisateur du service** (par défaut pour l'agent de service)
  Les comptes d'utilisateur du service sont des comptes système Windows utilisés pour exécuter des services. Ce paramètre présente l'avantage suivant : les politiques de sécurité du domaine n'affectent pas les droits d'utilisateur de ces comptes. Par défaut, l'agent est exécuté sous le compte **Système Local**.
- **Créer un nouveau compte**
  Le nom de compte pour l'agent sera Agent User.
- **Utiliser le compte suivant**
  Si vous installez l'agent sur un contrôleur de domaine, le système vous invite à spécifier des comptes existants (ou le même compte) pour l'agent. Pour des raisons de sécurité, le système ne crée pas automatiquement de nouveaux comptes sur un contrôleur de domaine.
  Le compte utilisateur que vous indiquez lorsque le programme d'installation est exécuté sur un contrôleur de domaine doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.
  Voir aussi "Utilisation de comptes gMSA avec l'agent Cyber Protection" (p. 68).
  Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.

© Acronis International GmbH, 2003-2026

Remarque
Si vous choisissez de **Créer un nouveau compte** ou choisissez l'option **Utiliser le compte suivant**, assurez-vous que les politiques de sécurité du domaine n'affectent pas les droits d'utilisateur des comptes liés. Si un compte est privé des droits d'utilisateur attribués lors de l'installation, le composant pourrait ne pas fonctionner correctement ou ne pas fonctionner.

Important
Nous ne recommandons pas de modifier manuellement le compte de connexion une fois l'installation terminée.

Privilèges requis pour le compte de connexion

L'agent Cyber Protection pour Windows s'exécute en tant que service de machine gérée (Managed Machine Service, MMS) sur les machines Windows protégées. Le compte sous lequel l'agent s'exécutera doit disposer de droits spécifiques pour fonctionner correctement. Le compte utilisateur MMS doit être configuré comme suit :

1. Inclus dans les groupes **Opérateurs de sauvegarde** et **Administrateurs**. Sur un contrôleur de domaine, l'utilisateur doit être inclus dans le groupe **Domaine Admins**.
2. Accordez l'autorisation **Contrôle total** sur le dossier `%PROGRAMDATA%\Acronis` et sur ses sous-dossiers.
   Pour Windows XP et Server 2003, les autorisations doivent être accordées sur le dossier `%ALLUSERSPROFILE%\Application Data\Acronis` et ses sous-dossiers.
3. Dispose de la permission **Contrôle complet** sur certaines clés de registre pour la clé suivante : `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Dispose des droits d'utilisateur suivants :
   - Connexion en tant que service
   - Ajuster les quotas de mémoire pour un processus
   - Remplacer un jeton de niveau processus
   - Modifier les valeurs d'environnement du firmware

Comment attribuer les droits d'utilisateur

Suivez les instructions ci-dessous pour attribuer les droits d'utilisateur (cet exemple utilise le droit d'utilisateur **Connexion en tant que service**, la procédure est la même que pour les autres droits d'utilisateur) :

1. Connectez-vous à l'ordinateur en utilisant un compte avec des privilèges d'administration.
2. Dans le **Panneau de configuration** Windows, ouvrez **Outils d'administration**, puis ouvrez **Règle de sécurité locale**.
3. Développez **Stratégies locales** et cliquez sur **Attribution des droits utilisateur.**
4. Dans le volet de droite, cliquez avec le bouton droit sur **Ouverture de session en tant que service**, puis sélectionnez **Propriétés**.

© Acronis International GmbH, 2003-2026

5. Cliquez sur le bouton **Ajouter un utilisateur ou un groupe...** pour ajouter un nouvel utilisateur.
6. Dans la fenêtre **Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes**, recherchez le compte auquel vous souhaitez affecter ce privilège, puis cliquez sur **OK**.
7. Dans **Propriétés de l'ouverture de session en tant que service**, cliquez sur **OK** pour enregistrer les modifications.

Important
Assurez-vous que l'utilisateur que vous avez ajouté au droit d'utilisateur **Connexion en tant que service** n'est pas répertorié dans la stratégie **Refuser la connexion en tant que service** sous **Stratégie de sécurité locale**.

Utilisation de comptes gMSA avec l'agent Cyber Protection

Les comptes de service gérés de groupe (gMSA) peuvent être utilisés pour exécuter des services sur plusieurs serveurs sans avoir à gérer le mot de passe.

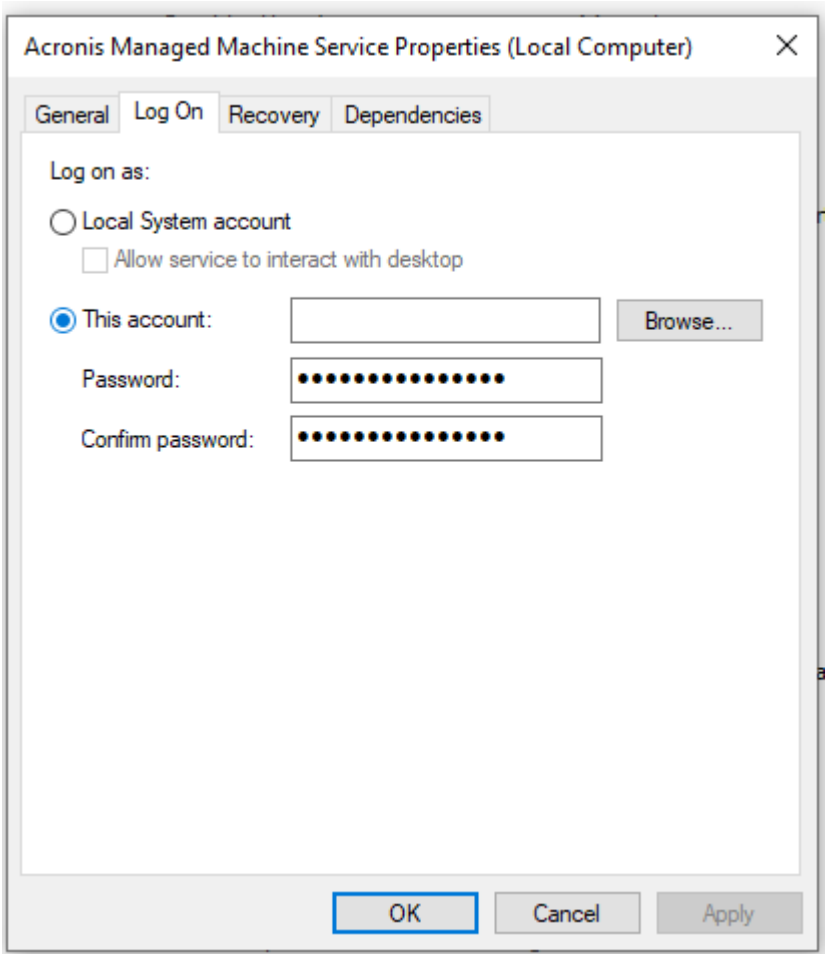
La procédure suivante s'applique si vous souhaitez modifier le compte utilisateur utilisé par l'agent Acronis Cyber Protection après l'installation, afin que l'agent puisse utiliser un gMSA.

Important
Tous les plans de protection précédemment affectés à l'ordinateur sur lequel vous modifiez le compte de connexion cesseront de fonctionner et vous devrez les révoquer et les réappliquer après avoir modifié le compte.

Pour activer l'utilisation d'un gMSA pour l'agent Cyber Protection

1. Créez un gMSA en suivant la procédure standard décrite dans la base de connaissances Microsoft.
2. Configurez le gMSA comme décrit dans la section "Privilèges requis pour le compte de connexion" (p. 67).
3. Affectez le gMSA comme compte de connexion pour le service MMS sur l'ordinateur où l'agent s'exécute.
   a. Ouvrez le menu Démarrer de Windows et entrez `services.msc` pour ouvrir la liste des services locaux.
   b. Cliquez avec le bouton droit sur **Acronis Managed Machine Service** et cliquez sur **Propriétés**.
   c. Dans l'onglet **Connexion**, sélectionnez **Ce compte**, puis cliquez sur **Parcourir** pour trouver le gMSA que vous souhaitez utiliser.

© Acronis International GmbH, 2003-2026



d. Cliquez sur **OK**.

4. Appliquez les plans de protection selon les besoins.
   - Si vous aviez des plans de protection appliqués à l'ordinateur avant de changer le compte de connexion, révoquez ces plans et réappliquez-les.
   - Si vous n'aviez pas de plans de protection appliqués à l'ordinateur, créez-en de nouveaux ou sélectionnez des plans existants et appliquez-les.

Installation des agents de protection sous Linux

Vous pouvez installer l'agent pour Linux en exécutant son fichier d'installation sur une machine locale.

Prérequis

- Vous avez téléchargé le fichier du programme d'installation pour l'agent pour Linux. Voir "Téléchargement d'agents de protection" (p. 47).

  Le programme d'installation 64 bits contient des agents supplémentaires, tels que l'agent pour Virtuozzo, l'agent pour Oracle, l'agent pour MySQL/MariaDB et l'agent pour Proxmox. Ces agents dépendent de l'agent pour Linux et sont installés avec lui.
- Vous avez installé les packages Linux requis.

© Acronis International GmbH, 2003-2026

- Au moins 2 Go d'espace disque libre sont disponibles sur l'ordinateur sur lequel vous souhaitez installer l'agent.
- Lors de l'installation de l'agent sous SUSE Linux, assurez-vous d'utiliser `su -` au lieu de `sudo`. Sinon, l'erreur suivante se produit lorsque vous tentez d'enregistrer l'agent via la console Cyber Protect : « Échec du lancement du navigateur web. Aucun affichage disponible ». Certaines distributions Linux, telles que SUSE, ne transmettent pas la variable DISPLAY lors de l'utilisation de `sudo`, et l'installateur ne peut pas ouvrir le navigateur dans l'interface graphique (GUI).

Limites

- Certaines distributions Linux n'autorisent pas l'installation de packages signés avec SHA-1. Dans ce cas, l'installation échoue avec le message suivant : « Impossible de trouver le package Agent de sauvegarde et de restauration ». Pour plus d'informations sur la façon de résoudre ce problème, voir cet article de la base de connaissances.

Pour installer l'agent pour Linux

1. Assurez-vous que la machine est connectée à Internet.
2. En tant qu'utilisateur root (superutilisateur), accédez au répertoire dans lequel est stocké le fichier d'installation, définissez-le comme fichier exécutable, puis exécutez-le.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

   Si un serveur proxy est activé sur votre réseau, lorsque vous exécutez le fichier d'installation, spécifiez le nom d'hôte/l'adresse IP et le port du serveur au format suivant : `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD`.

   Si vous souhaitez modifier la méthode par défaut d'enregistrement de la machine dans le service Cyber Protection, exécutez le fichier d'installation avec l'un des paramètres suivants :
   - `--register-with-credentials` : pour demander un nom d'utilisateur et un mot de passe lors de l'installation
   - `--token=STRING` : pour utiliser un jeton d'enregistrement
   - `--skip-registration` : pour ignorer l'enregistrement
3. Sélectionnez les cases à cocher correspondant aux agents que vous souhaitez installer. Les agents suivants sont disponibles dans le package d'installation 64 bits :
   - Agent pour Linux
   - Agent pour Virtuozzo
   - Agent pour Oracle
   - Agent pour MySQL/MariaDB
   - Agent pour Proxmox

© Acronis International GmbH, 2003-2026

4. Si vous avez conservé la méthode d'enregistrement par défaut à l'étape 2, passez à l'étape suivante. Sinon, saisissez le nom d'utilisateur et le mot de passe du service Cyber Protection, ou attendez que la machine soit enregistrée à l'aide du jeton.
5. Enregistrez l'agent sous un compte utilisateur d'un tenant de client. Pour plus d'informations sur l'inscription, voir "Enregistrement des ressources à l'aide de l'interface utilisateur graphique" (p. 110).
6. [Si vous avez enregistré l'agent dans un tenant qui utilise le mode de conformité] Définissez le mot de passe de chiffrement.
7. Si UEFI Secure Boot est activé sur l'ordinateur, vous êtes informé que vous devez redémarrer le système après l'installation. Lorsque vous êtes invité à saisir un mot de passe, utilisez le mot de passe de l'utilisateur root. Si ce mot de passe n'est pas accepté, utilisez le mot « acronis » comme mot de passe.

   Remarque
   L'installation génère une nouvelle clé utilisée pour la signature des modules noyau. Vous devez inscrire cette nouvelle clé dans la liste MOK (Machine Owner Key) en redémarrant l'ordinateur. Sans l'inscription de cette clé, votre agent ne sera pas opérationnel. Si vous activez UEFI Secure Boot après l'installation de l'agent, vous devez réinstaller l'agent.

8. Une fois l'installation terminée, effectuez l'une des actions suivantes :
   - Cliquez sur **Redémarrer**, si vous avez été invité à redémarrer le système à l'étape précédente. Lors du redémarrage du système, choisissez la gestion de clé MOK (Machine Owner Key), sélectionnez **Enroll MOK**, puis inscrivez la clé à l'aide du mot de passe recommandé à l'étape précédente.
   - Sinon, cliquez sur **Quitter**.

Les informations concernant le dépannage sont fournies dans le fichier :
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Installation des agents de protection sous macOS

Prérequis

- Un fichier de programme d'installation de l'agent de protection est téléchargé sur la ressource que vous souhaitez protéger. Voir "Téléchargement d'agents de protection" (p. 47).
- La ressource que vous souhaitez protéger est connectée à Internet.

Pour installer l'agent pour Mac (x64 ou ARM64)

1. Assurez-vous que la machine est connectée à Internet.
2. Double-cliquez sur le fichier d'installation (.dmg).
3. Patientez pendant que le système d'exploitation monte l'image du disque d'installation.
4. Double-cliquez sur **Installer**.

© Acronis International GmbH, 2003-2026

5. Si un serveur proxy est activé dans votre réseau, cliquez sur **Agent de protection** dans la barre de menu, puis sur **Paramètres de serveur proxy**. Spécifiez ensuite l'adresse IP/nom de l'hôte, le port et les informations d'identification de serveur proxy.
6. Si vous y êtes invité, fournissez les informations d'identification de l'administrateur.
7. Cliquez sur **Continuer**.
8. Attendez l'apparition de l'écran d'enregistrement.
9. Enregistrez l'agent sous un compte utilisateur d'un tenant de client. Pour plus d'informations sur l'inscription, voir "Enregistrement des ressources à l'aide de l'interface utilisateur graphique" (p. 110).
10. [Si vous avez enregistré l'agent dans un tenant qui utilise le mode de conformité] Définissez le mot de passe de chiffrement.
11. Si votre version de macOS est Mojave 10.14.x ou une version supérieure, accordez un accès complet au disque à l'agent de protection pour permettre les opérations de sauvegarde.
    Pour les instructions, consultez l'article Grant the 'Full Disk Access' permission to the Cyber Protection agent (64657).
12. Pour utiliser la fonctionnalité Bureau à distance, accordez les autorisations système requises à Agent Connect. Pour plus d'informations, voir "Attribution des autorisations système requises à Agent Connect" (p. 57).

Désinstallation d'agents

Lorsque vous désinstallez un agent d'une ressource, cette ressource est supprimée automatiquement de la console Cyber Protect. Si la ressource reste affichée après que vous avez désinstallé l'agent, en raison d'un problème réseau, par exemple, supprimez cette ressource manuellement de la console. Pour en savoir plus sur la procédure à suivre, reportez-vous à "Suppression de ressources de la console Cyber Protect" (p. 403).

Remarque
La désinstallation d'un agent ne supprime aucun plan ni sauvegarde.

Pour désinstaller un agent

Windows

Remarque
[Pour les plans de protection créés après novembre 2024] La désinstallation et la modification des agents de protection pour Windows sont interdites par défaut. L'agent pour Windows peut être modifié uniquement pendant une fenêtre de maintenance ou via la fonctionnalité de mise à jour automatique de l'agent. Pour obtenir des instructions sur l'autorisation de la désinstallation ou la modification ponctuelle d'un agent, voir "Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée" (p. 208). Pour désactiver la protection de désinstallation de l'agent, voir "Pour désactiver la protection contre la désinstallation de l'agent" (p. 209).

© Acronis International GmbH, 2003-2026

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent.
2. Dans le **Panneau de configuration**, accédez à **Programmes et fonctionnalités** (**Ajout ou suppression de programmes** sous Windows XP).
3. Cliquez avec le bouton droit sur **Acronis Cyber Protect**, puis sélectionnez **Désinstaller**.
4. [Pour les agents protégés par mot de passe] Spécifiez le mot de passe dont vous avez besoin pour désinstaller l'agent, puis cliquez sur **Suivant**.
5. [Facultatif] Cochez la case **Supprimer les journaux et les paramètres de configuration**.
   Ne cochez pas cette case si vous prévoyez de réinstaller le produit ultérieurement. Si vous cochez cette case, puis réinstallez l'agent, cette ressource pourrait être dupliquée dans la console Cyber Protect et ses anciennes sauvegardes risqueraient de ne pas lui être associée.
6. Cliquez sur **Désinstaller**.

Linux

1. Sur l'ordinateur avec l'agent, exécutez `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` en tant qu'utilisateur root.
2. [Facultatif] Cochez la case **Nettoyer toutes traces de produit (supprimer les paramètres de configuration, d'emplacements de stockage, de tâches, de journaux des produits)**.
   Ne cochez pas cette case si vous prévoyez de réinstaller le produit ultérieurement. Si vous cochez cette case, puis réinstallez l'agent, cette ressource pourrait être dupliquée dans la console Cyber Protect et ses anciennes sauvegardes risqueraient de ne pas lui être associée.
3. Confirmez votre choix.

macOS

1. Sur l'ordinateur avec l'agent, double-cliquez sur le fichier .dmg d'installation.
2. Patientez jusqu'à ce que le système d'exploitation monte l'image du disque d'installation.
3. Dans l'image, double-cliquez sur **Désinstaller**.
4. Si vous y êtes invité, fournissez les informations d'identification de l'administrateur.
5. Confirmez votre choix.

Pour désinstaller les composants fournis avec l'agent pour Windows

Vous pouvez désinstaller des composants fournis avec l'agent pour Windows tels que Cyber Protect Monitor, l'agent pour la prévention des pertes de données ou Bootable Media Builder sans désinstaller l'agent pour Windows.

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent.
2. Exécutez le programme d'installation, puis cliquez sur **Modifier les composants installés**.
3. Désélectionnez les cases situées à côté des composants que vous souhaitez désinstaller, puis cliquez sur **Terminé**.

Pour supprimer l'agent pour VMware (appliance virtuelle)

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. [Si l'appliance virtuelle est sous tension] Cliquez avec le bouton droit sur l'appliance virtuelle, puis cliquez sur **Alimentation** > **Mise hors tension**. Confirmez votre choix.
3. [Si l'appliance virtuelle utilise un stockage attaché localement sur un disque virtuel et que vous souhaitiez conserver les données sur ce disque] Supprimez le stockage virtuel de l'appliance virtuelle.
   a. Cliquez avec le bouton droit de la souris sur l'appliance virtuelle, puis cliquez sur **Modifier les paramètres**.
   b. Sélectionnez le disque avec le stockage, puis cliquez sur **Supprimer**.
   c. Sous **Options de suppression**, cliquez sur **Supprimer de la machine virtuelle**.
   d. Cliquez sur **OK**.

   En conséquence, le disque reste dans la banque de données. Vous pouvez attacher le disque à un autre appliance virtuelle.
4. Cliquez avec le bouton droit de la souris sur l'appliance virtuelle, puis cliquez sur **Supprimer du disque**. Confirmez votre choix.
5. [Facultatif] [Si vous n'envisagez pas de réutiliser cette appliance] Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Emplacements**, puis supprimez l'emplacement correspondant au stockage attaché localement.

Installation et désinstallation d'agents de protection à l'aide de l'interface de ligne de commande

Installation et désinstallation d'agents de protection sous Windows

Dans Windows, vous pouvez effectuer une installation ou une désinstallation sans assistance en procédant comme suit :

- En utilisant le fichier EXE du programme d'installation et en indiquant les paramètres d'installation dans la ligne de commande.
- En utilisant un fichier MSI que vous extrayez du programme d'installation et en indiquant les paramètres d'installation de l'une des manières suivantes :
  - Dans un fichier MST
  - Directement dans la ligne de commande

Installation et désinstallation sans assistance à l'aide d'un fichier EXE

Pour ce type d'installation sans assistance, téléchargez le programme d'installation, puis démarrez-le à partir de la ligne de commande avec les paramètres d'installation requis. Pour afficher les paramètres que vous pouvez utiliser, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 77).

Vous n'avez pas besoin d'extraire à l'avance les packages d'installation et les fichiers MSI et MST.

 © Acronis International GmbH, 2003-2026

Installation et désinstallation des agents et des composants (EXE)

Pour effectuer une installation sans assistance avec un fichier EXE, exécutez le programme d'installation et spécifiez les paramètres d'installation dans la ligne de commande.

Pour télécharger le Pour télécharger le programme d'installation, cliquez dans la console Cyber Protect sur l'icône de compte en haut à droite, puis sur **Téléchargements**. Le lien de téléchargement est également disponible dans le panneau **Ajouter des terminaux**.

Pour installer les agents et les composants

1. Démarrez l'interface de ligne de commande en tant qu'administrateur, puis accédez au fichier EXE du programme d'installation.
2. Pour démarrer le programme d'installation et spécifier les paramètres d'installation, exécutez la commande suivante :

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Utilisez des espaces pour séparer les paramètres, ainsi que des virgules sans espace pour séparer les valeurs des paramètres. Par exemple :

   ```
   C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
   components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
   Files\BackupClient" --reg-address=https://eu2.company.cloud --reg-token=34F6-8C39-
   4A5C --quiet
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 77).

Exemples

- Installation de l'agent pour Windows, de l'agent de protection antimalware et de filtrage d'URL, de l'outil de ligne de commande et de Cyber Protect Monitor. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un nom d'utilisateur et d'un mot de passe.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --agent-account=system --reg-
  address=https://company.cloud --reg-login=johndoe --reg-password=johnspassword
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Création d'un compte de connexion pour le service de l'agent dans Windows. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un jeton.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
  Files\BackupClient" --agent-account=new --reg-address=https://eu2.company.cloud --
  reg-token=34F6-8C39-4A5C
  ```


© Acronis International GmbH, 2003-2026

- Installation de l'agent pour Windows, de l'outil de ligne de commande, de l'agent pour Oracle et de Cyber Protect Monitor. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un nom d'utilisateur et d'un mot de passe.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
address=https://company.cloud --reg-login=johndoe --reg-password=johnspassword
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Définition de la langue de l'interface utilisateur sur Allemand. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un jeton. Définir un proxy HTTP.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
address=https://eu2.company.cloud --reg-token=34F6-8C39-4A5C --http-proxy-
address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
password=tomspassword
```

Pour supprimer un composant installé

1. Lancez l'interface de ligne de commande en tant qu'administrateur, puis accédez à `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Exécuter la commande suivante :

```
web_installer.exe --remove-components=<value 1>,<value 2> --quiet
```

Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 77).

Exemple

- Désinstallation de Cyber Protect Monitor.

```
C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-
components=trayMonitor --quiet
```

Pour désinstaller un agent

1. Lancez l'interface de ligne de commande en tant qu'administrateur, puis accédez à `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Exécuter la commande suivante :

```
Uninstaller.exe --quiet --delete-all-settings
```

Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (EXE)" (p. 77).

© Acronis International GmbH, 2003-2026

Exemples

- Désinstallation de l'agent pour Windows et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --
delete-all-settings
```

- Désinstallation d'un agent pour Windows protégé par mot de passe et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-
tamper-password=<password> --quiet --delete-all-settings
```

Paramètres d'une installation sans assistance (EXE)

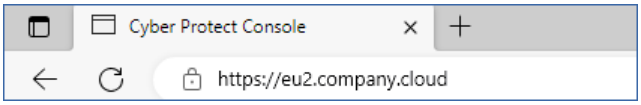
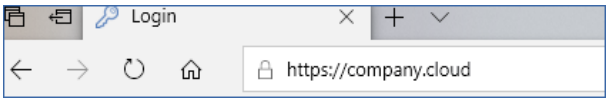
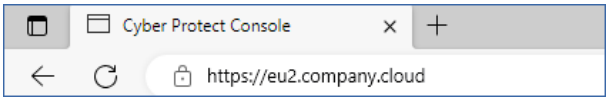
Le tableau suivant récapitule les paramètres de l'installation sans assistance avec un fichier EXE.

Paramètres	Description
Paramètres généraux	
`--add-components=`<component1,component2,...,componentN>	Les composants à installer. Vous trouverez la liste complète des composants disponibles dans "Composants d'une installation sans assistance (EXE)" (p. 82). Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. Si vous spécifiez des composants déjà installés, ces composants sont réparés ou mis à jour, selon leur version et celle du programme d'installation. Si vous ne spécifiez pas ce paramètre, un ensemble de composants sera installé, selon l'ordinateur sur lequel vous effectuez l'installation. Par exemple, l'agent pour SQL n'est installé que sur les ordinateurs qui exécutent MS SQL Server.
`--install-dir=`<path>	Dossier dans lequel les composants sélectionnés seront installés. Si le dossier spécifié n'existe pas, il sera créé. Si vous ne spécifiez pas ce paramètre, un dossier par défaut est utilisé : `C:\Program Files\BackupClient`.
`--log-dir=`<path>	Le dossier dans lequel les journaux d'installation seront enregistrés. Si vous ne spécifiez pas ce paramètre, un dossier par

© Acronis International GmbH, 2003-2026

Paramètres	Description
	défaut est utilisé : `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<code>	La langue du produit. Les valeurs suivantes sont disponibles : en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Si vous ne spécifiez pas ce paramètre et que le langage système de l'ordinateur sur lequel vous effectuez l'installation figure dans la liste ci-dessus, le langage système est utilisé. Dans tous les autres cas, la valeur est définie sur en.
`--quiet`	Utilisez ce paramètre pour exécuter le programme d'installation sans afficher l'interface graphique. Ne l'utilisez pas avec le paramètre `--register-only`.
`--help`	Utilisez ce paramètre pour voir la liste de tous les paramètres disponibles que vous pouvez utiliser dans la ligne de commande et dans leurs descriptions.
`--fss-onboarding-auto-start`	Utilisez ce paramètre avec le paramètre `--quiet` pour afficher l'assistant d'intégration File Sync & Share après une installation sans assistance.
`--fips={enabled | disabled}`	Utilisez ce paramètre avec la valeur `enabled` pour installer l'agent en mode compatible FIPS.
Paramètres d'enregistrement	
`--registration={skip | by-credentials | by-token | device-flow}`	Utilisez ce paramètre pour choisir le mode d'inscription de l'agent après l'installation. Pour passer l'enregistrement, spécifiez `skip`. Vous pouvez enregistrer l'agent ultérieurement à l'aide du paramètre `--register-only`. Pour enregistrer l'agent à l'aide d'identifiants, spécifiez `by-credentials`, puis utilisez les paramètres `--reg-login` et `--reg-password`. De la même manière, vous pouvez également utiliser uniquement les paramètres `--reg-login` et `--reg-password` ; dans ce cas, la spécification de `--registration=by-credentials` est facultative. Pour enregistrer l'agent avec un jeton d'enregistrement, spécifiez `by-token`, puis utilisez le paramètre `--reg-token`. De la même manière, vous pouvez utiliser uniquement le paramètre `--reg-token` ; dans ce cas, la spécification de -

© Acronis International GmbH, 2003-2026

Paramètres	Description
	`-registration=by-token` est facultative. Pour enregistrer l'agent à l'aide du protocole OAuth 2.0, spécifiez `device-flow`. Une fois l'installation terminée, la page d'inscription s'ouvre automatiquement. Lorsque vous utilisez `--registration=device-flow`, spécifiez l'adresse exacte du centre de données comme valeur du paramètre `--reg-address`. Il s'agit de l'URL que vous voyez après vous être connecté au service Cyber Protection. Par exemple, `https://eu2.company.cloud`.  N'utilisez pas `--registration=device-flow` avec le paramètre `--quiet`.
`--reg-address=`<url>	L'URL du service Cyber Protection. Vous pouvez utiliser ce paramètre avec les paramètres `--reg-login` et `--reg-password`, ou avec le paramètre `--reg-token`. • Lorsque vous l'utilisez avec les paramètres `--reg-login` et `--reg-password`, indiquez l'adresse que vous utilisez pour vous connecter au service Cyber Protection. Par exemple, `https://company.cloud` :  • Lorsque vous l'utilisez avec le paramètre `--reg-token`, spécifiez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez après vous être connecté au service Cyber Protection. Par exemple, `https://eu2.company.cloud`.  N'utilisez pas `https://company.cloud` avec le paramètre `--reg-token`.
`--reg-login=`<login> `--reg-password=`<password>	Les identifiants du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire. Lorsque vous utilisez ces paramètres, la spécification du paramètre `--registration` est facultative. N'utilisez pas ces paramètres avec le paramètre `--reg-token`.

© Acronis International GmbH, 2003-2026

Paramètres	Description
`--reg-token=`<token>	Le jeton d'enregistrement. Le jeton d'enregistrement est une série de 12 caractères, séparés en trois segments par des traits d'union. Pour plus d'informations sur sa génération, voir "Génération d'un jeton d'enregistrement" (p. 112). Lorsque vous utilisez ce paramètre, la spécification du paramètre `--registration` est facultative. N'utilisez pas ce paramètre avec les paramètres `--reg-login` et `--reg-password`.
`--register-only`	Utilisez ce paramètre pour ignorer l'installation et enregistrer l'agent à l'aide du protocole OAuth 2.0 (device-flow). Une fois l'installation terminée, la page d'inscription s'ouvre automatiquement. N'utilisez pas `--register-only` avec le paramètre `--quiet`.
Compte d'ouverture de session pour le service de l'agent	
`--agent-account={system | new | custom}` ou `--agent-account-login=`<login> `--agent-account-password=`<password>	Utilisez ce paramètre pour indiquer le compte de connexion sous lequel le service de l'agent sera exécuté. Pour plus d'informations sur les comptes de connexion, voir "Changer le compte de connexion sur les machines Windows" (p. 66). Pour utiliser le compte **Système local**, spécifiez `--agent-account=system` ou n'utilisez pas le paramètre `--agent-account` dans votre commande. Pour que le service de l'agent s'exécute sous un nouveau compte de connexion, **Acronis Agent User**, qui est créé automatiquement, spécifiez `new`. Pour que le service de l'agent s'exécute sous un compte existant, spécifiez les identifiants de ce compte à l'aide des paramètres `--agent-account-login` et `--agent-account-password`. Dans ce cas, la spécification du paramètre `--agent-account=custom` est facultative.
Paramètres vCenter/ESXi	
`--esxi-address=`<host>	Le nom d'hôte ou l'adresse IP de vCenter Server ou de l'hôte ESXi. Utilisez ce paramètres lorsque vous installez l'agent pour VMware.

© Acronis International GmbH, 2003-2026

Paramètres	Description
`--esxi-login=`<login> `--esxi-password=`<password>	Les identifiants d'accès à vCenter Server ou à l'hôte ESXi. Utilisez ces paramètres lorsque vous installez l'agent pour VMware.
Paramètres du proxy	
`--http-proxy={none | system | custom}`	Utilisez ce paramètre pour spécifier le serveur proxy HTTP que vous souhaitez utiliser pour la sauvegarde vers le stockage Cloud et pour la restauration à partir de ce stockage. Si vous désactivez les connexions du serveur proxy, spécifiez `--http-proxy=none`. Pour utiliser un serveur proxy à l'échelle du système, spécifiez `--http-proxy=system` ou n'utilisez pas le paramètre `--http-proxy` dans votre commande. Pour utiliser un autre serveur proxy, spécifiez l'adresse du serveur proxy et les identifiants à l'aide des paramètres `--http-proxy-address`, `--http-proxy-login` et `--http-proxy-password`. Dans ce cas, la spécification du paramètre `--http-proxy=custom` est facultative.
`--http-proxy-address=`<host>:<port>	Le nom d'hôte ou l'adresse IP, ainsi que le port du serveur proxy HTTP personnalisé.
`--http-proxy-login=`<login>	Identifiant du serveur proxy HTTP personnalisé.
`--http-proxy-password=`<password>	Mot de passe du serveur proxy HTTP personnalisé.
Paramètres de désinstallation	
`--remove-components=`<component1,component2,...,componentN>	Les composants à désinstaller. Vous trouverez la liste complète des composants disponibles dans "Composants d'une installation sans assistance (EXE)" (p. 82). Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. **Important** En utilisant ce paramètre, vous pouvez désinstaller uniquement les composants. Pour désinstaller le produit complètement, accédez au Panneau de configuration de Windows > Programmes et fonctionnalités, sélectionnez le produit, puis cliquez sur **Désinstaller**.

© Acronis International GmbH, 2003-2026

Paramètres	Description
`--delete-all-settings`	Utilisez ce paramètre facultatif lorsque vous utilisez le paramètre `--remove-components` pour supprimer tous les journaux du produit, les tâches et les paramètres de configuration.
`--anti-tamper-password=`<password>	Le mot de passe requis pour désinstaller un Agent pour Windows protégé par mot de passe ou modifier ses composants.

Composants d'une installation sans assistance (EXE)

Le tableau ci-dessous récapitule les composants que vous pouvez utiliser pour une installation sans assistance par l'intermédiaire d'un fichier EXE. Utilisez les noms de valeurs afin de spécifier des valeurs pour le paramètre `--add-components`.

Pour plus d'informations, voir "Paramètres d'une installation sans assistance (EXE)" (p. 77).

Nom de la valeur	Description du composant
`agentForWindows`	Agent pour Windows
`agentForSas`	Agent pour Files Sync & Share
`agentForAd`	Agent pour Active Directory
`agentForAmp`	Agent de protection antimalware et de filtrage d'URL
`agentForDlp`	Agent pour empêcher les pertes de données
`agentForEsx`	Agent pour VMware (Windows)
`agentForExchange`	Agent pour Exchange
`agentForHyperV`	Agent pour Hyper-V
`agentForOffice365`	Agent pour Office 365
`agentForOracle`	Agent pour Oracle
`agentForSql`	Agent pour SQL
`commandLine`	Outil de ligne de commande
`mediaBuilder`	Bootable Media Builder
`trayMonitor`	Cyber Protect Monitor
`all`	Cette valeur associe tous les composants.
`allAgents`	Cette valeur associe tous les agents.

© Acronis International GmbH, 2003-2026

Installation et désinstallation sans assistance à l'aide d'un fichier MSI

Pour ce type d'installation sans assistance, utilisez le programme d'installation Windows (programme `Msiexec`). Extrayez les packages d'installation et le fichier MSI à l'avance à l'aide de l'interface graphique du programme d'installation.

Lorsque vous installez les composants avec un fichier MSI, vous pouvez utiliser un fichier de transformation MST pour personnaliser les paramètres d'installation. Pour en savoir plus sur l'utilisation de la combinaison des fichiers MSI et MST, reportez-vous à "Installation des agents et des composants (combinaison MSI et MST)" (p. 84). Vous pouvez utiliser cette méthode d'installation dans un domaine Active Directory pour installer les agents de protection à l'aide de la stratégie de groupe Windows. Pour plus d'informations, voir "Déploiement d'agents de protection via la stratégie de groupe" (p. 135).

Vous pouvez également spécifier les paramètres d'installation manuellement dans la ligne de commande. Dans ce cas, vous n'avez pas besoin de fichier MST. Pour plus d'informations, voir "Exemples" (p. 85).

Extraction des fichiers MSI, MST et CAB

Extrayez les fichiers MSI, MST et CAB avec les packages d'installation en exécutant l'interface graphique du programme d'installation.

Pour extraire les fichiers MSI, MST et CAB

1. Exécutez l'interface graphique du programme d'installation, puis cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
2. Dans **Que faut-il installer**, sélectionnez les composants que vous souhaitez installer, puis cliquez sur **Terminé**.

   Remarque
   Lors de la modification d'une installation existante, sélectionnez les composants déjà installés et ceux que vous souhaitez ajouter.

   Les packages d'installation de ces composants seront extraits du programme d'installation sous forme de fichiers CAB.
3. Dans **Paramètres d'enregistrement**, sélectionnez **Utiliser les informations d'identification** ou **Utiliser un jeton d'enregistrement**. Selon votre choix, spécifiez les identifiants ou le jeton d'enregistrement, puis cliquez sur **Terminé**.

   Pour plus d'informations sur la génération d'un jeton d'enregistrement, voir "Génération d'un jeton d'enregistrement" (p. 112).
4. [Lors d'une installation sur un contrôleur de domaine uniquement] Dans **Compte d'ouverture de session pour le service de l'agent**, sélectionnez **Utiliser le compte suivant**. Spécifiez le compte utilisateur depuis lequel le service de l'agent sera exécuté, puis cliquez sur **Terminé**. Pour des raisons de sécurité, le programme d'installation ne crée pas automatiquement de

© Acronis International GmbH, 2003-2026

nouveaux comptes sur un contrôleur de domaine.

Remarque
Le compte utilisateur que vous indiquez doit disposer du droit `Se connecter en tant que service`. Ce compte doit avoir déjà été utilisé dans le contrôleur de domaine pour que son dossier de profil soit créé sur cet ordinateur.

Pour plus d'informations sur l'installation de l'agent sur un contrôleur de domaine en lecture seule, consultez cet article de la base de connaissances.

5. Vérifiez ou modifiez les autres paramètres d'installation qui seront ajoutés au fichier MST, puis cliquez sur **Poursuivre**.
6. Sélectionnez le dossier dans lequel les fichiers MSI, MST et CAB seront extraits, puis cliquez sur **Générer**.

Installation des agents et des composants (combinaison MSI et MST)

Utilisez le fichier MST pour personnaliser le paramètre d'installation du fichier MSI. Utilisez la combinaison de fichiers MSI et MST lorsque vous installez des agents sur plusieurs ordinateurs par l'intermédiaire d'une stratégie de groupe Windows. Pour plus d'informations, voir "Déploiement d'agents de protection via la stratégie de groupe" (p. 135).

Pour installer des composants avec des fichiers MSI et MST

1. Extrayez les fichiers MSI et MST en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 83).
2. Dans l'interface de ligne de commande de l'ordinateur sur lequel vous souhaitez installer des composants, exécutez la commande suivante :

```
msiexec /i <MSI file> TRANSFORMS=<MST file>
```

Par exemple :

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

Installation et désinstallation d'agents et de composants (MSI et sélection directe)

Exécutez le fichier MSI, sélectionnez manuellement les composants à installer, puis spécifiez leurs paramètres d'installation dans la ligne de commande. Dans ce cas, vous n'avez pas besoin du fichier MST.

Pour installer les agents et les composants

1. Extrayez le fichier MSI et les packages d'installation (fichiers CAB) en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 83).

   Pour cette méthode d'installation, vous n'avez besoin que des fichiers MSI et CAB. Vous n'avez pas besoin du fichier MST.
2. Dans l'interface de ligne de commande de la machine, exécutez la commande suivante :

© Acronis International GmbH, 2003-2026

```
msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Utilisez des espaces pour séparer les paramètres, ainsi que des virgules sans espace pour séparer les valeurs des paramètres. Par exemple :

```
msiexec.exe /i BackupClient64.msi
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_
ADDRESS=https://eu2.company.cloud REGISTRATION_TOKEN=34F6-8C39-4A5C
```

Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (MSI)" (p. 87).

Exemples

- Installation de l'agent pour Windows, de l'agent de protection antimalware et de filtrage d'URL, de l'outil de ligne de commande et de Cyber Protect Monitor. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un nom d'utilisateur et d'un mot de passe.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
  Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
  SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://company.cloud REGISTRATION_
  LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Création d'un compte de connexion pour le service de l'agent dans Windows. Enregistrement de la ressource dans le service Cyber Protection à l'aide d'un jeton.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
  ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2.company.cloud REGISTRATION_TOKEN=34F6-
  8C39-4A5C
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande, de l'agent pour Oracle et de Cyber Protect Monitor. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un nom d'utilisateur et encodé dans un mot de passe base64. Vous devrez peut-être encoder votre mot de passe s'il contient des caractères spéciaux ou des espaces vides. Pour plus d'informations sur l'encodage d'un mot de passe, voir "Utilisation de mots de passe comportant des caractères spéciaux ou des espaces vides" (p. 116).

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
  rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
  LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://company.cloud
  REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
  ```


© Acronis International GmbH, 2003-2026

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Enregistrement de la machine dans le service Cyber Protection à l'aide d'un jeton. Définir un proxy HTTP.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2.company.cloud REGISTRATION_
TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com HTTP_PROXY_
PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

Pour supprimer un composant installé

1. Extrayez le fichier MSI et les packages d'installation (fichiers CAB) en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 83).

   Pour cette méthode d'installation, vous n'avez besoin que des fichiers MSI et CAB. Vous n'avez pas besoin du fichier MST.
2. Dans l'interface de ligne de commande de la machine, exécutez la commande suivante :

   ```
   msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (MSI)" (p. 87).

Exemple

- Suppression de Cyber Protect Monitor.

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

Pour désinstaller un agent

1. Extrayez le fichier MSI et les packages d'installation (fichiers CAB) en suivant les indications de "Extraction des fichiers MSI, MST et CAB" (p. 83).

   Pour cette méthode d'installation, vous n'avez besoin que des fichiers MSI et CAB. Vous n'avez pas besoin du fichier MST.
2. Dans l'interface de ligne de commande de la machine, exécutez la commande suivante :

   ```
   msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
   REBOOT=ReallySuppress /qn
   ```

   Pour connaître les paramètres disponibles et leurs valeurs, reportez-vous à "Paramètres d'une installation sans assistance (MSI)" (p. 87).

© Acronis International GmbH, 2003-2026

Exemples

- Désinstallation de l'agent pour Windows et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- Désinstallation d'un agent pour Windows protégé par mot de passe et de tous ses composants. Suppression de tous les journaux, tâches et paramètres de configuration.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

Paramètres d'une installation sans assistance (MSI)

Le tableau suivant récapitule les paramètres de l'installation sans assistance lorsque vous utilisez un fichier MSI.

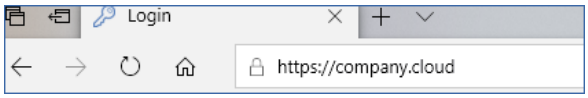
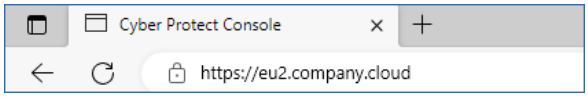
Vous pouvez également utiliser d'autres paramètres `msiexec`. Par exemple, utilisez la commande `/qn` pour empêcher l'affichage des éléments de l'interface utilisateur graphique. Pour en savoir plus sur les paramètres `msiexec`, consultez la documentation Microsoft.

Paramètres	Description
Paramètres généraux	
`ADDLOCAL=` <component1,component2,...,componentN>	Les composants à installer. Vous trouverez la liste complète des composants disponibles dans "Composants d'une installation sans assistance (MSI)" (p. 91). Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. **Remarque** Vous devez extraire les fichiers d'installation de tous les composants que vous souhaitez installer. Pour plus d'informations sur l'extraction, voir "Extraction des fichiers MSI, MST et CAB" (p. 83).
`TARGETDIR=`<path>	Dossier dans lequel les composants sélectionnés seront installés. Si le dossier spécifié n'existe pas, il sera créé. Si vous ne spécifiez pas ce paramètre, un dossier par défaut est utilisé : `C:\Program Files\BackupClient`.

© Acronis International GmbH, 2003-2026

Paramètres	Description
REBOOT=ReallySuppress	Spécifiez ce paramètre si vous souhaitez installer des composants sans redémarrer l'ordinateur.
/l*v <log file>	Spécifiez ce paramètre pour enregistrer un journal détaillé. Ce journal est nécessaire si vous souhaitez enquêter sur des problèmes d'installation.
CURRENT_LANGUAGE=<language ID>	La langue du produit. Les valeurs suivantes sont disponibles : en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Si vous ne spécifiez pas ce paramètre et que le langage système de l'ordinateur sur lequel vous effectuez l'installation figure dans la liste ci-dessus, le langage système est utilisé. Dans tous les autres cas, la valeur est définie sur en.
SKIP_SHA2_KB_CHECK={0,1}	Utilisez ce paramètre pour soit vérifier, soit ignorer la vérification de l'installation de la mise à jour Microsoft pour le support de signature de code SHA2 (KB4474419) sur un ordinateur. La vérification ne s'exécute que sur les systèmes d'exploitation qui nécessitent cette mise à jour. Pour voir si elle est requise pour votre système d'exploitation, voir "Systèmes d'exploitation et environnements pris en charge pour la sauvegarde et la restauration" (p. 513). Pour ignorer la vérification, définissez la valeur du paramètre à 1. Si vous n'indiquez pas ce paramètre ou définissez sa valeur sur 0, et si la mise à jour de la prise en charge de la signature du code SHA2 est introuvable sur l'ordinateur, l'installation échoue.
FSS_ONBOARDING_AUTO_START={0,1}	Utilisez ce paramètre avec la valeur définie sur 1 pour afficher l'assistant d'intégration File Sync & Share après une installation sans assistance. Si vous n'indiquez pas ce paramètre ou définissez sa valeur sur 0, l'assistant d'intégration ne s'affiche pas.
ENABLE_FIPS_COMPLIANCE_MODE={0,1}	Utilisez ce paramètre avec la valeur définie sur 1 pour installer l'agent en mode compatible FIPS.
Paramètres d'enregistrement	
REGISTRATION_ADDRESS	L'URL du service Cyber Protection. Vous pouvez utiliser

© Acronis International GmbH, 2003-2026

Paramètres	Description
	ce paramètre avec les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`, ou avec `REGISTRATION_TOKEN`. • Lorsque vous l'utilisez avec les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`, indiquez l'adresse que vous utilisez pour vous connecter au service Cyber Protection. Par exemple, `https://company.cloud` :  • Lorsque vous l'utilisez avec le paramètre `REGISTRATION_TOKEN`, spécifiez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez après vous être connecté au service Cyber Protection. Par exemple, `https://eu2.company.cloud`.  N'utilisez pas `https://company.cloud` avec le paramètre `REGISTRATION_TOKEN`.
`REGISTRATION_LOGIN` `REGISTRATION_PASSWORD`	Les identifiants du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire. N'utilisez pas ces paramètres avec le paramètre `REGISTRATION_TOKEN`.
`REGISTRATION_PASSWORD_ENCODED`	Le mot de passe du compte sous lequel l'agent sera enregistré dans le service Cyber Protection, encodé en base64. Pour plus d'informations sur l'encodage de votre mot de passe, voir "Utilisation de mots de passe comportant des caractères spéciaux ou des espaces vides" (p. 116).
`REGISTRATION_TOKEN`	Le jeton d'enregistrement. Le jeton d'enregistrement est une série de 12 caractères, séparés en trois segments par des traits d'union. Pour plus d'informations sur sa génération, voir "Génération d'un jeton d'enregistrement" (p. 112). N'utilisez pas ce paramètre avec les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`.
`REGISTRATION_REQUIRED={0,1}`	Utilisez ce paramètre pour choisir les événements qui se produisent en cas d'échec de l'inscription.

© Acronis International GmbH, 2003-2026

Paramètres	Description
	Si vous définissez la valeur sur `1`, l'installation échoue également. Si vous définissez la valeur sur `0` ou ne spécifiez pas le paramètre, l'installation se déroule correctement, même si l'inscription échoue.
Compte d'ouverture de session pour le service de l'agent	
`MMS_USE_SYSTEM_ACCOUNT={0,1}`	Utilisez ce paramètre avec la valeur `1` pour que le service s'exécute sous le compte de connexion **Système local**. Pour plus d'informations sur les comptes de connexion, voir "Changer le compte de connexion sur les machines Windows" (p. 66).
`MMS_CREATE_NEW_ACCOUNT={0,1}`	Utilisez ce paramètre avec la valeur `1` pour que le service de l'agent s'exécute sous le nouveau compte de connexion **Acronis Agent User** qui est créé automatiquement.
`MMS_SERVICE_USERNAME=`<user name> `MMS_SERVICE_PASSWORD=`<password>	Utilisez ces paramètres pour indiquer un compte de connexion existant sous lequel le service de l'agent sera exécuté.
Paramètres vCenter/ESXi	
`SET_ESX_SERVER={0,1}`	Utilisez ce paramètres lorsque vous installez l'agent pour VMware. Si vous définissez la valeur sur `0`, l'agent pour VMware ne sera pas connecté à vCenter Server ou à un hôte ESXi. Si vous définissez la valeur sur `1`, spécifiez les paramètres suivants : `ESX_HOST`, `EXI_USER`, `ESX_PASSWORD`.
`ESX_HOST=`<host name>	Le nom d'hôte ou l'adresse IP de vCenter Server ou de l'hôte ESXi.
`ESX_USER=`<user name> `ESX_PASSWORD=`<password>	Les identifiants d'accès à vCenter Server ou à l'hôte ESXi.
Paramètres du proxy	
`HTTP_PROXY_ADDRESS=`<IP address> `HTTP_PROXY_PORT=`<port>	Utilisez ces paramètres pour indiquer le serveur proxy HTTP que l'agent utilisera. Si vous n'utilisez pas de serveur proxy, ne spécifiez pas ces paramètres.

© Acronis International GmbH, 2003-2026

Paramètres	Description
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	Les accréditations pour le serveur proxy HTTP. Utilisez ces paramètres si le serveur proxy exige une authentification.
Paramètres de désinstallation	
REMOVE={<component1,component2,...,componentN>|ALL}	Les composants à désinstaller. Lorsque vous spécifiez plusieurs composants, séparez-les par des virgules. N'ajoutez pas d'espaces avant ou après la virgule. Pour supprimer tous les composants de produit, définissez la valeur sur ALL.
DELETE_ALL_SETTINGS={0,1}	Pour supprimer tous les journaux du produit, les tâches et les paramètres de configuration, définissez la valeur sur 1. Utilisez ce paramètre facultatif lorsque vous utilisez le paramètre REMOVE.
ANTI_TAMPER_PASSWORD=<password>	Le mot de passe requis pour désinstaller un Agent pour Windows protégé par mot de passe ou modifier ses composants.

Composants d'une installation sans assistance (MSI)

Le tableau ci-dessous récapitule les composants que vous pouvez utiliser pour une installation sans assistance à l'aide d'un fichier MSI. Utilisez les noms de valeurs pour spécifier les valeurs du paramètre ADDLOCAL.

Pour plus d'informations, voir "Paramètres d'une installation sans assistance (MSI)" (p. 87).

Nom de la valeur	Description du composant	Doit être installé avec	Nombre de bits
AgentFeature	Composants clés pour les agents		32 bits/64 bits
MmsMspComponents	Composants clés pour la sauvegarde	AgentFeature	32 bits/64 bits
BackupAndRecoveryAgent	Agent pour Windows	MmsMspComponents	32 bits/64 bits
AmpAgentFeature	Agent for Antimalware	BackupAndRecoveryAgent	32 bits/64 bits

© Acronis International GmbH, 2003-2026

	protection and URL filtering		
DlpAgentFeature	Agent pour empêcher les pertes de données	BackupAndRecoveryAgent	32 bits/64 bits
SasAgentFeature	Agent pour File Sync & Share	TrayMonitor	32 bits/64 bits
ArxAgentFeature	Agent pour Exchange	MmsMspComponents	32 bits/64 bits
ArsAgentFeature	Agent pour SQL	BackupAndRecoveryAgent	32 bits/64 bits
ARADAgentFeature	Agent pour Active Directory	BackupAndRecoveryAgent	32 bits/64 bits
ArxOnlineAgentFeature	Agent pour Microsoft 365	MmsMspComponents	32 bits/64 bits
OracleAgentFeature	Agent pour Oracle	BackupAndRecoveryAgent	32 bits/64 bits
AcronisESXSupport	Agent pour VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64 bits
HyperVAgent	Agent pour Hyper-V	BackupAndRecoveryAgent	32 bits/64 bits
CommandLineTool	Outil de ligne de commande		32 bits/64 bits
TrayMonitor	Cyber Protect Monitor	AgentFeature	32 bits/64 bits
BackupAndRecoveryBootableComponents	Bootable Media Builder		32 bits/64 bits

Installation et désinstallation d'agents de protection sous Linux

Cette section décrit l'installation ou la désinstallation d'agents de protection sans assistance sur une machine sous Linux via la ligne de commande.

Prérequis

- Vous avez téléchargé le fichier du programme d'installation pour l'agent pour Linux. Voir "Téléchargement d'agents de protection" (p. 47).

© Acronis International GmbH, 2003-2026

Le programme d'installation 64 bits contient des agents supplémentaires, tels que l'agent pour Virtuozzo, l'agent pour Oracle, l'agent pour MySQL/MariaDB et l'agent pour Proxmox. Ces agents dépendent de l'agent pour Linux et sont installés avec lui.

- Vous avez installé les packages Linux requis.
- Au moins 2 Go d'espace disque libre sont disponibles sur l'ordinateur sur lequel vous souhaitez installer l'agent.
- Lors de l'installation de l'agent sous SUSE Linux, assurez-vous d'utiliser `su -` au lieu de `sudo`. Sinon, l'erreur suivante se produit lorsque vous tentez d'enregistrer l'agent via la console Cyber Protect : « Échec du lancement du navigateur web. Aucun affichage disponible ». Certaines distributions Linux, telles que SUSE, ne transmettent pas la variable DISPLAY lors de l'utilisation de `sudo`, et l'installateur ne peut pas ouvrir le navigateur dans l'interface graphique (GUI).

Limites

- Certaines distributions Linux n'autorisent pas l'installation de packages signés avec SHA-1. Dans ce cas, l'installation échoue avec le message suivant : « Impossible de trouver le package Agent de sauvegarde et de restauration ». Pour plus d'informations sur la façon de résoudre ce problème, voir cet article de la base de connaissances.

Pour installer un agent

1. Ouvrir l'application Terminal.
2. Effectuez l'une des opérations suivantes :
   - Pour commencer l'installation en précisant les paramètres dans la ligne de commande, exécutez la commande suivante :

     ```
     <package name> -a <parameter 1> ... <parameter N>
     ```

     Ici, `<package name>` est le nom du package d'installation (32 bits ou 64 bits). Voir tous les paramètres disponibles et leurs valeurs dans "Paramètres d'installation ou de désinstallation sans assistance" (p. 95).
   - Pour démarrer l'installation avec des paramètres indiqués dans un fichier texte séparé, exécutez la commande suivante :

     ```
     <package name> -a --options-file=<path to the file>
     ```

     Cette approche peut s'avérer utile si vous ne souhaitez pas saisir d'informations sensibles sur la ligne de commande. Dans ce cas, vous pouvez spécifier les paramètres de configuration dans un fichier texte séparé et vous assurer que vous êtes le seul à pouvoir y accéder. Placez chaque paramètre sur une nouvelle ligne, suivi de la valeur de ce paramètre. Par exemple :

     ```
     --rain=https://company.cloud
     --login=johndoe
     --password=johnspassword
     --auto
     ```

     ou

© Acronis International GmbH, 2003-2026

```
-C
https://company.cloud
-g
johndoe
-w
johnspassword
-a
--language
en
```

Si le même paramètre est indiqué dans la ligne de commande et dans le fichier texte, la valeur de la ligne de commande est prioritaire.

3. Si UEFI Secure Boot est activé sur l'ordinateur, vous êtes invité à redémarrer le système après l'installation. Lorsque vous êtes invité à saisir un mot de passe, utilisez le mot de passe de l'utilisateur root. Si ce mot de passe n'est pas accepté, utilisez le mot « acronis » comme mot de passe. Au redémarrage du système, choisissez la gestion MOK (Machine Owner Key), sélectionnez **Enroll MOK**, puis inscrivez la clé en utilisant le mot de passe recommandé.
   Si vous activez UEFI Secure Boot après l'installation de l'agent, répétez l'installation en incluant l'étape 3. Sinon, les sauvegardes échoueront.

Pour désinstaller un agent

1. Ouvrir l'application Terminal.
2. Effectuez l'une des actions suivantes :
   - Pour désinstaller l'agent et supprimer tous les journaux, tâches et paramètres de configuration, exécutez la commande suivante :

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - Pour désinstaller l'agent tout en conservant son identifiant (par exemple, si vous prévoyez d'installer l'agent ultérieurement), exécutez la commande suivante :

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - Pour désinstaller l'agent à l'aide du fichier d'installation, exécutez la commande suivante :

     ```
     <package name> -a -u
     ```

     Ici, `<package name>` est le nom du package d'installation (32 bits ou 64 bits). Voir tous les paramètres disponibles et leurs valeurs dans "Paramètres d'installation ou de désinstallation sans assistance" (p. 95).

     Remarque
     Utilisez cette commande uniquement lorsque le package d'installation est la même version que l'agent installé et si `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` est corrompu ou inaccessible.

© Acronis International GmbH, 2003-2026

Paramètres d'installation ou de désinstallation sans assistance

Cette section décrit les paramètres d'installation ou de désinstallation sans assistance sous Linux.

La configuration minimale pour une installation sans assistance inclut les paramètres `-a` et d'enregistrement (par exemple, paramètres `--login` et `--password` ; `--rain` et `--token`). Vous pouvez utiliser d'autres paramètres pour personnaliser votre installation.

Paramètres d'installation

Paramètres de base

`{-i |--id=}<list of components>`

Les composants à installer, séparés par des virgules et sans espaces. Les composants suivants sont disponibles dans le package d'installation 64 bits (x86_64) :

Composant	Description du composant
`BackupAndRecoveryAgent`	Agent pour Linux
`AgentForPCS`	Agent pour Virtuozzo
`OracleAgentFeature`	Agent pour Oracle
`MySQLAgentFeature`	Agent pour MySQL/MariaDB
`AgentForProxmox`	Agent pour Proxmox

Sans ce paramètre, tous les composants ci-dessus seront installés.

L'agent pour Virtuozzo, l'agent pour Oracle, l'agent pour MySQL/MariaDB et l'agent pour Proxmox nécessitent que l'agent pour Linux soit également installé.

Le package d'installation 32 bits contient uniquement BackupAndRecoveryAgent.

`{-a|--auto}`

Le processus d'installation et d'enregistrement s'achèvera sans autre intervention de l'utilisateur. Lorsque vous utilisez ce paramètre, vous devez préciser le compte sous lequel l'agent sera enregistré dans le service Cyber Protection, soit à l'aide du paramètre `--token`, soit à l'aide des paramètres `--login` et `--password`.

`{-t|--strict}`

Si le paramètre est spécifié, tous les avertissements pendant l'installation conduiront à un échec de l'installation. Sans ce paramètre, l'installation se termine avec succès même en cas d'avertissement.

`{-n|--nodeps}`

L'absence des packages Linux requis sera ignorée pendant l'installation.

© Acronis International GmbH, 2003-2026

`{-d|--debug}`

Rédige le journal d'installation en mode détaillé.

`--options-file=<location>`

Les paramètres d'installation seront lus depuis un texte source plutôt que depuis la ligne de commande.

`--language=<language ID>`

La langue du produit. Les valeurs disponibles sont les suivantes : `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, vi, zh, zh_TW`.
Si ce paramètre n'est pas précisé, la langue du produit sera définie par la langue de votre système, à condition qu'elle se trouve dans la liste ci-dessus. Sinon, la langue du produit sera définie sur Anglais (`en`).

Paramètres d'enregistrement

Spécifiez l'un des paramètres suivants :

- `{-g|--login=}<user name>` et `{-w|--password=}<password>`

  Les identifiants du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire.

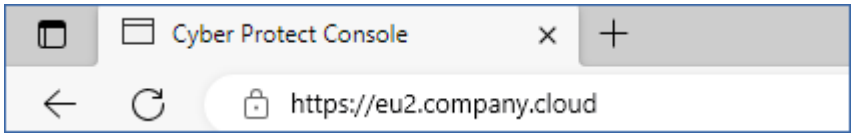
- `--token=<token>`

  Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Pour plus d'informations, voir "Génération d'un jeton d'enregistrement" (p. 112).

  Remarque
  Lorsque vous utilisez le paramètre `--token`, vous devez également inclure le paramètre `{-C|--rain=}` et spécifier l'adresse exacte du centre de données.
  Vous ne pouvez pas utiliser le paramètre `--token` en plus des paramètres `--login`, `--password` et `--register-with-credentials`.

  - `{-C|--rain=}<service address>`

    L'URL du service Cyber Protection.
    Vous devez utiliser le paramètre `{-C|--rain=}` et spécifier l'adresse exacte du centre de données lorsque vous utilisez le paramètre `--token`. L'adresse exacte du centre de données est l'URL que vous voyez **après vous être connecté** à la console Cyber Protection. Par exemple :

    Vous pouvez ignorer le paramètre `{-C|--rain=}` lorsque vous utilisez les paramètres `--login` et `--password` pour l'inscription, car le programme d'installation utilise l'adresse correcte par

© Acronis International GmbH, 2003-2026

défaut.

- `--register-with-credentials`

  Si ce paramètre est spécifié, l'interface graphique de l'installateur démarrera. Pour finaliser l'inscription, saisissez le nom d'utilisateur et le mot de passe du compte sous lequel l'agent sera enregistré dans le service Cyber Protection. Il ne peut pas s'agir d'un compte administrateur partenaire.

- `--skip-registration`

  Utilisez ce paramètre si vous souhaitez installer l'agent, mais que vous prévoyez de l'enregistrer ultérieurement dans le service Cyber Protection. Pour plus d'informations sur la procédure, voir "Enregistrement et désenregistrement de ressources à l'aide de l'interface de ligne de commande" (p. 115).

Paramètres supplémentaires

`--http-proxy-host=<IP address>` et `--http-proxy-port=<port>`

Le serveur proxy HTTP que l'agent utilisera pour la sauvegarde et la restauration depuis le Cloud, ainsi que pour la connexion au serveur de gestion. Sans ces paramètres, aucun serveur proxy ne sera utilisé.

`--http-proxy-login=<login>` et `--http-proxy-password=<password>`

Les accréditations pour le serveur proxy HTTP. Utilisez ces paramètres si le serveur exige une authentification.

`--tmp-dir=<location>`

Indique le dossier dans lequel les fichiers temporaires sont stockés lors de l'installation. Le dossier par défaut est **/var/tmp**.

`{-s|--disable-native-shared}`

Les bibliothèques redistribuables seront utilisées lors de l'installation, même s'il se peut qu'elles soient déjà présentes dans votre système.

`--skip-prereq-check`

Aucune vérification de l'installation des packages nécessaires à la compilation du module snapapi ne sera effectuée.

`--force-weak-snapapi`

L'installateur ne compilera pas de module snapapi. Il utilisera plutôt un module tout prêt qui peut ne pas correspondre exactement au noyau Linux. Nous ne recommandons pas d'utiliser cette option.

`--skip-svc-start`

Les services ne démarreront pas automatiquement après l'installation. La plupart du temps, ce paramètre est utilisé avec `--skip-registration`.

© Acronis International GmbH, 2003-2026

Paramètres d'information

`{-?|--help}`

Affiche la description des paramètres.

`--usage`

Affiche une brève description de la syntaxe de la commande.

`{-v|--version}`

Affiche la version du package d'installation.

`--product-info`

Affiche le nom du produit et la version du package d'installation.

`--snapapi-list`

Affiche les modules snapapi tout prêts disponibles.

`--components-list`

Affiche les composants de l'installateur.

Paramètres pour les fonctionnalités héritées

Ces paramètres se rapportent à un composant hérité, agent.exe.

`{-e|--ssl=}<path>`

Précise le chemin d'accès à un fichier de certificat personnalisé pour la communication SSL.

`{-p|--port=}<port>`

Précise le port qu'agent.exe utilise pour les connexions. Le port par défaut est 9876.

Paramètres de désinstallation

`{-u|--uninstall}`

Désinstalle le produit.

`--purge`

Désinstalle le produit et supprime ses journaux, ses tâches et ses paramètres de configuration. Il est inutile d'indiquer le paramètre `--uninstall` de façon explicite lorsque vous utilisez le paramètre `--purge`.

© Acronis International GmbH, 2003-2026

Exemples

- Installation de l'agent pour Linux sans l'enregistrer.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Installation de l'agent pour Linux, de l'agent pour Virtuozzo et de l'agent pour Oracle, et enregistrement à l'aide des identifiants.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- Installation de l'agent pour Oracle et de l'agent pour Linux, et enregistrement à l'aide d'un jeton d'enregistrement.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2.company.cloud --token=34F6-8C39-4A5C
```

- Installation de l'agent pour Linux, de l'agent pour Virtuozzo et de l'agent pour Oracle, avec des paramètres de configuration dans un fichier texte séparé.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Désinstallation de l'agent pour Linux, de l'agent pour Virtuozzo et de l'agent pour Oracle, et suppression de tous leurs journaux, tâches et paramètres de configuration.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

Installation et désinstallation d'agents de protection dans macOS

Cette section décrit l'installation et la désinstallation de l'agent de protection en mode sans assistance sur un ordinateur sous macOS via la ligne de commande.

Autorisations requises

Avant de lancer une installation sans assistance sur une ressource Mac, vous devez modifier le contrôle des préférences de la politique de confidentialité afin d'autoriser l'accès aux applications et les extensions du noyau et du système dans la ressource macOS pour permettre l'installation de l'agent Cyber Protection. Voir "Autorisations nécessaires à l'installation sans assistance sous macOS" (p. 101).

Après avoir déployé la charge active PPPC, vous pouvez passer aux procédures ci-dessous.

Pour télécharger le fichier d'installation (.dmg)

© Acronis International GmbH, 2003-2026

1. Connectez-vous à la console Cyber Protect.
2. [Pour télécharger le programme d'installation Web pour Mac] Cliquez sur l'icône du compte dans le coin supérieur droit > **Téléchargements**, puis cliquez sur **Agent pour Mac OS**.
   Alternativement, allez à **Terminaux** > **Tous les terminaux**, cliquez sur **Ajouter**, puis cliquez sur **Mac**.
3. [Pour télécharger le programme d'installation complet pour Mac] Cliquez sur l'icône du compte dans le coin supérieur droit > **Téléchargements**, puis cliquez sur **Agent pour Mac OS (64 bits)** ou **Agent pour Mac OS (ARM)**, selon vos besoins.

Pour installer un agent

1. Ouvrir l'application Terminal.
2. Créez un répertoire temporaire dans lequel vous monterez le fichier d'installation (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Remplacez `<dmg_root>` par le nom de répertoire de votre choix.
3. Montez le fichier .dmg.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   Remplacez `<dmg_file>` par le nom du fichier d'installation. Par exemple, **Cyber_Protection_Agent_for_MAC_x64.dmg**.
4. Exécutez le programme d'installation.
   - Si vous utilisez un programme d'installation complet pour Mac, comme `CyberProtect_AgentForMac_x64.dmg` ou `CyberProtect_AgentForMac_arm64.dmg`, exécutez la commande suivante :

     ```
     sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
     ```

     Remarque
     Si vous devez activer l'intégration automatique pour File Sync & Share, exécutez plutôt la commande suivante. Cette option demande le mot de passe de l'administrateur.

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - Si vous utilisez un programme d'installation Web pour Mac, comme `CyberProtect_AgentForMac_web.dmg`, exécutez la commande suivante :

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```
5. Détachez le fichier d'installation (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```


© Acronis International GmbH, 2003-2026

Exemple

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

Pour désinstaller un agent

1. Ouvrir l'application Terminal.
2. Effectuez l'une des actions suivantes :
   - Pour désinstaller l'agent, exécutez la commande suivante :

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm
     ```

   - Pour désinstaller l'agent et supprimer tous les journaux, tâches et paramètres de configuration, exécutez la commande suivante :

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
     ```

Autorisations nécessaires à l'installation sans assistance sous macOS

Avant de lancer une installation sans assistance sur une ressource Mac, vous devez modifier le contrôle des préférences de la politique de confidentialité afin d'autoriser l'accès aux applications et les extensions du noyau et du système dans la ressource macOS pour permettre l'installation de l'agent Cyber Protection. Vous pouvez le faire en déployant une charge active PPPC personnalisée ou en configurant les préférences dans l'interface utilisateur graphique de la ressource. Les tableaux suivants répertorient les autorisations requises.

Voir aussi "Dépannage des problèmes d’autorisation sur macOS" (p. 109).

Configuration requise pour macOS 11 (Big Sur) ou versions ultérieures

Onglet	Section	Champs	Valeur

© Acronis International GmbH, 2003-2026

Contrôle de la stratégie concernant les préférences de confidentialité	Accès à l'application	Identifiant	com.acronis.backup

© Acronis International GmbH, 2003-2026

		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifiant	com.acronis.backup.aakore
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifié	com.acronis.backup.activeprotection
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser

© Acronis International GmbH, 2003-2026

	Accès à l'application	Identifiant	cyber-protect-service
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
Extensions système		Autoriser les utilisateurs à approuver des extensions système	Activé
	Identifiants d'équipe et extensions système autorisés	Nom affiché	Extensions système de l'agent Acronis Cyber Protect
		Types d'extensions système	Identifiants d'équipe autorisés
		Identifiant d'équipe	ZU2TV78AA6

Configuration requise pour les versions macOS antérieures à la version 11

Onglet	Section	Champs	Valeur

© Acronis International GmbH, 2003-2026

Contrôle de la stratégie concernant les préférences de confidentialité	Accès à l'application	Identifiant	com.acronis.backup

© Acronis International GmbH, 2003-2026

		Type d'identifiant	Identifiant du pack

© Acronis International GmbH, 2003-2026

		Exigence de code	`identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifiant	com.acronis.backup.aakore
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
	Accès à l'application	Identifié	com.acronis.backup.activeprotection
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser

© Acronis International GmbH, 2003-2026

	Accès à l'application	Identifiant	cyber-protect-service
		Type d'identifiant	Identifiant du pack
		Exigence de code	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APPLICATION OU SERVICE	SystemPolicyAllFiles
		ACCESS	Autoriser
Extensions du noyau approuvées		Autoriser les utilisateurs à approuver des extensions du noyau	Activé
		Autoriser les utilisateurs standard à approuver les extensions du noyau (macOS 11 ou versions ultérieures)	Activé
	Identifiants d'équipe et Extensions du noyau approuvés	Identifiant de l'équipe approuvé - Nom affiché	Extensions du noyau de l'agent Acronis Cyber Protect
		Identifiant de l'équipe	ZU2TV78AA6
		Identifiants de l'offre groupée des extensions du noyau	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Extensions système		Autoriser les utilisateurs à approuver des extensions système	Activé
	Identifiants d'équipe et	Nom affiché	Acronis Cyber Protection Agent System Extensions

© Acronis International GmbH, 2003-2026

	extensions système autorisés		
		Types d'extensions système	Identifiants d'équipe autorisés
		Identifiant d'équipe	ZU2TV78AA6

Dépannage des problèmes d'autorisation sur macOS

Le message « Blocage de l'extension système » peut apparaître lors de l'installation de l'agent pour macOS sur l'écran de la machine Mac protégée. Les procédures suivantes sont effectuées sur la machine protégée.

Pour approuver l'extension du système de l'agent de cyberprotection Acronis

1. Cliquez sur **Ouvrir Réglages système**.
   Si vous fermez accidentellement la boîte de dialogue, vous pouvez accéder aux **Paramètres/Préférences système** à partir du menu **Apple**.
2. Accédez à **Confidentialité et sécurité**.
3. Faites défiler vers le bas pour trouver le message indiquant que l'extension système a été bloquée.
4. Cliquez sur le bouton **Autoriser** à côté de l'extension bloquée.
5. Redémarrez l'ordinateur Mac pour que les modifications prennent effet.

Remarque
Si le bouton **Autoriser** n'apparaît pas, vous devrez peut-être ajuster les paramètres de sécurité en mode de restauration.

Pour ajuster les paramètres de sécurité en mode de restauration

1. Éteignez le Mac.
2. Appuyez sur le bouton d'alimentation et maintenez-le enfoncé jusqu'à ce que vous voyiez les options de démarrage.
3. Cliquez sur **Options**, puis continuez vers l'écran suivant.
4. Dans le menu **Utilitaires**, sélectionnez **Utilitaire de sécurité de démarrage**.
5. Dans l'utilitaire de sécurité de démarrage, cliquez sur le bouton **Stratégie de sécurité**.
6. Sélectionnez **Réduire la sécurité**, puis sélectionnez la case à cocher **Autoriser la gestion par l'utilisateur des extensions de noyau des développeurs identifiés**.
7. Cliquez sur **OK**, saisissez votre mot de passe d'administrateur et attendez que les modifications soient appliquées.
8. Dans la barre de menu, cliquez sur **Disque de démarrage**, puis cliquez sur **Quitter le disque de démarrage**.
   Cela vous ramènera à l'écran précédent.

© Acronis International GmbH, 2003-2026

9. Cliquez sur l'icône Apple et sélectionnez **Redémarrer**.

Enregistrement des ressources

Un enregistrement connecte une ressource sur laquelle un agent de protection est installé à un compte utilisateur dans un tenant client. Une fois l'enregistrement terminé, vous pouvez voir la ressource dans la console Cyber Protect, sous **Terminaux** > **Machines avec agents**. Vous pouvez gérer les ressources enregistrées en leur appliquant des plans.

Lorsque vous installez un agent de protection à l'aide de l'interface graphique, l'enregistrement fait partie de la procédure d'installation.

Lorsque vous utilisez l'interface de ligne de commande, vous pouvez effectuer l'enregistrement en tant que procédure autonome.

Enregistrement des ressources à l'aide de l'interface utilisateur graphique

Lorsque vous installez un agent de protection à l'aide de l'interface graphique, l'enregistrement fait partie de la procédure d'installation.

Les méthodes d'enregistrement suivantes sont disponibles :

- Enregistrement dans la console Cyber Protect
- Enregistrement avec les identifiants du compte utilisateur
- Enregistrement avec un jeton d'enregistrement

L'agent est automatiquement désenregistré lorsque vous le désinstallez.

Enregistrement des ressources à l'aide de la console Cyber Protect

Lors de l'utilisation de la console Cyber Protect, l'inscription des ressources fait partie de l'installation des agents de protection.

Prérequis

- Vous avez terminé l'installation d'un agent de protection avec les paramètres d'installation par défaut (**Paramètres d'inscription** > **Utiliser la console Cyber Protect**), et l'assistant d'installation est toujours ouvert.

  Remarque
  Ne fermez pas l'assistant d'installation avant d'avoir terminé l'enregistrement. Sinon, vous devrez répéter l'installation et recommencer l'enregistrement.

- Pour pouvoir sélectionner un plan lors de l'inscription, l'authentification à deux facteurs (2FA) doit être activée pour le tenant auquel appartient votre compte. Pour plus d'informations, voir "Plans préselectionnés" (p. 238).

 © Acronis International GmbH, 2003-2026

Pour enregistrer une ressource à partir de la console Cyber Protect

1. Dans l'assistant d'installation, cliquez sur **Enregistrer la ressource**.
   La console Cyber Protect s'ouvre.
2. Connectez-vous à la console Cyber Protect.
   L'assistant **Enregistrer la ressource** s'ouvre.
3. [Si vous vous connectez en tant qu'administrateur] Dans l'onglet **Sélectionner le compte**, sélectionnez le compte sous lequel vous souhaitez enregistrer la ressource.
   Ce compte doit se trouver dans un tenant client ou dans une unité. Les administrateurs partenaires peuvent voir les tenants clients qu'ils gèrent et peuvent enregistrer des ressources sous des comptes situés dans ces tenants.

   Remarque
   Si un seul compte existe dans le tenant ou l'unité sélectionné, ce champ est prérempli.
4. Cliquez sur **Valider le code**.
5. Cliquez sur **Suivant**.
6. [Si l'authentification à deux facteurs est activée pour votre compte] Dans l'onglet **Sélectionner des plans**, examinez les plans présélectionnés qui seront appliqués à la ressource.
7. [Facultatif] [Si l'authentification à deux facteurs est activée pour votre compte] Pour changer un plan préselectionné, cliquez sur **Changer**.
   - Sélectionnez un plan.
   - Cliquez sur **Sélectionner**.
8. [Facultatif] Si vous ne souhaitez pas appliquer un plan présélectionné, cliquez sur **Changer**, puis cliquez sur **Ne pas appliquer**.
9. Dans l'écran **Examiner et enregistrer**, vérifiez les quotas requis, puis effectuez l'une des opérations suivantes :
   a. Pour enregistrer la ressource, cliquez sur **Enregistrer**.
      Si vous êtes connecté en tant qu'administrateur partenaire, tous les packs Advanced requis seront automatiquement activés pour le tenant dans lequel vous enregistrez la ressource.
      Si vous n'êtes pas connecté en tant qu'administrateur partenaire, aucun pack Advanced requis ne sera activé automatiquement. Vous pouvez toujours appliquer les plans sélectionnés, mais ils peuvent ne pas fonctionner correctement. Pour résoudre ce problème, demandez à votre administrateur partenaire d'activer les packs Advanced requis ou de modifier les plans présélectionnés.
   b. Pour sélectionner d'autres plans, accédez à l'onglet **Sélectionner des plans**, puis poursuivez cette procédure.

En conséquence, la ressource est enregistrée sous le compte spécifié et les plans sélectionnés sont appliqués automatiquement.

© Acronis International GmbH, 2003-2026

Enregistrement des ressources à l'aide des identifiants utilisateur

Vous pouvez modifier la procédure d'installation par défaut et sélectionner l'enregistrement avec un nom d'utilisateur et un mot de passe, au lieu de celui dans la console Cyber Protect.

Pour inscrire une ressource à l'aide d'un nom d'utilisateur et d'un mot de passe

1. Dans l'assistant d'installation, cliquez sur **Personnaliser les paramètres d'installation**.
2. Dans la section **Paramètres d'enregistrement**, cliquez sur **Modifier**.
3. Sélectionnez **Utiliser les informations d'identification**.
4. Indiquez le nom d'utilisateur et le mot de passe du compte sous lequel vous souhaitez enregistrer la ressource.
   Ce compte doit être un compte de tenant client.

   Remarque
   Vous ne pouvez utiliser que les comptes pour lesquels l'authentification à deux facteurs n'est pas activée.
5. Cliquez sur **Terminé**, puis terminez l'installation.

Enregistrement des ressources à l'aide d'un jeton d'enregistrement

Vous pouvez modifier la procédure d'installation par défaut et sélectionner l'enregistrement avec un jeton d'enregistrement, au lieu de celui dans la console Cyber Protect.

Pour inscrire une ressource à l'aide d'un jeton d'enregistrement

1. Dans l'assistant d'installation, cliquez sur **Personnaliser les paramètres d'installation**.
2. Dans la section **Paramètres d'enregistrement**, cliquez sur **Modifier**.
3. Sélectionnez **Utiliser le jeton d'enregistrement**.
4. Saisissez le jeton d'enregistrement.
5. Cliquez sur **Terminé**, puis terminez l'installation.

Génération d'un jeton d'enregistrement

Un jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Le jeton d'enregistrement transmet l'identité d'un utilisateur au programme d'installation de l'agent, sans stocker les identifiants utilisateur pour la console Cyber Protect. Cela permet aux utilisateurs d'enregistrer des ressources sous leur compte ou d'appliquer des plans de protection à des ressources sans se connecter à la console.

Remarque
Les plans de protection ne sont pas appliqués automatiquement lors de l'enregistrement de la ressource. L'application d'un plan de protection est une tâche distincte.

© Acronis International GmbH, 2003-2026

Pour des raisons de sécurité, la durée de vie des jetons est limitée, mais elle peut être modifiée. La durée de vie par défaut est de trois jours.

Les administrateurs peuvent générer des jetons d'enregistrement pour tous les comptes d'utilisateurs du tenant qu'ils gèrent. Les utilisateurs ne peuvent générer des jetons d'enregistrement que pour leurs propres comptes.

Générer un jeton d'enregistrement

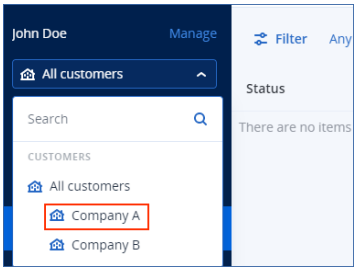
En tant qu'administrateur

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.

   Si vous êtes déjà connecté au portail de gestion, vous pouvez accéder à la console Cyber Protect en sélectionnant **Surveillance** > **Utilisation**, puis en cliquant dans l'onglet **Protection** sur **Gérer le service**.

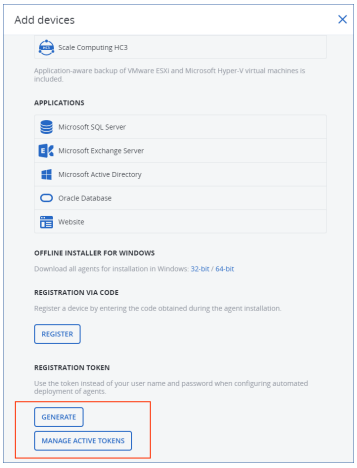
   [Pour les administrateurs partenaires qui gèrent les tenants des clients] Dans la console Cyber Protect, sélectionnez le tenant comportant l'utilisateur pour lequel vous souhaitez générer un jeton. Vous ne pouvez pas générer de jeton au niveau **Tous les clients**.

2. Sous **Terminaux**, cliquez sur **Tous les terminaux** > **Ajouter**.

   Le panneau **Ajouter des terminaux** s'ouvre à droite.

3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Générer**.

4. Spécifiez la durée de vie du jeton.

© Acronis International GmbH, 2003-2026

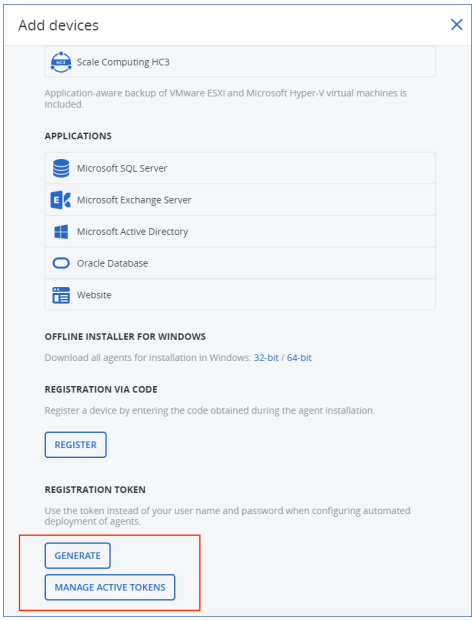
5. Sélectionnez l'utilisateur pour qui vous souhaitez générer un jeton.

> **Remarque**
> Lorsque vous utilisez le jeton, les ressources sont inscrites dans le compte utilisateur sélectionné ici.

6. [Facultatif] Pour permettre à l'utilisateur du jeton d'appliquer ou de révoquer un plan de protection sur les ressources ajoutées, sélectionnez le plan dans la liste déroulante.
   Pour appliquer ou révoquer le plan de protection sur les ressources ajoutées, vous devez exécuter un script. Pour plus d'informations, voir cet article de la base de connaissances.
7. Cliquez sur **Générer le jeton**.
8. Cliquez sur **Copier** pour copier le jeton dans le Presse-papiers de votre terminal ou notez le jeton manuellement.

En tant qu'utilisateur

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter**.
   Le panneau **Ajouter des terminaux** s'ouvre à droite.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Générer**.



4. Spécifiez la durée de vie du jeton.
5. Cliquez sur **Générer le jeton**.
6. Cliquez sur **Copier** pour copier le jeton dans le Presse-papiers de votre terminal ou notez le jeton manuellement.

Gestion des jetons d'enregistrement

Vous pouvez consulter et supprimer les jetons d'enregistrement actifs.

Pour visualiser les jetons d'enregistrement

© Acronis International GmbH, 2003-2026

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter**.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Gérer les jetons actifs**.
   La liste des jetons actifs qui sont générés pour le tenant s'ouvre à droite.

   Remarque
   Pour des raisons de sécurité, seuls les deux premiers caractères de la valeur de jeton sont affichés dans la colonne **Jeton**.

Pour supprimer un jeton d'enregistrement

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter**.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Gérer les jetons actifs**.
   La liste des jetons actifs qui sont générés pour le tenant s'ouvre à droite.

   Remarque
   Pour des raisons de sécurité, seuls les deux premiers caractères de la valeur de jeton sont affichés dans la colonne **Jeton**.

4. Sélectionnez le jeton, puis cliquez sur **Supprimer**.

Enregistrement et désenregistrement de ressources à l'aide de l'interface de ligne de commande

Lorsque vous utilisez l'interface de ligne de commande, vous pouvez effectuer l'enregistrement en tant que procédure autonome.

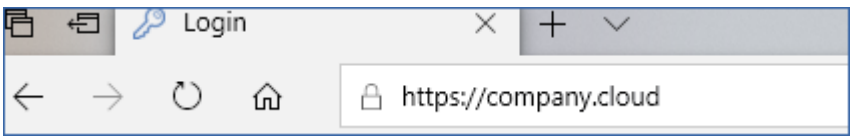
Par exemple, vous ne devez pas désinstaller l'agent de protection si vous souhaitez l'enregistrer sous un autre compte.

Enregistrement des ressources à l'aide des identifiants utilisateur

Utilisez le nom d'utilisateur et le mot de passe du compte sous lequel vous souhaitez enregistrer la ressource. Ce compte doit être un compte d'un tenant client. Si le mot de passe contient des caractères spéciaux ou des espaces vides, voir "Utilisation de mots de passe comportant des caractères spéciaux ou des espaces vides" (p. 116).

L'adresse du service est l'URL que vous utilisez pour vous connecter au service Cyber Protection.

Par exemple, `https://company.cloud`.



© Acronis International GmbH, 2003-2026

Pour inscrire une ressource à l'aide d'un nom d'utilisateur et d'un mot de passe

Sous Windows

- À l'invite de commandes, exécutez la commande suivante :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a <service address> -u <user name> -p <password>
```

Par exemple :

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://company.cloud -u johndoe -p johnspassword
```

Sous Linux

- Dans l'interface de ligne de commande, exécutez la commande suivante :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> -u <user name> -p <password>
```

Par exemple :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://company.cloud -u johndoe -p johnspassword
```

Sous macOS

Important
Si vous utilisez macOS 10.14 ou une version ultérieure, accordez un accès complet au disque à l'agent de protection. Pour ce faire, allez dans **Applications** >**Utilitaires**, puis exécutez **Assistant Cyber Protect Agent**. Suivez ensuite les instructions de la fenêtre de l'application.

- Dans l'interface de ligne de commande, exécutez la commande suivante :

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> -u <user name> -p <password>
```

Par exemple :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://company.cloud -u johndoe -p johnspassword
```

Utilisation de mots de passe comportant des caractères spéciaux ou des espaces vides

Si votre mot de passe contient des caractères spéciaux ou des espaces vides, mettez-le entre guillemets lorsque vous le saisissez dans la ligne de commande.

Par exemple, sous Windows, exécutez cette commande dans l'invite de commande :

© Acronis International GmbH, 2003-2026

Modèle de commande

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

Exemples de commandes

- Windows

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://company.cloud -u johndoe -p "johnspassword"
```

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://company.cloud -u johndoe -p "johnspassword"
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://company.cloud -u johndoe -p "johnspassword"
```

En cas d'échec de la commande, chiffrez votre mot de passe au format base64 sur https://www.base64encode.org/. Indiquez ensuite, dans la ligne de commande, le mot de passe chiffré à l'aide du paramètre -b ou --base64.

Par exemple, sous Windows, exécutez cette commande dans l'invite de commande :

Modèle de commande

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

Exemples de commandes

- Windows

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://company.cloud -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://company.cloud -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://company.cloud -u johndoe -b -p am9obnNwYXNzd29yZA==
```


© Acronis International GmbH, 2003-2026

Enregistrement des ressources à l'aide d'un jeton d'enregistrement

Un jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Le jeton d'enregistrement transmet l'identité d'un utilisateur au programme d'installation de l'agent, sans stocker les identifiants utilisateur pour la console Cyber Protect. Cela permet aux utilisateurs d'enregistrer des ressources sous leur compte ou d'appliquer des plans de protection à des ressources sans se connecter à la console.

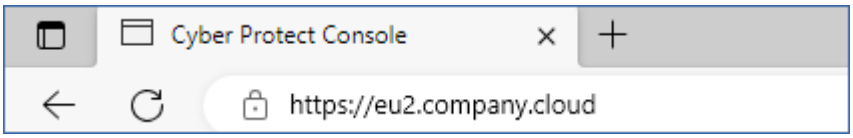
Pour plus d'informations, voir "Génération d'un jeton d'enregistrement" (p. 112).

Remarque
Les plans de protection ne sont pas appliqués automatiquement lors de l'enregistrement de la ressource. L'application d'un plan de protection est une tâche distincte.

Pour plus d'informations, voir cet article de la base de connaissances.

Lorsque vous utilisez un jeton d'enregistrement, vous devez spécifier l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez après votre connexion au service Cyber Protection.

Par exemple, `https://eu2.company.cloud`.



Pour inscrire une ressource à l'aide d'un jeton d'enregistrement

Sous Windows

- À l'invite de commandes, exécutez la commande suivante :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a <service address> --token <registration token>
```

Par exemple :

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://au1.company.cloud --token 3B4C-E967-4FBD
```

Sous Linux

- Dans l'interface de ligne de commande, exécutez la commande suivante :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> --token <registration token>
```

Par exemple :

© Acronis International GmbH, 2003-2026

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2.company.cloud --token 34F6-8C39-4A5C
```

Sous macOS

Important
Si vous utilisez macOS 10.14 ou une version ultérieure, accordez un accès complet au disque à l'agent de protection. Pour ce faire, allez dans **Applications** >**Utilitaires**, puis exécutez **Assistant Cyber Protect Agent**. Suivez ensuite les instructions de la fenêtre de l'application.

- Dans l'interface de ligne de commande, exécutez la commande suivante :

  ```
  sudo "/Library/Application
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
  <service address> --token <registration token>
  ```

Par exemple :

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5.company.cloud --token 9DBF-3DA9-4DAB
```

Appliance virtuelle

1. Dans la console de l'appliance virtuelle, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
2. Dans l'interface de ligne de commande, exécutez la commande suivante :

   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   Par exemple :

   ```
   register_agent -o register -t cloud -a https://eu2.company.cloud --token 34F6-8C39-
   4A5C
   ```

3. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

Support de démarrage

1. Dans l'interface graphique du support de démarrage, cliquez sur **Actions** > **Démarrer le shell**.
2. Dans l'interface de ligne de commande, accédez au dossier `/bin` :

   ```
   cd /bin
   ```

3. Dans l'interface de ligne de commande, exécutez la commande suivante :

   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   Par exemple :

© Acronis International GmbH, 2003-2026

```
register_agent -o register -t cloud -a https://eu2.company.cloud --token 34F6-8C39-
4A5C
```

4. Pour revenir à l'interface graphique du support de démarrage, appuyez sur ALT+F1.

Désenregistrement des ressources

Vous pouvez désenregistrer un agent de protection depuis l'interface de ligne de commande sans le désinstaller.

Pour désinscrire une ressource

Sous Windows

- À l'invite de commandes, exécutez la commande suivante :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Par exemple :

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Sous Linux

- Dans l'interface de ligne de commande, exécutez la commande suivante :

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Sous macOS

- Dans l'interface de ligne de commande, exécutez la commande suivante :

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Appliance virtuelle

1. Dans la console de l'appliance virtuelle, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
2. Dans l'interface de ligne de commande, exécutez la commande suivante :

```
register_agent -o unregister
```

3. Pour revenir à l'interface graphique de l'appliance, appuyez sur ALT+F1.

Modification de l'inscription d'une ressource

Vous pouvez modifier l'inscription actuelle d'une ressource en l'inscrivant dans un nouveau tenant ou sous un nouveau compte utilisateur.

© Acronis International GmbH, 2003-2026

Important
Lorsque vous modifiez l'inscription d'une ressource, tous les plans de protection qui lui sont appliqués sont révoqués. Pour continuer à protéger la ressource, appliquez-lui un nouveau plan de protection.

Si vous inscrivez la ressource dans un nouveau tenant, cette ressource perd l'accès aux sauvegardes enregistrées dans le stockage dans le cloud du tenant d'origine. Les sauvegardes enregistrées ailleurs que dans des stockages dans le cloud restent accessibles.

Pour modifier l'inscription d'une ressource

En utilisant l'interface de ligne de commande

1. Désinscrivez l'agent de protection en suivant les indications figurant dans "Désenregistrement des ressources" (p. 120).
2. Inscrivez l'agent de protection dans le nouveau tenant ou sous le nouveau compte utilisateur en suivant les indications de "Enregistrement des ressources à l'aide des identifiants utilisateur" (p. 115) ou de "Enregistrement des ressources à l'aide d'un jeton d'enregistrement" (p. 118).

En utilisant l'interface utilisateur graphique

1. Désinstallez l'agent de protection.
2. Installez l'agent de protection, puis inscrivez-le dans le nouveau tenant ou sous le nouveau compte utilisateur.

Pour plus d'informations sur l'installation et l'enregistrement d'un agent, voir "Installation des agents de protection à l'aide de l'interface utilisateur graphique" (p. 64).

Déplacement des ressources vers un autre tenant

Le déplacement d'une ressource vers un autre tenant n'est pas pris en charge de manière native. Vous pouvez dans ce cas annuler l'enregistrement de la ressource, puis l'enregistrer dans un autre tenant. Tous les plans de protection appliqués sont révoqués de cette ressource et perdent l'accès à ses sauvegardes enregistrées dans le stockage dans le cloud du tenant d'origine.

Pour plus d'informations sur l'enregistrement d'une ressource dans un nouveau tenant ou sous un nouveau compte utilisateur, voir "Modification de l'inscription d'une ressource" (p. 120).

Mise à jour des agents de protection

Vous pouvez mettre à jour manuellement tous les agents à l'aide de la console Cyber Protect ou en téléchargeant et en exécutant le fichier d'installation.

Vous pouvez configurer les mises à jour automatiques pour les agents suivants :

- Agent pour Windows
- Agent pour Linux

© Acronis International GmbH, 2003-2026

- Agent pour Mac
- Agent de Cloud Cyber Files pour File Sync & Share

Espace disque libre nécessaire pour la mise à jour

Un espace libre est nécessaire pour la mise à jour automatique ou manuelle d'un agent à l'aide de la console Cyber Protect.

Système d'exploitation	Emplacement de téléchargement	Espace disque requis
Linux	/opt/acronis/Acroinst2/	3 Go
Mac	/Library/Application Support/Acronis/Acroinst2	2 Go
Windows	%ProgramData%\Acronis\Acroinst2\ %ProgramData%\Acronis\InstallationCache\	2 Go

Remarque
[Pour tous les agents fournis sous la forme d'une appliance virtuelle, y compris Agent pour VMware, Agent pour Scale Computing, Agent pour Virtuozzo Hybrid Infrastructure, Agent pour RHV (oVirt)]

Pour effectuer une mise à jour automatique ou manuelle d'une appliance virtuelle située derrière un proxy, vous devez configurer le serveur proxy sur chaque appliance comme suit.

Dans le fichier `/opt/acronis/etc/va-updater/config.yaml`, ajoutez la ligne suivante en bas du fichier, puis saisissez les valeurs correspondant à votre environnement :

```
httpProxy : http://proxy_login:proxy_password@proxy_address:port
```

Configuration de la méthode par défaut pour mettre à jour les agents

Vous pouvez configurer la méthode par défaut de mise à jour des agents - manuelle ou automatique, pour tous les agents sur tous les ordinateurs ou sur des ordinateurs individuels.

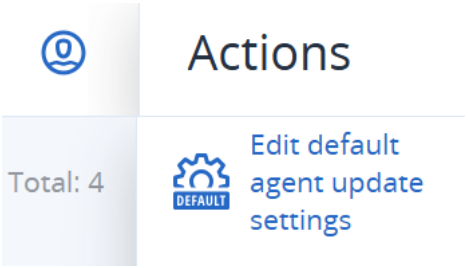
Les paramètres par défaut pour les mises à jour d'agent sont accessibles depuis la console Cyber Protection et le Portail de gestion, pour tous les rôles d'utilisateur.

Mises à jour automatiques

Pour configurer les paramètres par défaut pour les mises à jour automatiques pour tous les agents dans la console Cyber Protect

1. Sélectionnez **Paramètres** > **Agents**.
2. Dans le coin supérieur droit, sous **Actions**, cliquez sur **Modifier les paramètres de mise à jour par défaut de l'agent**.

© Acronis International GmbH, 2003-2026



3. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

4. Vérifiez que l'option **Mettre à jour automatiquement les agents** est activée.

Remarque
Les mises à jour automatiques ne sont disponibles que pour les agents suivants :

- Agent Cyber Protect version 26986 (publiée en mai 2021) ou versions ultérieures.
- L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

Les agents plus anciens doivent d'abord être mis à jour vers la dernière version avant que les mises à jour automatiques entrent en vigueur.

5. [Facultatif] Définissez la fenêtre de maintenance.
La fenêtre par défaut est quotidienne, de 23 h 00 à 8 h 00, sur la machine où l'agent est installé.

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

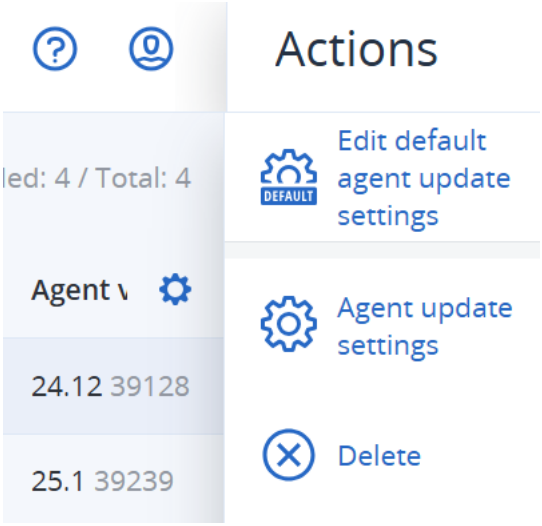
6. Cliquez sur **Enregistrer**.

Pour configurer les paramètres par défaut pour les mises à jour automatiques pour les agents sélectionnés dans la console Cyber Protect.

1. Sélectionnez **Paramètres** > **Agents**.
2. Dans la liste des agents, sélectionnez l'agent pour lequel vous souhaitez configurer les paramètres de mise à jour automatique.

© Acronis International GmbH, 2003-2026

3. Dans le coin supérieur droit, sous **Actions**, cliquez sur **Paramètres de mise à jour d'agent**.



4. Cliquez sur **Modifier les paramètres de mise à jour d'agent par défaut**.
5. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

6. Vérifiez que l'option **Mettre à jour automatiquement les agents** est activée.

Remarque
Les mises à jour automatiques ne sont disponibles que pour les agents suivants :

- Agent Cyber Protect version 26986 (publiée en mai 2021) ou versions ultérieures.
- L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

Les agents plus anciens doivent d'abord être mis à jour vers la dernière version avant que les mises à jour automatiques entrent en vigueur.

7. [Facultatif] Définissez la fenêtre de maintenance.
La fenêtre par défaut est quotidienne, de 23 h 00 à 8 h 00, sur la machine où l'agent est installé.

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

8. Cliquez sur **Enregistrer**.

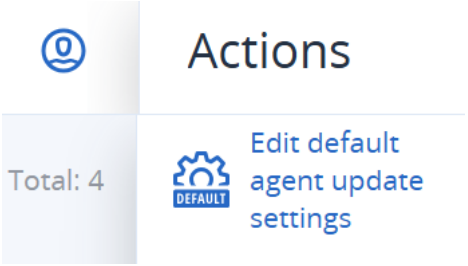
Mises à jour manuelles

© Acronis International GmbH, 2003-2026

Important
Nous vous recommandons vivement d'activer les mises à jour automatiques pour vos agents. Grâce aux mises à jour régulières, vous tenez vos agents à jour, obtenez de meilleures performances, corrigez les problèmes de bogues, et améliorez les fonctionnalités de protection et de sécurité.

Pour configurer les paramètres par défaut pour les mises à jour manuelles pour tous les agents dans la console Cyber Protection

1. Accédez à **Paramètres** > **Agents**.
2. Dans le coin supérieur droit, sous **Actions**, cliquez sur **Modifier les paramètres de mise à jour par défaut de l'agent**.

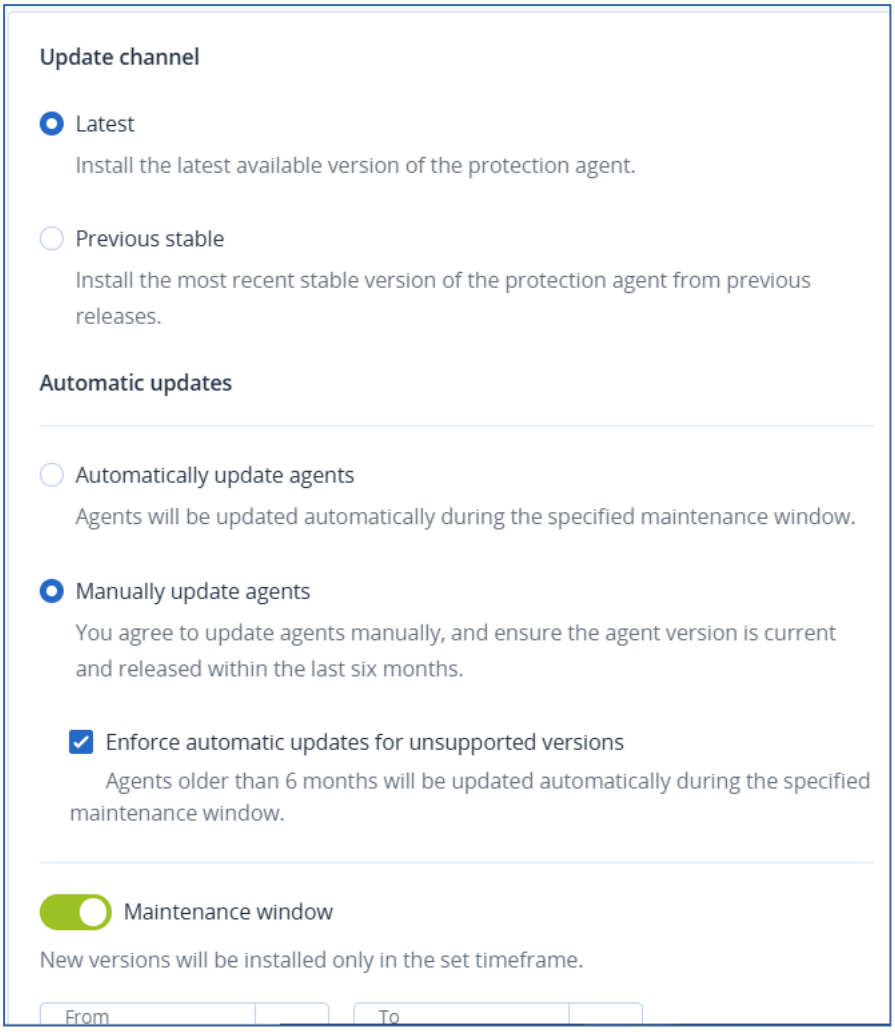


3. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

4. Sélectionnez **Mettre à jour les agents manuellement**.

© Acronis International GmbH, 2003-2026



5. [Facultatif] Pour éviter les risques de sécurité, garantir l'accès aux dernières fonctionnalités et minimiser les problèmes techniques causés par des agents très obsolètes, activez les mises à jour automatiques des agents de plus de 6 mois.
   a. Sélectionnez **Appliquer les mises à jour automatiques des versions non prises en charge**.

      Important
      Si vous n'avez pas activé les mises à jour automatiques des agents avant de passer à la version C25.02, cette option est activée automatiquement pour tous les tenants de votre environnement.

   b. [Facultatif] Définissez la fenêtre de maintenance.
      La fenêtre de maintenance par défaut est quotidienne, de 23 h 00 à 08 h 00 sur l'ordinateur où l'agent est installé.

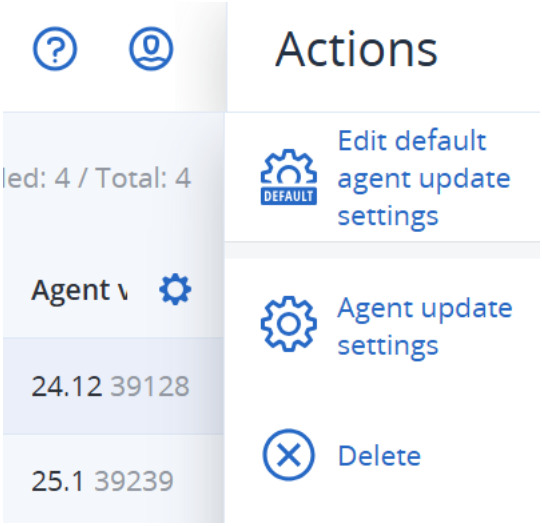
© Acronis International GmbH, 2003-2026

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

6. Cliquez sur **Enregistrer**.

Pour configurer des mises à jour manuelles pour les agents sélectionnés dans la console Cyber Protect.

1. Accédez à **Paramètres** > **Agents**.
2. Dans la liste des agents, sélectionnez l'agent pour lequel vous souhaitez configurer les paramètres de mise à jour automatique.
3. Dans le coin supérieur droit, sous **Actions**, cliquez sur **Paramètres de mise à jour d'agent**.

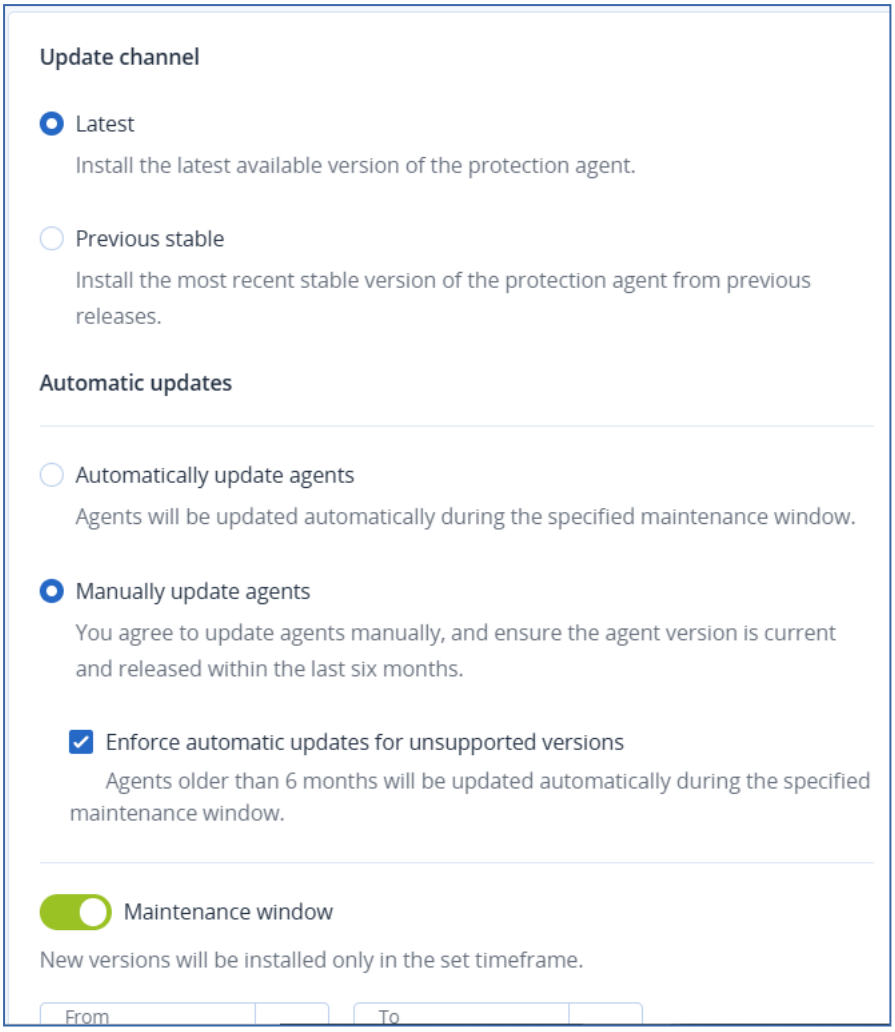


4. Cliquez sur **Modifier les paramètres de mise à jour d'agent par défaut**.
5. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

6. Sélectionnez **Mettre à jour les agents manuellement**.

© Acronis International GmbH, 2003-2026



7. [Facultatif] Pour éviter les risques de sécurité, garantir l'accès aux dernières fonctionnalités et minimiser les problèmes techniques causés par des agents très obsolètes, activez les mises à jour automatiques des agents de plus de 6 mois.
   a. Sélectionnez **Appliquer les mises à jour automatiques des versions non prises en charge**.

   Important
   Si vous n'avez pas activé les mises à jour automatiques des agents avant de passer à la version C25.02, cette option est activée automatiquement pour tous les tenants de votre environnement.

   b. [Facultatif] Définissez la fenêtre de maintenance.
   La fenêtre de maintenance par défaut est quotidienne, de 23h00 à 8h00, sur la machine où l'agent est installé.

© Acronis International GmbH, 2003-2026

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

8. Cliquez sur **Enregistrer**.

Surveillance des mises à jour de l'agent

Pour surveiller les mises à jour de l'agent, voir les sections "Le tableau de bord des alertes" (p. 300) et "Le tableau de bord Activités" (p. 299).

Mise à jour manuelle des agents de protection

Vous pouvez mettre à jour les agents à l'aide de la console Cyber Protect ou en téléchargeant et en exécutant le fichier d'installation.

Les appliances virtuelles avec les versions suivantes doivent être mises à jour uniquement à l'aide de la console Cyber Protect :

- Agent pour VMware (appliance virtuelle) : version 12.5.23094 et ultérieures.
- Agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) : version 12.5.23094 et ultérieures.

Les versions suivantes des agents peuvent aussi être mises à jour via la console Cyber Protect :

- Agent pour Windows, agent pour VMware (Windows), agent pour Hyper-V : version 12.5.21670 et ultérieures.
- Agent pour Linux : version 12.5.23094 et ultérieures.
- Autres agents : version 12.5.23094 et ultérieures.

Pour effectuer une mise à jour des agents à partir de versions antérieures, téléchargez et installez manuellement la version la plus récente. Pour trouver les liens de téléchargement, cliquez sur **Tous les terminaux** > **Ajouter**.

Pour trouver la version de l'agent, dans la console Cyber Protect, sélectionnez l'ordinateur, puis cliquez sur **Détails**.

Prérequis

Sur les machines Windows, les fonctionnalités Cyber Protect nécessitent le package redistribuable Microsoft Visual C++ 2017. Veillez à ce qu'il soit déjà installé sur votre ordinateur, ou installez-le avant de mettre l'agent à jour. Après l'installation, il peut être nécessaire de redémarrer l'ordinateur. Le package redistribuable Microsoft Visual C++ est disponible sur le site Web de Microsoft : https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

© Acronis International GmbH, 2003-2026

Pour mettre à jour un agent via la console Cyber Protect

Remarque
[Pour les plans de protection créés après novembre 2024] La désinstallation et la modification des agents de protection pour Windows sont interdites par défaut. L'agent pour Windows peut être modifié uniquement pendant une fenêtre de maintenance ou via la fonctionnalité de mise à jour automatique de l'agent. Pour obtenir des instructions sur l'autorisation de la désinstallation ou la modification ponctuelle d'un agent, voir "Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée" (p. 208). Pour désactiver la protection de désinstallation de l'agent, voir "Pour désactiver la protection contre la désinstallation de l'agent" (p. 209).

1. Cliquez sur **Paramètres** > **Agents**.
   La liste des machines protégées apparaît. Les machines dont la version des agents est obsolète sont marquées d'un point d'exclamation orange.
2. Sélectionnez les machines sur lesquelles vous souhaitez effectuer une mise à jour des agents.

   Remarque
   Ces machines doivent être en ligne.

3. Cliquez sur **Mise à jour de l'agent**.

Remarque
Lors de la mise à jour, toute sauvegarde en cours échouera.

Pour mettre à jour les définitions de cyberprotection sur une machine

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez la machine sur laquelle vous souhaitez effectuer une mise à jour des définitions de cyberprotection, puis cliquez sur **Mettre les définitions à jour**. La machine doit être en ligne.

Pour attribuer le rôle Responsable de la mise à jour à un agent

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur auquel vous souhaitez affecter le rôle Responsable de la mise à jour, cliquez sur **Détails**, puis activez dans la section **Définitions de la cyberprotection** l'option **Utilisez cet agent pour télécharger et distribuer des correctifs et des mises à jour**.

   Remarque
   Un agent avec le rôle Responsable de la mise à jour ne peut télécharger et distribuer des correctifs que pour les produits tiers Windows. Pour les produits Microsoft, la distribution des correctifs n'est pas prise en charge par l'agent Responsable de la mise à jour.

Pour effacer les données en cache sur un agent

© Acronis International GmbH, 2003-2026

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez la machine dont vous souhaitez effacer les données en cache (fichiers de mise à jour et données de gestion des correctifs obsolètes), puis cliquez sur **Vider le cache**.

Mise à jour automatique des agents de protection

Pour faciliter la gestion de nombreuses ressources, vous pouvez configurer les mises à jour automatiques de l'agent pour Windows, de l'agent pour Linux et de l'agent pour Mac. Les mises à jour automatiques sont disponibles pour les agents version 26986 (publiée en mai 2021) ou versions ultérieures. Pour les agents plus anciens, vous devez d'abord effectuer une mise à jour vers la dernière version.

Remarque
La configuration des mises à jour automatiques pour un agent de protection remplace le paramètre **Protection contre la désinstallation de l'agent** dans tous les plans de protection de l'agent.

Les mises à jour automatiques sont prises en charge sur les ordinateurs exécutant l'un des systèmes d'exploitation suivants :

- Windows XP SP 3 et versions ultérieures
- Red Hat Enterprise Linux 6 et versions ultérieures, CentOS 6 et versions ultérieures
- OS X 10.9 Mavericks et versions ultérieures

Les paramètres de mise à jour automatique sont préconfigurés au niveau du centre de données. Un administrateur partenaire ou d'entreprise peut personnaliser ces paramètres, pour tous les ordinateurs d'une entreprise ou d'une unité, ou pour des machines individuelles. Si aucun paramètre personnalisé n'est appliqué, les paramètres du niveau supérieur sont utilisés, dans cet ordre :

1. Centre de données Cyber Protection
2. Entreprise (tenant client)
3. Unité
4. Machine

Par exemple, un administrateur d'unité peut configurer des paramètres de mise à jour automatique pour tous les ordinateurs de l'unité, qui peuvent être différents des paramètres appliqués aux ordinateurs au niveau de l'entreprise. L'administrateur peut aussi configurer différents paramètres pour un ou plusieurs ordinateurs individuels de l'unité, sur lesquels les paramètres au niveau de l'unité et de l'entreprise ne seront pas appliqués.
Même lors de la fenêtre de maintenance activée, les mises à jour ne seront pas installées tant que l'agent exécutera l'une des opérations suivantes :

- Sauvegarde
- Restauration

© Acronis International GmbH, 2003-2026

- Réplication de sauvegarde
- Réplication de machine virtuelle
- Test d'un réplica
- Exécution d'une machine virtuelle à partir d'une sauvegarde (y compris finalisation)
- Basculement pour reprise d'activité après sinistre
- Restauration automatique pour reprise d'activité après sinistre
- Exécution d'un script (pour la fonctionnalité de création de cyber-scripts)
- Installation des correctifs
- Sauvegarde de la configuration ESXi

Mises à jour automatiques pour tous les agents

Pour configurer les mises à jour automatiques des agents à partir de la console Cyber Protection

1. Sélectionnez **Paramètres > Agents**.
2. Sous **Actions** dans le coin supérieur droit, cliquez sur **Modifier les paramètres de mise à jour de l'agent par défaut**.
3. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

4. Vérifiez que l'option **Mettre à jour automatiquement les agents** est activée.

   Remarque
   Les mises à jour automatiques ne sont disponibles que pour les agents suivants :
   - Agent Cyber Protect version 26986 (publiée en mai 2021) ou versions ultérieures.
   - L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

   Les agents plus anciens doivent d'abord être mis à jour vers la dernière version avant que les mises à jour automatiques entrent en vigueur.

5. [Facultatif] Activez la fenêtre de maintenance.
   La fenêtre par défaut est quotidienne, de 23 h 00 à 08 h 00 sur l'ordinateur où l'agent est installé.

© Acronis International GmbH, 2003-2026

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

6. Cliquez sur **Enregistrer**.

Mises à jour automatiques d'un seul agent

Important
Nous vous recommandons vivement d'activer les mises à jour automatiques pour vos agents. Grâce aux mises à jour régulières, vous tenez vos agents à jour, obtenez de meilleures performances, corrigez les problèmes de bogues, et améliorez les fonctionnalités de protection et de sécurité.

Pour configurer les mises à jour automatiques d'un agent à partir de la console Cyber Protection

1. Sélectionnez **Paramètres > Agents**.
2. Dans la liste des agents, sélectionnez l'agent pour lequel vous souhaitez configurer les paramètres de mise à jour automatique.
3. Sous **Actions** dans le coin supérieur droit, cliquez sur **Paramètres de mise à jour de l'agent**.
4. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

5. Vérifiez que l'option **Mettre à jour automatiquement les agents** est activée.

Remarque
Les mises à jour automatiques ne sont disponibles que pour les agents suivants :
- Agent Cyber Protect version 26986 (publiée en mai 2021) ou versions ultérieures.
- L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

Les agents plus anciens doivent d'abord être mis à jour vers la dernière version avant que les mises à jour automatiques entrent en vigueur.

6. [Facultatif] Activez la fenêtre de maintenance.
La fenêtre par défaut est quotidienne, de 23 h 00 à 08 h 00 sur l'ordinateur où l'agent est installé.

© Acronis International GmbH, 2003-2026

Remarque
Bien que les processus de mise à jour des agents soient conçus pour être rapides et transparents, nous vous recommandons de choisir une fenêtre qui engendrera le moins de perturbation pour les utilisateurs. En effet, les utilisateurs ne peuvent pas empêcher ni reporter les mises à jour automatiques.

7. Cliquez sur **Enregistrer**.

Surveillance de l'état de la mise à jour automatique

Vérifier le statut de mise à jour automatique

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis assurez-vous que la case **Mise à jour automatique** est cochée.
3. Consultez le statut qui s'affiche dans la colonne **Mise à jour automatique**.

Suppression des paramètres de mise à jour automatique

Important
Pour garantir le bon fonctionnement et la protection efficace de vos ressources, nous recommandons de ne pas désactiver les mises à jour automatiques des agents de protection.

Supprimer les paramètres de mise à jour automatique personnalisés

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionner la portée des paramètres :
   - Pour supprimer les paramètres personnalisés pour tous les ordinateurs, cliquez sur **Modifier les paramètres de mise à jour d'agent par défaut**.
   - Pour supprimer les paramètres pour des ordinateurs spécifiques, sélectionnez les ordinateurs souhaités, puis cliquez sur **Paramètres de mise à jour d'agent**.
3. Cliquez sur **Réinitialiser les paramètres par défaut**, puis sur **Enregistrer**.

Mise à jour des agents de protection sur les ressources chiffrées par BitLocker

Les mises à jour d'agents qui introduisent des changements sur Startup Recovery Manager interfèrent avec BitLocker sur les ressources sur lesquelles BitLocker et Startup Recovery Manager sont activés. Dans ce cas, après un redémarrage, la clé de restauration BitLocker est requise. Pour atténuer ce problème, suspendez ou désactivez BitLocker avant de mettre à jour l'agent.

Versions de l'agent concernées :

- 23.12.36943, sortie en décembre 2023
- 25.01.XXXXX publiée en janvier 2025

© Acronis International GmbH, 2003-2026

- 25.03.XXXXX publié en mars 2025

Vous pouvez également vérifier dans les notes de publication de l'agent de protection si la mise à jour apporte des modifications à Startup Recovery Manager.

Pour mettre à jour l'agent sur une ressource avec BitLocker et Startup Recovery Manager activés

1. Sur la ressource sur laquelle vous voulez mettre à jour l'agent, suspendez ou désactivez BitLocker.
2. Mettre à jour l'agent.
3. Redémarrez la ressource.
4. Activer BitLocker.

Déploiement d'agents de protection via la stratégie de groupe

Vous pouvez installer (ou déployer) de manière centralisée l'agent pour Windows sur des ordinateurs membres d'un domaine Active Directory à l'aide de la stratégie de groupe de Windows.

Dans cette section, vous apprendrez comment configurer un objet de stratégie de groupe pour déployer des agents sur les machines d'un domaine entier ou dans son unité organisationnelle.

Chaque fois qu'une machine se connecte au domaine, l'objet de stratégie de groupe obtenu garantit que l'agent est installé et enregistré.

Prérequis

- Domaine Active Directory avec contrôleur de domaine exécutant Microsoft Windows Server 2003 ou une version ultérieure.
- Vous devez être membre du groupe **Admins du domaine** dans ce domaine.
- Vous avez téléchargé le programme d'installation **Tous les agents pour Windows**.
  Pour télécharger le Pour télécharger le programme d'installation, cliquez dans la console Cyber Protect sur l'icône de compte en haut à droite, puis sur **Téléchargements**. Le lien de téléchargement est également disponible dans le panneau **Ajouter des terminaux**.

Pour déployer des agents via la stratégie de groupe

1. Générez un jeton d'enregistrement en suivant les indications de "Génération d'un jeton d'enregistrement" (p. 112).
2. Créez le fichier .mst, le fichier .msi et les fichiers .cab en suivant les indications de "Création du fichier de transformation et extraction des packages d'installation" (p. 136).
3. Configurez l'objet de stratégie de groupe en suivant les indications de "Configuration de l'objet de stratégie de groupe" (p. 137).

© Acronis International GmbH, 2003-2026

Création du fichier de transformation et extraction des packages d'installation

Pour déployer des agents de protection via la stratégie de groupe de Windows, vous avez besoin d'un fichier de transformation (.mst) et des packages d'installation (fichiers .msi et .cab).

Remarque
La procédure ci-dessous utilise l'option d'inscription par défaut, c'est-à-dire l'inscription par jeton. Pour en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Génération d'un jeton d'enregistrement" (p. 112).

Pour créer le fichier .mst et extraire les packages d'installation (fichiers .msi et .cab)

1. Connectez-vous en tant qu'administrateur sur n'importe quel ordinateur du domaine Active Directory.
2. Créez un dossier partagé contenant les paquets d'installation. Assurez-vous que les utilisateurs du domaine peuvent accéder au dossier partagé — par exemple, en laissant les paramètres de partage par défaut sur **Tout le monde**.
3. Exécutez le programme d'installation de l'agent.
4. Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
5. Dans **Que faut-il installer**, sélectionnez les composants que vous souhaitez inclure dans l'installation, puis cliquez sur **Terminé**.
6. Dans **Paramètres d'Inscription**, cliquez sur **Spécifier**, saisissez un jeton d'enregistrement, puis acliquez sur **Terminé**.

   Vous pouvez modifier la méthode d'inscription en passant de **Utiliser un jeton d'enregistrement** (par défaut) à **Utiliser les identifiants** ou à **Ignorer l'inscription**. L'option **Ignorer l'inscription** suppose que vous enregistrerez manuellement les ressources ultérieurement.
7. Vérifiez ou modifiez les paramètres d'installation qui seront ajoutés au fichier .mst, puis cliquez sur **Poursuivre**.
8. Dans **Enregistrer les fichiers dans**, spécifiez le chemin d'accès au dossier partagé que vous avez créé.
9. Cliquez sur **Générer**.

Le fichier .mst, le fichier .msi et les fichiers .cab sont créés et copiés dans le dossier partagé que vous avez spécifié.

Configurez ensuite l'objet de stratégie de groupe Windows. Pour savoir comment procéder, voir "Configuration de l'objet de stratégie de groupe" (p. 137).

© Acronis International GmbH, 2003-2026

Configuration de l'objet de stratégie de groupe

Dans cette procédure, vous utilisez les packages d'installation que vous avez créés dans "Création du fichier de transformation et extraction des packages d'installation" (p. 136) pour configurer un objet de stratégie de groupe (GPO). L'objet de stratégie de groupe déploiera les agents sur les ordinateurs de votre domaine.

Pour configurer l'objet de stratégie de groupe

1. Connectez-vous au contrôleur de domaine en tant qu'administrateur de domaine.
   Si le domaine possède plusieurs contrôleurs de domaine, connectez-vous à l'un d'eux en tant qu'administrateur de domaine.
2. [Si vous déployez des agents dans une unité d'organisation] Assurez-vous que l'unité d'organisation dans laquelle vous souhaitez déployer les agents existe dans ce domaine.
3. Dans le menu **Démarrer** de Windows, pointez sur **Outils d'administration**, puis cliquez sur **Gestion des stratégies de groupe** (ou **Utilisateurs et ordinateurs Active Directory** sous Windows Server 2003).
4. [Pour Windows Server 2008 ou versions ultérieures] Cliquez avec le bouton droit sur le nom du domaine ou de l'unité d'organisation, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.
5. [Pour Windows Server 2003] Cliquez avec le bouton droit sur le nom du domaine ou de l'unité d'organisation, puis cliquez sur **Propriétés**. Dans la boîte de dialogue, cliquez sur l'onglet **Stratégie de groupe**, puis cliquez sur **Nouvelle**.
6. Nommez le nouvel objet de la Stratégie de groupe **Agent pour Windows.**
7. Ouvrez l'objet de stratégie de groupe **Agent pour Windows** pour le modifier :
   - [Dans Windows Server 2008 ou versions ultérieures] Sous **Objets de stratégie de groupe**, cliquez avec le bouton droit sur l'objet stratégie de groupe, puis cliquez sur **Modifier**.
   - [Dans Windows Server 2003], cliquez sur l'objet de stratégie de groupe, puis cliquez sur **Modifier**.
8. Dans le composant logiciel enfichable de l'Editeur d'objet Stratégie de groupe, développez **Configuration de l'ordinateur**.
9. [Pour Windows Server 2012 ou versions ultérieures] Développez **Stratégies** > **Paramètres du logiciel**.
10. [Pour Windows Server 2003 et Windows Server 2008] Développez **Paramètres du logiciel**.
11. Cliquez avec le bouton droit sur **Installation du logiciel**, pointez sur **Nouveau**, puis cliquez sur **Package**.
12. Sélectionnez le package .msi d'installation de l'agent dans le dossier partagé que vous avez créé, puis cliquez sur **Ouvrir**.
13. Dans la boîte de dialogue **Déployer le logiciel**, cliquez sur **Avancées**, puis sur **OK**.
14. Dans l'onglet **Modifications**, cliquez sur **Ajouter**, puis sélectionnez le fichier .mst dans le dossier

© Acronis International GmbH, 2003-2026

partagé que vous avez créé.

15. Cliquez sur **OK** pour fermer la boîte de dialogue **Déployer le logiciel**.

Déploiement d'appliances virtuelles

Déploiement de l'agent pour VMware (appliance virtuelle)

Avant de commencer

Configuration système requise pour l'agent

Par défaut, 4 Go de RAM et 2 vCPU sont attribués à l'appliance virtuelle, ce qui est optimal et suffisant pour la plupart des opérations.

Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 16 Go de RAM et 4 vCPU dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

Les propres disques virtuels de l'appliance n'occupent pas plus de 6 Go de stockage. Le format du disque (dynamique ou statique) n'a pas d'importance et n'affecte pas les performances du matériel.

De combien d'agents ai-je besoin ?

Même si une appliance virtuelle est capable de protéger un environnement vSphere tout entier, une bonne pratique consiste à déployer une appliance virtuelle par cluster vSphere (ou par hôte s'il n'y a pas de clusters). Cela rend les sauvegardes plus rapides, car le matériel peut attacher les disques sauvegardés via le transport HotAdd. Par conséquent, le trafic de sauvegarde est dirigé d'un disque local à l'autre.

Il est normal d'utiliser simultanément l'appliance virtuelle et l'agent pour VMware (Windows), à condition qu'ils soient connectés au même vCenter Server *ou* qu'ils soient connectés à des hôtes ESXi différents. Évitez les situations pendant lesquelles un agent est connecté directement à un ESXi et un autre agent est connecté au vCenter Server qui gère ce même ESXi.

Si vous avez plusieurs agents, nous vous déconseillons d'utiliser un stockage attaché localement (c.-à-d. de stocker des sauvegardes sur des disques virtuels ajoutés à l'appliance virtuelle). Pour plus d'informations importantes à prendre en compte, voir "Utilisation d'un stockage localement connecté" (p. 970).

Désactiver le planificateur de ressources partagées (PRP) automatique pour l'agent

Si l'appliance virtuelle est déployée sur un cluster vSphere, veillez à désactiver le vMotion automatique pour celle-ci. Dans les paramètres RPR du cluster, activez des niveaux

© Acronis International GmbH, 2003-2026

d'automatisation de machine virtuelle individuels, puis définissez **Niveau d'automatisation** de l'appliance virtuelle sur **Désactivé**.

Déploiement du modèle OVF

1. Cliquez sur **Tous les terminaux** > **Ajouter** > **Broadcom (VMware) ESXi** > **Appliance virtuelle (OVF)**.
   L'archive ZIP est téléchargée sur votre machine.
2. Décompressez l'archive ZIP. Le dossier contient un fichier .ovf et trois fichiers .vmdk.
3. Assurez-vous que ces fichiers sont accessibles à partir de la machine exécutant vSphere Client.
4. Lancez vSphere Client et connectez-vous à vCenter Server.
5. Déployez le modèle OVF.
   - Lors de la configuration du stockage, sélectionnez le magasin de données partagé, s'il existe. Le format du disque (dynamique ou statique) n'a pas d'importance et n'affecte pas les performances du matériel.
   - Lors de la configuration de connexions réseau, assurez-vous de sélectionner un réseau qui autorise une connexion Internet, afin que l'agent puisse s'enregistrer correctement dans le Cloud.

Configuration de l'appliance virtuelle

Après avoir déployé l'appliance virtuelle, vous devez la configurer afin qu'elle puisse accéder à vCenter Server ou à l'hôte ESXi, ainsi qu'au service Cyber Protection.

Pour configurer l'appliance virtuelle

1. Dans vSphere Client, ouvrez la console de l'appliance virtuelle.
2. Vérifiez que la connexion réseau est configurée.
   La connexion est configurée automatiquement par l'intermédiaire du protocole DHCP (Dynamic Host Configuration Protocol).
   Pour modifier la configuration par défaut, sous **Options de l'agent**, dans le champ **eth0**, cliquez sur **Modifier** et spécifiez les paramètres réseau.
3. Connectez l'appliance virtuelle à vCenter Server ou à l'hôte ESXi.
   a. Sous **Options de l'agent**, dans le champ **vCenter/ESX(i)**, cliquez sur **Modifier** et spécifiez les informations suivantes.
      - [Si vous utilisez vCenter Server] Nom ou adresse IP de vCenter Server.
      - [Si vous n'utilisez pas vCenter Server] Nom ou adresse IP de l'hôte ESXi sur lequel vous souhaitez sauvegarder et restaurer les machines virtuelles. Pour accélérer les sauvegardes, déployez l'appliance virtuelle sur le même hôte.
      - Identifiants requis pour que l'appliance se connecte à vCenter Server ou à l'hôte ESXi.
        Nous vous recommandons d'utiliser un compte dédié pour accéder à vCenter Server ou à l'hôte ESXi, plutôt que d'utiliser un compte existant avec le rôle d'administrateur. Pour plus d'informations, voir "Privilèges requis pour l'agent pour VMware" (p. 977).

© Acronis International GmbH, 2003-2026

b. Cliquez sur **Vérifier la connexion** pour vous assurer que les paramètres sont corrects.

c. Cliquez sur **OK**.

(missing or bad snippet)

4. [Facultatif] Ajoutez un stockage de sauvegarde local à l'appliance virtuelle.

   a. Dans votre environnement de machine virtuelle, sélectionnez l'appliance virtuelle, puis ouvrez ses paramètres pour les modifier.

   b. Ajoutez un nouveau disque dur à l'appliance virtuelle.

      La taille du disque doit être d'au moins 10 Go.

      Avertissement !
      Si vous utilisez un disque qui contient des données, les données seront supprimées.

   c. Dans votre environnement de machine virtuelle, ouvrez la console de l'appliance virtuelle.

   d. Sous **Stockages locaux**, cliquez sur **Actualiser**.

      Le bouton **Créer un stockage** devient actif.

   e. Cliquez sur **Créer un stockage**, puis sélectionnez le disque que vous avez ajouté à l'appliance virtuelle.

      - Sélectionnez une lettre de lecteur.
      - [Facultatif] Spécifiez une étiquette de disque.

        La longueur du nom est limitée à 16 caractères à cause des limites du système de fichiers.

   f. Cliquez sur **OK**.

   g. Cliquez sur **Oui**.

5. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.

   a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.

   b. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.

   c. Localisez la section **env** ou créez-la et ajoutez les lignes suivantes :

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

   d. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

   e. Exécutez la commande `reboot`.

© Acronis International GmbH, 2003-2026

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Déploiement de l'agent pour Scale Computing HC3 (appliance virtuelle)

Avant de commencer

Cette appliance est une machine virtuelle préconfigurée que vous déployez dans un cluster Scale Computing HC3. Elle contient un agent de protection qui vous permet d'administrer la cyberprotection pour toutes les machines virtuelles du cluster.

Configuration système requise pour l'agent

Par défaut, la machine virtuelle avec l'agent utilise 2 vCPU et 4 Gio de RAM. Ces paramètres sont suffisants pour la plupart des opérations, mais vous pouvez les modifier en éditant la machine virtuelle dans l'interface web Scale Computing HC3.

Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 4 vCPU et 8 Gio de RAM dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

La taille du disque virtuel de l'appliance est d'environ 9 Gio.

De combien d'agents ai-je besoin ?

Un seul agent peut protéger l'intégralité du cluster. Vous pouvez cependant avoir plus d'un agent dans le cluster si vous devez distribuer la bande passante du trafic de sauvegarde.

Si vous avez plus d'un agent dans un cluster, les machines virtuelles sont automatiquement distribuées de manière égale entre les agents, afin que chacun d'entre eux gère un nombre similaire de machines.

La redistribution automatique a lieu lorsque le déséquilibre de charge entre les agents atteint 20 %. Cela peut se produire, par exemple, lorsque vous ajoutez ou supprimez une machine ou un agent.

© Acronis International GmbH, 2003-2026

Par exemple, vous réalisez que vous avez besoin de plus d'agents pour prendre en charge le débit et vous déployez une appliance virtuelle supplémentaire dans le cluster. Le serveur de gestion assignera les machines les plus appropriées au nouvel agent. La charge des anciens agents sera réduite. Lorsque vous supprimez un agent du serveur de gestion, les machines assignées à l'agent sont redistribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement du cluster Scale Computing HC3. La redistribution démarrera seulement après que vous avez supprimé cet agent de la console Cyber Protect.

Pour vérifier quel agent gère une machine spécifique

1. Dans la console Cyber Protect, cliquez sur **Terminaux**, puis sélectionnez **Scale Computing**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis, sous **Système** cochez la case **Agent**.
3. Cochez le nom de l'agent dans la colonne qui apparaît.

Déploiement du modèle QCOW2

1. Connectez-vous à votre compte Cyber Protection.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Scale Computing HyperCore**. L'archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP, puis enregistrez le fichier .qcow2 et le fichier .xml dans un dossier appelé **ScaleAppliance**.
4. Transférez le dossier **ScaleAppliance** vers un partage réseau, puis assurez-vous que le cluster Scale Computing HC3 peut y accéder.
5. Connectez-vous au cluster Scale Computing HC3 en tant qu'administrateur disposant du rôle **Création/Modification de MV**. Pour plus d'informations sur les rôles requis pour les opérations avec les machines virtuelles Scale Computing HC3, reportez-vous à "Agent pour Scale Computing HC3 – Rôles requis" (p. 145).
6. Dans l'interface web de Scale Computing HC3, importez le modèle de machine virtuelle depuis le dossier **ScaleAppliance**.
   a. Cliquez sur l'icône **Importer MV HC3**.
   b. Dans la fenêtre **Importer MV HC3**, indiquez les informations suivantes :
      - Un nom pour la nouvelle machine virtuelle.
      - Le partage réseau sur lequel se trouve le dossier **ScaleAppliance**.
      - Le nom d'utilisateur et le mot de passe requis pour accéder à ce partage réseau.
      - [Facultatif] Un libellé de domaine pour la nouvelle machine virtuelle.
      - Le chemin d'accès au dossier **ScaleAppliance** sur le partage réseau.
   c. Cliquez sur **Importer**.

Une fois le déploiement terminé, vous devez configurer l'appliance virtuelle. Pour en savoir plus sur sa configuration, reportez-vous à "Configuration de l'appliance virtuelle" (p. 143).

© Acronis International GmbH, 2003-2026

Remarque
Si vous avez besoin de plus d'une appliance virtuelle dans votre cluster, répétez les étapes ci-dessus et déployez d'autres appliances virtuelles. Ne clonez pas une appliance virtuelle existante à l'aide de l'option **Cloner MV** dans l'interface web de Scale Computing HC3.

Configuration de l'appliance virtuelle

Après avoir déployé l'appliance virtuelle, vous devez la configurer afin qu'elle puisse atteindre aussi bien le cluster Scale Computing HC3 qu'elle protégera que le service Cyber Protection.

Pour configurer l'appliance virtuelle

1. Connectez-vous à votre compte Scale Computing HC3.
2. Sélectionnez l'appliance virtuelle que vous souhaitez configurer, puis cliquez sur l'icône **Console**.
3. Dans le champ **eth0**, configurez les interfaces réseau de l'appliance.
   Assurez-vous que les adresses DHCP attribuées automatiquement (s'il y en a) sont valides au sein des réseaux que votre machine virtuelle utilise, ou attribuez-les manuellement. Selon le nombre de réseaux que l'appliance utilise, vous aurez peut-être une ou plusieurs interfaces à configurer.
4. Dans le champ **Scale Computing**, cliquez sur **Modifier** pour indiquer l'adresse et les identifiants du cluster Scale Computing HC3 afin d'y accéder.
   a. Dans le champ **Nom/IP du serveur**, entrez le nom DNS ou l'adresse IP du cluster.
   b. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants du compte administrateur Scale Computing HC3.
      Assurez-vous que ce compte administrateur dispose des rôles requis pour effectuer des opérations avec des machines virtuelles Scale Computing HC3. Pour plus d'informations sur ces rôles, reportez-vous à "Agent pour Scale Computing HC3 – Rôles requis" (p. 145).
   c. Cliquez sur **Vérifier la connexion** pour vous assurer que les paramètres sont corrects.
   d. Cliquez sur **OK**.
   (missing or bad snippet)
5. [Facultatif] Dans le champ **Nom**, cliquez sur **Modifier** pour modifier le nom par défaut de l'appliance virtuelle, qui est **localhost**. Ce nom s'affiche dans la console Cyber Protect.
6. [Facultatif] Dans le champ **Heure**, cliquez sur **Modifier**, puis sélectionnez le fuseau horaire de votre emplacement afin de vous assurer que les opérations planifiées sont exécutées au bon moment.
7. [Facultatif] Ajoutez un stockage de sauvegarde local à l'appliance virtuelle.
   a. Dans votre environnement de machine virtuelle, sélectionnez l'appliance virtuelle, puis ouvrez ses paramètres pour les modifier.
   b. Ajoutez un nouveau disque dur à l'appliance virtuelle.
      La taille du disque doit être d'au moins 10 Go.

© Acronis International GmbH, 2003-2026

Avertissement !
Si vous utilisez un disque qui contient des données, les données seront supprimées.

c. Dans votre environnement de machine virtuelle, ouvrez la console de l'appliance virtuelle.

d. Sous **Stockages locaux**, cliquez sur **Actualiser**.
Le bouton **Créer un stockage** devient actif.

e. Cliquez sur **Créer un stockage**, puis sélectionnez le disque que vous avez ajouté à l'appliance virtuelle.
- Sélectionnez une lettre de lecteur.
- [Facultatif] Spécifiez une étiquette de disque.
  La longueur du nom est limitée à 16 caractères à cause des limites du système de fichiers.

f. Cliquez sur **OK**.

g. Cliquez sur **Oui**.

8. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.

a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.

b. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.

c. Localisez la section **env** ou créez-la et ajoutez les lignes suivantes :

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

d. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

e. Exécutez la commande `reboot`.

Remarque
Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pour protéger des machines virtuelles dans le cluster Scale Computing HC3

1. Connectez-vous à votre compte Cyber Protection.
2. Accédez à **Terminaux** > **Scale Computing HyperCore** > <your cluster>, ou recherchez vos

© Acronis International GmbH, 2003-2026

ordinateurs dans **Terminaux** > **Tous les terminaux**.

3. Sélectionnez les ordinateurs et appliquez-leur un plan de protection.

Agent pour Scale Computing HC3 – Rôles requis

Cette section décrit les rôles nécessaires pour les opérations avec les machines virtuelles Scale Computing HC3.

Opération	Rôle
Sauvegarder une machine virtuelle	Sauvegarde Création/Modification de MV Suppression de MV
Restaurer sur une machine virtuelle existante	Sauvegarde Création/Modification de MV Contrôle de l'alimentation des MV Suppression de MV Paramètres de cluster
Récupérer sur une nouvelle machine virtuelle	Sauvegarde Création/Modification de MV Contrôle de l'alimentation des MV Suppression de MV Paramètres de cluster

Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)

Avant de commencer

Cette appliance est une machine virtuelle préconfigurée que vous déployez dans Virtuozzo Hybrid Infrastructure. Elle contient un agent de protection qui vous permet d'administrer la cyber protection pour toutes les machines virtuelles d'un cluster Virtuozzo Hybrid Infrastructure.

Remarque
Pour vous assurer que les sauvegardes sur lesquelles l'option de sauvegarde **Service de cliché instantané des volumes (VSS) pour les machines virtuelles** est activée s'exécutent correctement et capturent les données dans un état cohérent avec les applications, vérifiez que les outils invités de Virtuozzo sont installés et à jour sur les machines virtuelles protégées.

© Acronis International GmbH, 2003-2026

Configuration système requise pour l'agent

Lorsque vous déployez l'appliance virtuelle, vous pouvez choisir parmi différentes combinaisons prédéfinies de vCPUs et RAM (variétés). Vous pouvez également créer vos propres variétés.

2 vCPU et 4 Go de RAM (variété moyenne) sont optimaux et suffisants pour la plupart des opérations. Pour améliorer les performances de sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, nous vous recommandons d'augmenter ces ressources à 4 vCPU et 8 Go de RAM dans les situations les plus exigeantes. Par exemple, augmentez les ressources affectées lorsque vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Go ou plus).

De combien d'agents ai-je besoin ?

Un seul agent peut protéger l'intégralité du cluster. Vous pouvez cependant avoir plus d'un agent dans le cluster si vous devez distribuer la bande passante du trafic de sauvegarde.

Si vous avez plus d'un agent dans un cluster, les machines virtuelles sont automatiquement distribuées de manière égale entre les agents, afin que chacun d'entre eux gère un nombre similaire de machines.

La redistribution automatique a lieu lorsque le déséquilibre de charge entre les agents atteint 20 %. Cela peut se produire, par exemple, lorsque vous ajoutez ou supprimez une machine ou un agent. Par exemple, vous réalisez que vous avez besoin de plus d'agents pour prendre en charge le débit et vous déployez une appliance virtuelle supplémentaire dans le cluster. Le serveur de gestion assignera les machines les plus appropriées au nouvel agent. La charge des anciens agents sera réduite. Lorsque vous supprimez un agent du serveur de gestion, les machines assignées à l'agent sont redistribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement du nœud de Virtuozzo Hybrid Infrastructure. La redistribution démarrera seulement après que vous avez supprimé cet agent de l'interface Web Cyber Protection.

Pour vérifier quel agent gère une machine spécifique

1. Dans la console Cyber Protect, cliquez sur **Terminaux**, puis sélectionnez **Virtuozzo Hybrid Infrastructure**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis, sous **Système** cochez la case **Agent**.
3. Cochez le nom de l'agent dans la colonne qui apparaît.

Limites

- L'appliance de Virtuozzo Hybrid Infrastructure ne peut pas être déployée à distance.
- La sauvegarde reconnaissant les applications des machines virtuelles n'est pas prise en charge.

© Acronis International GmbH, 2003-2026

Configurations de réseaux dans Virtuozzo Hybrid Infrastructure

Avant de déployer et de configurer l'appliance virtuelle, vous devez avoir configuré vos réseaux dans Virtuozzo Hybrid Infrastructure.

Configuration réseau requise pour Agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)

- L'appliance virtuelle nécessite deux adaptateurs réseau.
- L'appliance virtuelle doit être connecté aux réseaux Virtuozzo avec les types de trafic réseau suivants :
  - API de calcul
  - Sauvegarde de MV
  - ABGW Public
  - MV publique

Pour plus d'informations sur la configuration des réseaux, voir Exigences relatives au cluster de calcul dans la documentation Virtuozzo.

Configurations de comptes utilisateur dans Virtuozzo Hybrid Infrastructure

Pour configurer l'appliance virtuelle, vous avez besoin d'un compte utilisateur Virtuozzo Hybrid Infrastructure.

Vous pouvez utiliser l'un des comptes suivants :

- Administrateur système (dans le domaine **Par défaut** ou dans un autre domaine)

  Assurez-vous d'accorder à ce compte l'accès à tous les projets du domaine sélectionné. Ainsi, l'appliance virtuelle pourra sauvegarder et restaurer toutes les machines virtuelles de tous les projets enfants du domaine sélectionné.
- Administrateur de projet

  Avec ce compte, l'appliance virtuelle ne pourra sauvegarder et restaurer que les machines virtuelles du projet dans lequel le compte est créé. Aucune information sur les autres projets du domaine ne sera disponible pour l'appliance virtuelle.

  Remarque

  Si vous souhaitez protéger plusieurs projets, vous devez déployer une appliance virtuelle distincte pour chaque projet.

  Chaque appliance virtuelle doit utiliser un compte d'administrateur de projet distinct qui est créé dans le projet correspondant. L'appliance peut être déployée n'importe où dans le cluster Virtuozzo Hybrid Infrastructure, même en dehors du projet protégé.

  Vous ne pouvez utiliser le compte d'administrateur de projet qu'avec Virtuozzo Hybrid Infrastructure 6.2 et les versions ultérieures.

© Acronis International GmbH, 2003-2026

Pour plus d'informations sur les domaines et les projets, consultez la section relatvie à la gestion multitenant dans la documentation de Virtuozzo Hybrid Infrastructure.

Utilisation d'un compte d'administrateur système

Avec le compte d'administrateur système, l'appliance virtuelle peut sauvegarder et restaurer toutes les machines virtuelles dans le domaine de Virtuozzo Hybrid Infrastructure.

Pour plus d'informations sur les domaines et les projets, consultez la section relatvie à la gestion multitenant dans la documentation de Virtuozzo Hybrid Infrastructure.

Prérequis

- Vous devez pouvoir vous connecter au cluster Virtuozzo Hybrid Infrastructure en utilisant l'interface de ligne de commande OpenStack. Pour plus d'informations, voir Connexion à l'interface de ligne de commande OpenStack dans la documentation Virtuozzo Hybrid Infrastructure.

Pour utiliser le compte d'administrateur système

1. Connectez-vous au cluster Virtuozzo Hybrid Infrastructure en utilisant l'interface de ligne de commande OpenStack, puis exécutez le script suivant pour créer un fichier d'environnement pour l'administrateur système.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Utilisez le fichier d'environnement pour autoriser davantage de commandes OpenStack.

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. Créez un compte d'administrateur dans le domaine **Par défaut**.

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <user name>
   ```

   `<user name>` est le compte Virtuozzo Hybrid Infrastructure. L'appliance virtuelle utilisera ce compte pour sauvegarder et restaurer les machines virtuelles dans n'importe quel projet enfant du domaine **Par défaut**.

4. Affectez le rôle `admin` au compte.

   ```
   openstack --insecure role add --domain Default --user <user name> --user-domain
   Default admin --inherited
   ```

5. [Facultatif] Autorisez le compte à accéder à d'autres domaines dans Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2026

```
openstack --insecure role add --domain <domain name> --inherited --user <user name> -
-user-domain Default admin
```

`<domain name>` est le domaine auquel ce compte aura accès. Si le nom de domaine contient des espaces, mettez-le entre guillemets.

Répétez cette étape pour chaque domaine supplémentaire que vous souhaitez rendre accessible.

6. Vérifiez les rôles affectés au compte.

```
openstack --insecure role assignment list --user <user name> --names
```

7. [Facultatif] Vérifiez les rôles effectifs du compte.

   Les rôles effectifs incluent les rôles affectés, hérités et implicites.

```
openstack --insecure role assignment list --user <user name> --names --effective
```

Exemples

Attribution de l'accès au domaine par défaut

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Attribution de l'accès au domaine par défaut et à un domaine supplémentaire

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
openstack --insecure role add --domain "New Domain"  --user johndoe --user-domain
Default admin --inherited
```

Vérification des rôles affectés

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
```


© Acronis International GmbH, 2003-2026

```
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | New Domain  |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

Dans cet exemple, les options `Rôle -c`, `Utilisateur -c`, `Projet -c` et `Domaine -c` servent à abréger la sortie de commande pour s'adapter à la page.

Vérification des rôles effectifs

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
```

```
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

Dans cet exemple, les options `Rôle -c`, `Utilisateur -c`, `Projet -c` et `Domaine -c` servent à abréger la sortie de commande pour s'adapter à la page.

Utilisation d'un compte d'administrateur de projet

Avec ce compte, l'appliance virtuelle ne pourra sauvegarder et restaurer que les machines virtuelles du projet dans lequel le compte est créé. Aucune information sur les autres projets du domaine ne sera disponible pour l'appliance virtuelle.

© Acronis International GmbH, 2003-2026

Remarque
Si vous souhaitez protéger plusieurs projets, vous devez déployer une appliance virtuelle distincte pour chaque projet.

Chaque appliance virtuelle doit utiliser un compte d'administrateur de projet distinct qui est créé dans le projet correspondant. L'appliance peut être déployée n'importe où dans le cluster Virtuozzo Hybrid Infrastructure, même en dehors du projet protégé.

Vous ne pouvez utiliser le compte d'administrateur de projet qu'avec Virtuozzo Hybrid Infrastructure 6.2 et les versions ultérieures.

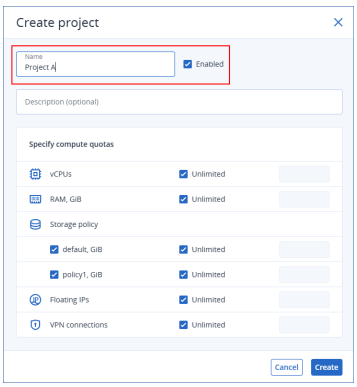
Pour plus d'informations sur les domaines et les projets, consultez la section relatvie à la gestion multitenant dans la documentation de Virtuozzo Hybrid Infrastructure.

Prérequis

- Vous devez pouvoir vous connecter au cluster Virtuozzo Hybrid Infrastructure en utilisant l'interface de ligne de commande OpenStack. Pour plus d'informations, voir Connexion à l'interface de ligne de commande OpenStack dans la documentation Virtuozzo Hybrid Infrastructure.

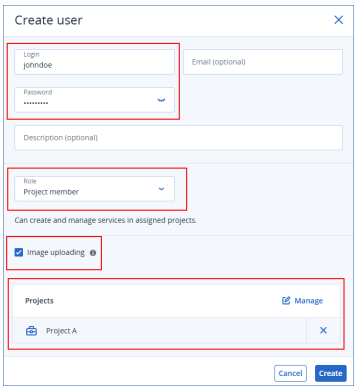
Pour utiliser le compte d'administrateur de projet

1. Dans le panneau d'administration de Virtuozzo Hybrid Infrastructure, accédez à **Paramètres** > **Projets et utilisateurs**.
2. Choisissez un domaine et créez un projet dans ce domaine.



3. Dans le même domaine, créez un compte utilisateur. Affectez le rôle **Membre du projet** à ce compte, cochez la case **Transfert d'image**, puis affectez l'utilisateur au projet que vous avez créé.

© Acronis International GmbH, 2003-2026



Remarque

Dans l'interface de ligne de commande, le rôle **Membre du projet** est appelé **project_admin**.

```
+---------------+------------------+-------+--------------------+--------+--------+-----------+
| Role          | User             | Group | Project            | Domain | System | Inherited |
+---------------+------------------+-------+--------------------+--------+--------+-----------+
| project_admin | johndoe@Domain A |       | Project A@Domain A |        |        | False     |
| image_upload  | johndoe@Domain A |       | Project A@Domain A |        |        | False     |
+---------------+------------------+-------+--------------------+--------+--------+-----------+
```

4. Connectez-vous au cluster Virtuozzo Hybrid Infrastructure en utilisant l'interface de ligne de commande OpenStack.
   a. Exécutez le script suivant pour créer un fichier d'environnement.

      ```
      su - vstoradmin
      kolla-ansible post-deploy
      exit
      ```

   b. Utilisez le fichier d'environnement pour autoriser davantage de commandes OpenStack.

      ```
      . /etc/kolla/admin-openrc.sh
      ```

   c. Affectez le rôle `compute` au compte utilisateur que vous avez créé dans le panneau d'administration.

      ```
      openstack --insecure role add --project <project name> --user <user name> --
      project-domain <project domain name> --user-domain <user domain name> compute
      ```

      `<project name>` est le nom du projet, `<user name>` est le compte Virtuozzo Hybrid Infrastructure, `<project domain name>` est le domaine parent du projet et `<user domain name>` est le domaine parent du compte utilisateur.

      Si un nom contient des espaces, mettez-le entre guillemets.

   d. Affectez le rôle `quota_manager` au compte.

      ```
      openstack --insecure role add --project <project name> --user <user name> --
      project-domain <project domain name> --user-domain <user domain name> quota_
      manager
      ```

   e. Vérifiez les rôles affectés au compte.

© Acronis International GmbH, 2003-2026

```
openstack --insecure role assignment list --names --user <user name> --user-domain
<user domain name>
```

f. [Facultatif] Vérifiez les rôles effectifs du compte.

Les rôles effectifs incluent les rôles affectés, hérités et implicites.

```
openstack --insecure role assignment list --names --effective  --user <user
name> --user-domain <user domain name>
```

Exemples

Dans les exemples, le compte utilisateur est `johndoe` et le projet est `Project A`. Le compte utilisateur et le projet sont créés dans `Domain A`.

Attribution de rôles

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure role add --project "Project A" --user johndoe --project-domain
"Domain A" --user-domain "Domain A" compute
openstack --insecure role add --project "Project A" --user johndoe --project-domain
"Domain A" --user-domain "Domain A" quota_manager
```

Vérification des rôles affectés

```
openstack --insecure role assignment list --names --user johndoe --user-domain "Domain
A" -c Role -c User -c Project -c Domain
```

```
+--------------+------------------+------------------+-------------+
| Role         | User             | Project          | Domain      |
+--------------+------------------+------------------+-------------+
| compute      | johndoe@Domain A | Project A@Domain A|             |
| project_admin| johndoe@Domain A | Project A@Domain A|             |
| image-upload | johndoe@Domain A | Project A@Domain A|             |
| quota_manager| johndoe@Domain A | Project A@Domain A|             |
+--------------+------------------+------------------+-------------+
```

Dans cet exemple, les options `Rôle -c`, `Utilisateur -c`, `Projet -c` et `Domaine -c` servent à abréger la sortie de commande pour s'adapter à la page.

Vérification des rôles effectifs

```
openstack --insecure role assignment list --names --effective  --user johndoe --user-
domain "Domain A"  -c Role -c User -c Project -c Domain
```


© Acronis International GmbH, 2003-2026

```
+--------------+-----------------+---------------------+---------+
| Role         | User            | Project             | Domain  |
+--------------+-----------------+---------------------+---------+
| compute      | johndoe@Domain A | Project A@Domain A |         |
| project_admin| johndoe@Domain A | Project A@Domain A |         |
| image_upload | johndoe@Domain A | Project A@Domain A |         |
| quota_manager| johndoe@Domain A | Project A@Domain A |         |
| project_user | johndoe@Domain A | Project A@Domain A |         |
| member       | johndoe@Domain A | Project A@Domain A |         |
| reader       | johndoe@Domain A | Project A@Domain A |         |
+--------------+-----------------+---------------------+---------+
```

Dans cet exemple, les options `Rôle -c`, `Utilisateur -c`, `Projet -c` et `Domaine -c` servent à abréger la sortie de commande pour s'adapter à la page.

Déploiement du modèle QCOW2

1. Connectez-vous à votre compte Cyber Protection.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Virtuozzo Hybrid Infrastructure**. L'archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP. Elle contient un fichier image .qcow2.
4. Connectez-vous à votre compte sur Virtuozzo Hybrid Infrastructure.
5. Ajoutez le fichier image .qcow2 au cluster de calcul de Virtuozzo Hybrid Infrastructure, comme suit :
   - Dans l'onglet **Calcul** > **Machines virtuelles** > **Images**, cliquez sur **Ajouter une image**.
   - Dans la fenêtre **Ajouter une image**, cliquez sur **Parcourir**, puis sélectionnez le fichier .qcow2.
   - Indiquez le nom de l'image, sélectionnez le type **OS Linux générique**, puis cliquez sur **Ajouter**.
6. Dans l'onglet **Calcul** > **Machines virtuelles** > **Machines virtuelles**, cliquez sur **Créer une machine virtuelle**. Une fenêtre s'ouvrira, dans laquelle vous devez indiquer les paramètres suivants :
   - Un nom pour la nouvelle machine virtuelle.
   - Dans **Déployer à partir de**, choisissez **Image**.
   - Dans la fenêtre **Images**, sélectionnez le fichier image .qcow2 de l'appliance, puis cliquez sur **Terminé**.
   - Dans la fenêtre **Volumes**, vous n'avez pas besoin d'ajouter de volumes. Le volume ajouté automatiquement pour le disque système est suffisant.
   - Dans la fenêtre **Variété**, choisissez votre combinaison souhaitée de vCPU et RAM, puis cliquez sur **Terminé**. 2 vCPU et 4 Go de RAM sont généralement suffisants.
   - Dans la fenêtre **Interfaces réseau**, cliquez sur **Ajouter**, sélectionnez le réseau virtuel de type *public*, puis cliquez sur **Ajouter**. Il apparaîtra dans la liste **Interfaces réseau**.
     Si vous utilisez une configuration possédant plus d'un réseau physique (et donc avec plus d'un

© Acronis International GmbH, 2003-2026

réseau virtuel de type public), répétez cette étape et sélectionnez les réseaux virtuels dont vous avez besoin.

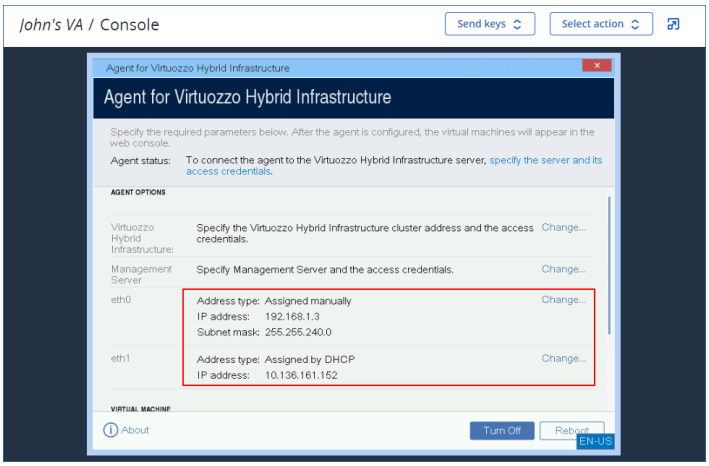
7. Cliquez sur **Terminé**.
8. De nouveau, dans la fenêtre **Créer une machine virtuelle**, cliquez sur **Déployer** pour créer et démarrer la machine virtuelle.

Configuration de l'appliance virtuelle

Après le déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle), vous devez configurer l'appliance virtuelle pour atteindre à la fois le cluster Virtuozzo Hybrid Infrastructure et le service cloud Cyber Protection.

Pour configurer l'appliance virtuelle

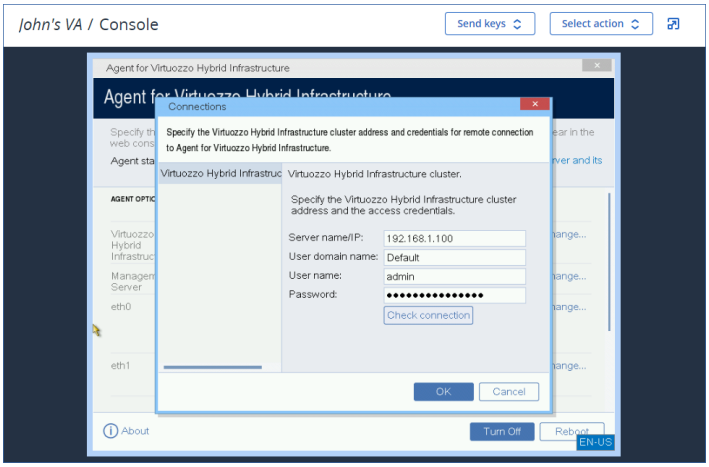
1. Connectez-vous au panneau en libre-service de Virtuozzo Hybrid Infrastructure.
2. Accédez à **Calcul** > **Machines virtuelles**, puis sélectionnez l'onglet **Machines virtuelles** dans le menu horizontal.
3. Cliquez sur l'icône représentant des pointillés (...) à côté de la machine virtuelle que vous avez créée, puis cliquez sur **Console**.
4. Configurez les interfaces réseau de l'appliance. Vous aurez peut-être une ou plusieurs interfaces à configurer, selon le nombre de réseaux virtuels que l'appliance utilise. Assurez-vous que les adresses DHCP attribuées automatiquement (le cas échéant) sont valides au sein des réseaux que votre machine virtuelle utilise, ou attribuez-les manuellement.



5. Indiquez l'adresse et les identifiants du cluster Virtuozzo.
   - Nom DNS ou adresse IP du cluster Virtuozzo Hybrid Infrastructure : il s'agit de l'adresse du nœud de gestion du cluster. Le port par défaut 5000 sera automatiquement configuré. Si vous utilisez un autre port, vous devez l'indiquer manuellement.
   - Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants du compte utilisateur de Virtuozzo Hybrid Infrastructure. Il peut s'agir d'un compte d'administrateur système ou d'administrateur de projet. Pour plus d'informations sur les utilisateurs, les rôles et les domaines, voir Configuration des comptes utilisateur dans Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2026

- Dans le champ **Nom de domaine de l'utilisateur**, indiquez le domaine parent du compte utilisateur. Par exemple, **Défaut**. Le nom de domaine est sensible à la casse.



(missing or bad snippet)

6. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.
   a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
   b. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.
   c. Localisez la section **env** ou créez-la et ajoutez les lignes suivantes :

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

   d. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.
   e. Exécutez la commande `reboot`.

Remarque
Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

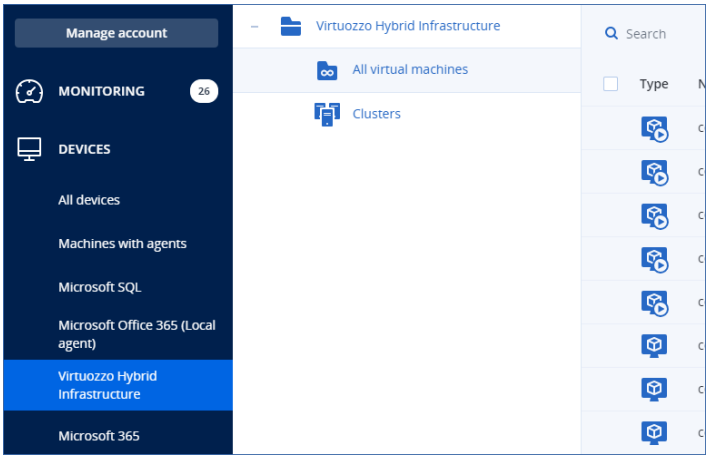
```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pour protéger les machines virtuelles du cluster de Virtuozzo Hybrid Infrastructure

1. Connectez-vous à la console Cyber Protection.
2. Accédez à **Terminaux** > **Virtuozzo Hybrid Infrastructure** > <your cluster> > **Projet par défaut** > **admin** ou recherchez vos ordinateurs dans **Terminaux** > **Tous les terminaux**.

© Acronis International GmbH, 2003-2026

3. Sélectionnez les ordinateurs et appliquez-leur un plan de protection.



Déploiement de l'agent pour oVirt (appliance virtuelle)

Avant de commencer

Cet appliance est une machine virtuelle préconfigurée que vous pouvez déployer dans un environnement Red Hat Virtualization/oVirt. Elle contient un agent de protection qui peut sauvegarder et restaurer les machines virtuelles de l'environnement.

Configuration système requise pour l'agent

Par défaut, l'appliance virtuelle utilise 2 vCPU et 4 Go de RAM. Ces paramètres sont suffisants pour la plupart des opérations.

Pour améliorer les performances de la sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, vous pouvez augmenter le nombre de vCPU et le faire passer à quatre et augmenter la mémoire RAM jusqu'à 8 Gio dans les situations les plus exigeantes. Par exemple, augmentez ces ressources si vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Gio ou plus).

La taille du disque virtuel de l'appliance est de 8 Gio.

De combien d'agents ai-je besoin ?

Une seule appliance virtuelle peut sauvegarder et restaurer toutes les machines virtuelles de l'environnement. Si vous souhaitez distribuer la charge de la bande passante du trafic de sauvegarde, vous pouvez utiliser plusieurs appliances virtuelles.

Si plusieurs appliances virtuelles sont déployées dans l'environnement, les machines virtuelles sauvegardées sont redistribuées automatiquement lorsque le déséquilibre de charge entre les appliances atteint 20 %.

Lorsque vous déployez un autre appliance virtuelle, le serveur de gestion affecte les machines virtuelles les plus appropriées à la nouvelle appliance et la charge de l'appliance existante diminue.

© Acronis International GmbH, 2003-2026

Lorsque vous supprimez un appliance virtuelle, les machines virtuelles sauvegardées sont redistribuées entre les appliances restantes. La redistribution se produit uniquement si vous supprimez l'appliance virtuelle de la console Cyber Protect. La redistribution ne démarrera pas si vous supprimez l'appliance virtuelle du portail d'administration Red Hat Virtualization/oVirt ou si l'appliance est corrompue.

Pour vérifier quel agent gère une machine spécifique

1. Dans la console Cyber Protect, cliquez sur **Terminaux**, puis sélectionnez **oVirt**.
2. Cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis, sous **Système** cochez la case **Agent**.
3. Cochez le nom de l'agent dans la colonne qui apparaît.

Limites

Les opérations suivantes ne sont pas prises en charge pour les machines virtuelles Red Hat Virtualization/oVirt.

- Sauvegarde reconnaissant les applications
- Exécution d'une machine virtuelle à partir d'une sauvegarde
- Réplication de machines virtuelles
- Suivi des blocs modifiés

Déploiement du modèle OVA

Vous pouvez déployer l'appliance virtuelle oVirt en créant une machine virtuelle dans l'environnement Red Hat Virtualization/oVirt et en déployant le modèle QCOW que vous téléchargez à partir de la console Cyber Protect.

Si vous avez besoin de plusieurs appliances virtuelles dans votre environnement, déployez d'autres appliances virtuelles. Ne clonez pas une appliance virtuelle existante à l'aide de l'option **Cloner MV** dans le portail d'administration Red Hat Virtualization/oVirt.

Pour déployer le modèle OVA

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Red Hat Virtualization (oVirt)**.
   Une archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP et extrayez le fichier image OVA.
4. Transférez le fichier OVA vers un hôte dans l'environnement Red Hat Virtualization/oVirt que vous souhaitez protéger.
5. Connectez-vous au portail d'administration Red Hat Virtualization/oVirt en tant qu'administrateur. Pour plus d'informations sur les rôles requis pour les opérations avec les machines virtuelles, reportez-vous à "Agent pour oVirt - Rôles et ports requis" (p. 162).
6. Dans le menu de navigation, sélectionnez **Calcul** > **Machines virtuelles**.

© Acronis International GmbH, 2003-2026

7. Cliquez sur l'icône représentant trois points verticaux  au-dessus du tableau principal, puis cliquez sur **Importer**.
8. Dans la fenêtre **Importer machine(s) virtuelle(s)**, procédez comme suit :
   a. Dans **Centre de données**, sélectionnez le centre de données que vous souhaitez protéger.
   b. Dans **Source**, sélectionnez **Appliance virtuelle (OVA)**.
   c. Dans **Hôte**, sélectionnez l'hôte sur lequel vous avez transféré le fichier OVA.
   d. Dans **Chemin d'accès au fichier**, indiquez le chemin d'accès au répertoire qui contient le fichier OVA.
   e. Cliquez sur **Charger**.
      Le modèle d'appliance virtuelle oVirt du fichier OVA apparaît dans le panneau **Machines virtuelles dans la source**.
      Si le modèle n'apparaît pas dans ce panneau, assurez-vous que vous avez indiqué le bon chemin d'accès au fichier, que le fichier n'est pas endommagé et qu'il est possible d'accéder à l'hôte.
   f. Dans **Machines virtuelles dans la source**, sélectionnez le modèle d'appliance virtuelle oVirt, puis cliquez sur la flèche de droite.
      Le modèle apparaît dans le panneau **Machines virtuelles à importer**.
   g. Cliquez sur **Suivant**.
9. Dans la nouvelle fenêtre, cliquez sur le nom de l'appliance, puis configurez les paramètres suivants :
   - Dans l'onglet **Interfaces réseau**, configurez les interfaces réseau.
   - Dans l'onglet **Général**, modifiez le nom par défaut de la machine virtuelle avec l'agent
10. [Facultatif] Pour masquer l'appliance virtuelle dans la console Cyber Protect, attribuez la balise `acronis_virtual_appliance` à l'appliance virtuelle.
    Cela évitera que vous appliquiez accidentellement des plans de protection à l'appliance proprement dite et que vous les incluyez dans des groupes dynamiques.

Le déploiement est maintenant terminé. Vous devez ensuite configurer l'appliance. Voir "Configuration de l'appliance virtuelle" (p. 160).

Remarque
Si vous utilisez une appliance virtuelle oVirt avec Oracle Linux Virtualization Manager, vous pourriez recevoir l'erreur suivante : « La machine virtuelle <name of the virtual appliance> est arrêtée avec une erreur. Message de résultat : configuration non prise en charge : la configuration du domaine ne prend pas en charge le modèle vidéo qxl. » Pour résoudre cette erreur, changez l'adaptateur graphique de l'appliance virtuelle et sélectionnez un adaptateur **CIRRUS**. Voir "Modification de l'adaptateur graphique d'une appliance virtuelle" (p. 161).

© Acronis International GmbH, 2003-2026

Configuration de l'appliance virtuelle

Après avoir déployé l'appliance virtuelle, vous devez la configurer afin qu'elle puisse atteindre aussi bien l'oVirt Engine que le service Cyber Protection.

Pour configurer l'appliance virtuelle

1. Connectez-vous au portail d'administration Red Hat Virtualization/oVirt.
2. Sélectionnez l'appliance virtuelle que vous souhaitez configurer, puis cliquez sur l'icône **Console**.
3. Dans le champ **eth0**, configurez les interfaces réseau de l'appliance.
   Assurez-vous que les adresses DHCP attribuées automatiquement (s'il y en a) sont valides au sein des réseaux que votre machine virtuelle utilise, ou attribuez-les manuellement. Selon le nombre de réseaux que l'appliance utilise, vous aurez peut-être une ou plusieurs interfaces à configurer.
4. Dans le champ **oVirt**, cliquez sur **Modifier** pour indiquer l'adresse et les identifiants d'oVirt Engine afin d'y accéder :
   a. Dans le champ **Nom/IP du serveur**, entrez le nom DNS ou l'adresse IP du moteur.
   b. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants d'administrateur pour ce moteur.
      Assurez-vous que ce compte administrateur dispose des rôles requis pour effectuer des opérations avec des machines virtuelles Red Hat Virtualization/oVirt. Pour plus d'informations sur ces rôles, reportez-vous à "Agent pour oVirt - Rôles et ports requis" (p. 162).
      Si le fournisseur d'authentification unique pour l'oVirt Engine est Keycloak (par défaut dans oVirt 4.5.1), utilisez le format Keycloak lorsque vous indiquez le nom d'utilisateur. Par exemple, indiquez comme compte administrateur par défaut le compte `admin@ovirt@internalsso` au lieu d'`admin@internal`.
   c. [Facultatif] Cliquez sur **Vérifier la connexion** pour vous assurer que les identifiants fournis sont corrects.
   d. Cliquez sur **OK**.

   (missing or bad snippet)
5. [Facultatif] Dans le champ **Nom**, cliquez sur **Modifier** pour modifier le nom par défaut de l'appliance virtuelle, qui est **localhost**. Ce nom s'affiche dans la console Cyber Protect.
6. [Facultatif] Dans le champ **Heure**, cliquez sur **Modifier**, puis sélectionnez le fuseau horaire de votre emplacement afin de vous assurer que les opérations planifiées sont exécutées au bon moment.
7. [Facultatif] [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.
   a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
   b. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.
   c. Localisez la section **env** ou créez-la et ajoutez les lignes suivantes :

      ```
      env:
      ```


© Acronis International GmbH, 2003-2026

```
http-proxy: proxy_login:proxy_password@proxy_address:port
https-proxy: proxy_login:proxy_password@proxy_address:port
```

d. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

e. Exécutez la commande `reboot`.

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pour protéger des machines virtuelles dans le centre de données Red Hat Virtualization/oVirt

1. Connectez-vous à votre compte Cyber Protection.
2. Accédez à **Terminaux** > **oVirt** > <your cluster>, ou recherchez vos ordinateurs dans **Terminaux** > **Tous les terminaux**.
3. Sélectionnez les ordinateurs et appliquez-leur un plan de protection.

Modification de l'adaptateur graphique d'une appliance virtuelle

Si vous utilisez une appliance virtuelle oVirt avec Oracle Linux Virtualization Manager, vous pourriez recevoir l'erreur suivante : « La machine virtuelle <name of the virtual appliance> s'est arrêtée avec une erreur. Message de résultat : configuration non prise en charge : la configuration du domaine ne prend pas en charge le modèle vidéo qxl. »

Pour résoudre cette erreur, changez l'adaptateur graphique de l'appliance virtuelle et sélectionnez un adaptateur **CIRRUS**.

Pour modifier l'adaptateur graphique d'une appliance virtuelle

1. Connectez-vous au portail d'administration Oracle Linux en tant qu'administrateur.
2. Accédez à **Calcul** > **Machines virtuelles**.
3. Eteindre[Si l'appliance virtuelle est sous tension] Cliquez avec le bouton droit sur l'appliance virtuelle, puis sélectionnez **Éteindre**.
4. Cliquez avec le bouton droit sur l'appliance virtuelle, puis sélectionnez **Modifier**.
5. [Si vous ne voyez que l'onglet **Général**] Cliquez sur **Afficher les options avancées**.
6. Cliquez sur **Console**.

© Acronis International GmbH, 2003-2026

7. Dans **Console graphique**, pour **Type vidéo**, sélectionnez **CIRRUS**.
8. Cliquez sur **OK**.
9. Dans le portail d'administration d'Oracle Linux, mettez l'appliance virtuelle sous tension.

Agent pour oVirt - Rôles et ports requis

Rôles requis

Pour son déploiement et son fonctionnement, l'agent pour oVirt nécessite un compte administrateur avec les rôles suivants attribués.

oVirt/Red Hat Virtualization 4.2 et 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Ports requis

L'agent pour oVirt se connecte a l'oVirt Engine à l'aide de l'URL que vous spécifiez lors de la configuration de l'appliance virtuelle. Généralement, l'URL du moteur possède le format suivant : `https://ovirt.company.com`.Dans ce cas, le protocole HTTPS et le port 443 sont utilisés.

Les paramètres oVirt différents des paramètres par défaut peuvent nécessiter d'autres ports. Vous pouvez déterminer le port exact en analysant le format de l'URL.Par exemple :

URL d'oVirt Engine	Port	Protocole
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

Aucun port supplémentaire n'est requis pour les opérations de lecture/écriture de disque, car la sauvegarde est effectuée en mode HotAdd.

Déploiement de l'agent pour Azure

Vous pouvez effectuer une sauvegarde sans agent des machines virtuelles Microsoft Azure en configurant l'agent pour Azure, un agent unique qui peut accéder aux données des machines

© Acronis International GmbH, 2003-2026

virtuelles Microsoft Azure de manière transparente.

Agent pour Azure garantit :

- La fonctionnalité de sauvegarde et de restauration pour les machines virtuelles Microsoft Azure exécutant Windows ou Linux.
- La réduction des frais généraux des machines virtuelles Microsoft Azure, avec un seul agent à gérer.
- La migration transparente de toutes les sauvegardes de machines sur site ou dans le cloud vers des machines virtuelles Microsoft Azure, configurables via la console Cyber Protect.
- La réduction des coûts des ressources Microsoft Azure, avec des frais généraux de processeur et de RAM pour un seul agent dans la machine virtuelle.

Avant de commencer

Configuration système requise pour l'agent

Par défaut, l'appliance virtuelle est affectée à la taille **Standard_B2s** (4 Gio de RAM et 2 processeurs). C'est la taille optimale et suffisante pour les opérations comprenant jusqu'à dix machines virtuelles sauvegardées en parallèle. Pour améliorer les performances de sauvegarde et éviter les échecs liés à une mémoire RAM insuffisante, nous vous recommandons de modifier la taille de l'appliance virtuelle (taille dans Azure) pour obtenir 4 processeurs virtuels et 8 Go de RAM dans les cas les plus exigeants. Par exemple, augmentez les ressources affectées lorsque vous sauvegardez plus de dix machines virtuelles en parallèle ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande taille (500 Go ou plus).

Pour plus d'informations sur cette propriété et sur d'autres propriétés des machines virtuelles Azure, consultez la documentation Microsoft Azure.

Déploiement de l'appliance virtuelle Agent pour Azure

Vous déployez l'appliance virtuelle Agent pour Azure en vous connectant d'abord à l'abonnement Microsoft Azure pertinent, puis en définissant les paramètres de déploiement Azure.

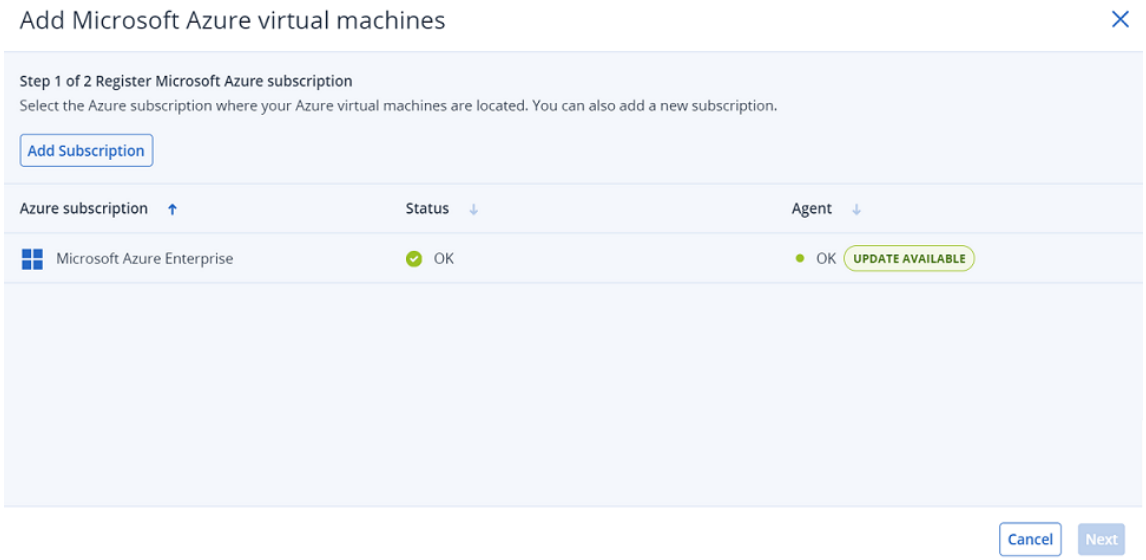
Remarque
La connexion à un abonnement Microsoft Azure peut être configurée lors de la création d'un emplacement de sauvegarde via le menu **Terminaux** ou **Stockage de sauvegarde**, comme le décrit la section "Définition d'un emplacement de sauvegarde dans Microsoft Azure" (p. 745).

Pour déployer l'appliance virtuelle Agent pour Azure

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans la section **Ressources cloud**, sélectionnez **Machines virtuelles Microsoft Azure**.
   - Si vous avez déjà des abonnements Microsoft Azure en cours d'utilisation, l'Assistant Ajouter des machines virtuelles Microsoft Azure s'affiche, avec vos abonnements existants

© Acronis International GmbH, 2003-2026

répertoriés. Vous pouvez sélectionner l'abonnement pertinent et cliquer sur **Suivant**. Passez ensuite à l'étape 8.



- Si vous avez des abonnements Microsoft Azure existants en cours d'utilisation mais que vous souhaitez ajouter un nouvel abonnement, cliquez sur **Ajouter un abonnement**.
- Si vous n'avez aucun abonnement existant, cliquez sur **Ajouter** pour ajouter un abonnement.

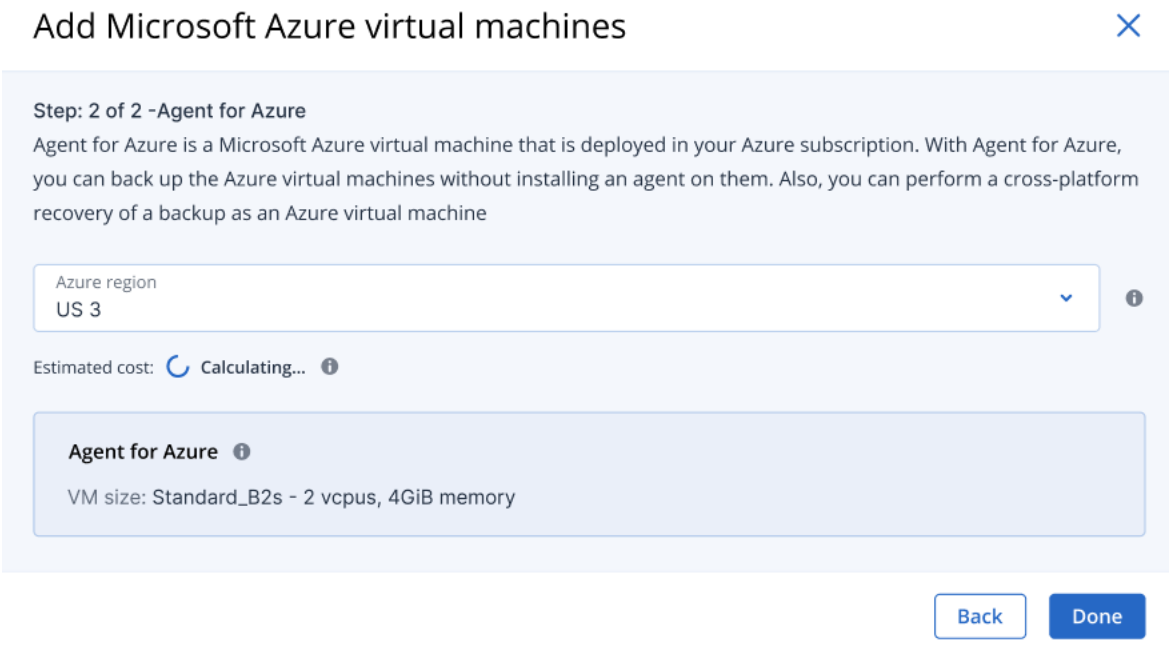
4. Dans la boîte de dialogue qui s'affiche, cliquez sur **Se connecter**. Vous êtes redirigé vers la page de connexion de Microsoft.

Remarque
Pour établir la connexion à l'abonnement, vous devez disposer de l'un des rôles suivants dans Microsoft Entra ID: administrateur d'applications dans le cloud, administrateur d'applications ou administrateur global. Vous devez également recevoir le rôle de propriétaire pour chaque abonnement sélectionné.

5. Saisissez vos identifiants de connexion Microsoft et acceptez les autorisations demandées. Le processus de connexion démarre et peut prendre plusieurs minutes.
   Pour plus d'informations sur l'accès sécurisé à votre abonnement Microsoft Azure, reportez-vous à l'article Microsoft Azure – sécurité de la connexion et audit (72684).
6. Une fois la connexion établie :
   - Si vous avez plusieurs abonnements, sélectionnez l'abonnement approprié dans la liste déroulante de la boîte de dialogue affichée, puis cliquez sur **Ajouter un abonnement**. Vous êtes alors redirigé vers l'écran principal de l'assistant.
   - Si vous ajoutez votre premier abonnement, vous êtes redirigé vers l'écran principal de l'assistant.
7. Sélectionnez le client pertinent, puis cliquez sur **Suivant**.
8. Dans la liste déroulante **Région Azure**, sélectionnez la région pertinente pour l'abonnement. Vous devez sélectionner une région Azure où la plupart des machines virtuelles à protéger sont déployées afin d'optimiser les performances de sauvegarde.

© Acronis International GmbH, 2003-2026

Le coût estimé pour la région est calculé et affiché. Ces coûts seront imputés à votre abonnement Microsoft Azure et facturés par Microsoft.



Remarque
L'agent pour Azure déployé utilise la taille Standard_B2s.

9. Cliquez sur **Terminé**.
   Vous êtes redirigé vers l'écran **Terminaux** > **Microsoft Azure** qui affiche la progression du déploiement. Lorsque le déploiement est terminé, vous pouvez commencer à définir des plans de protection avec le nouvel abonnement ajouté.
   Pour plus d'informations sur les options supplémentaires de sauvegarde et de restauration Microsoft Azure, voir "Points de restauration Azure" (p. 606) et "Restauration de machines virtuelles" (p. 689).

Affichage et mise à jour d'un agent pour Azure déployé

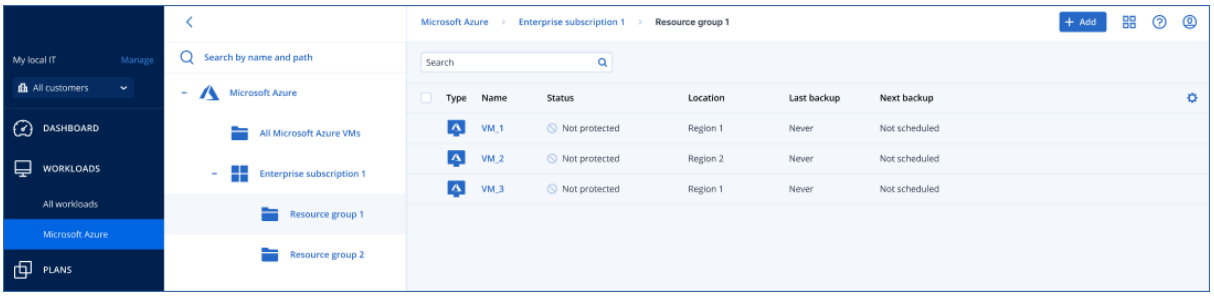
Vous pouvez afficher et mettre à jour le déploiement de l'agent pour Azure de la manière suivante :

- Affichez les déploiements actuels via le menu **Terminaux > Microsoft Azure**.
- Affichez, mettez à jour, accédez aux les déploiements actuels via le menu **Infrastructure > Clouds publics** et redéployez-les.

Pour afficher les déploiements actuels via le menu Microsoft Azure

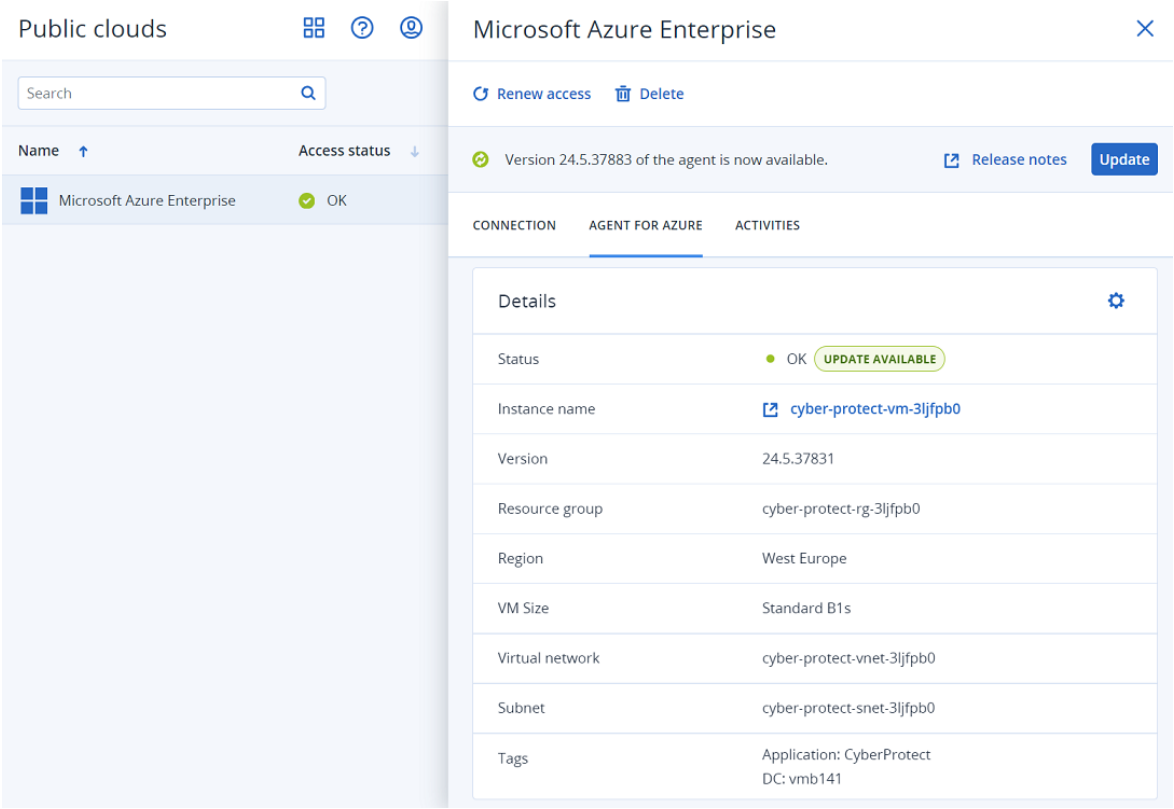
Dans la console Cyber Protect, accédez à **Terminaux > Microsoft Azure**. La liste actuelle des déploiements de l'agent pour Azure s'affiche. Notez que chaque abonnement répertorié affiche les groupes de ressources pertinents ci-dessous dans l'arborescence hiérarchique.

© Acronis International GmbH, 2003-2026



Pour afficher et mettre à jour les déploiements actuels via le menu Infrastructure > Clouds publics

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
   La liste actuelle des connexions au cloud public s'affiche.
2. Sélectionnez l'abonnement Microsoft Azure dans lequel l'agent pour Azure est déployé.
3. Dans le volet de droite, cliquez sur l'onglet **Agent pour Azure**.



4. Vous pouvez :
   - Afficher le statut actuel du déploiement.
   - Cliquez sur le lien dans le champ **Nom de l'instance** pour accéder à l'instance dans laquelle est déployé l'agent pour Azure. Notez que vous devrez être connecté à votre compte Microsoft Azure pour accéder à l'instance.
   - Cliquez sur ⚙ pour redéployer l'agent pour Azure.
   - Cliquez sur **Mettre à jour** si une mise à jour est disponible.

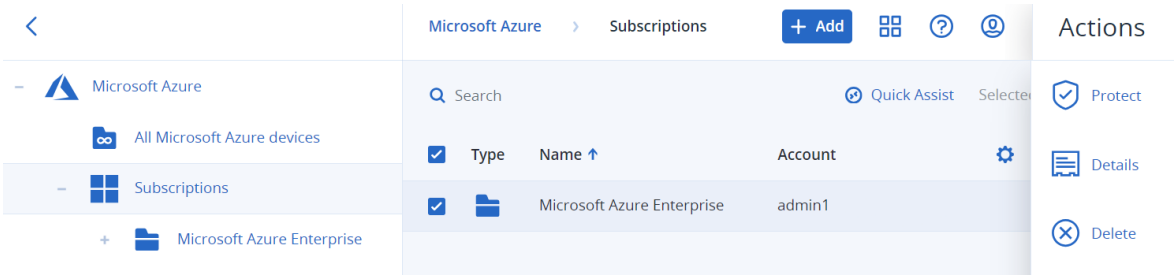
© Acronis International GmbH, 2003-2026

Suppression de l'appliance virtuelle de l'agent pour Azure

L'appliance virtuelle de l'agent pour Azure est automatiquement supprimée lorsque vous supprimez l'abonnement Microsoft Azure correspondant.

Pour supprimer l'appliance virtuelle de l'agent pour Azure

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft Azure**.
2. Cliquez sur le nœud **Abonnements** dans l'arborescence hiérarchique, puis sélectionnez l'abonnement pertinent dans la liste affichée à droite.



3. Dans le volet de droite, cliquez sur **Supprimer**.
4. Dans le message de confirmation qui s'affiche, cliquez sur **Supprimer**.
   Lorsque l'abonnement est supprimé, l'appliance virtuelle de l'agent pour Azure est déprovisionnée et n'utilise plus les ressources Microsoft Azure.

Remarque
Vous ne pouvez pas supprimer l'abonnement s'il est utilisé par des machines virtuelles Microsoft Azure.

Déploiement de l'agent pour Nutanix AHV

Avant de commencer

Cet appliance est une machine virtuelle préconfigurée que vous pouvez déployer sur un cluster Nutanix. Elle contient un agent de protection qui peut sauvegarder et restaurer les machines virtuelles du cluster.

Configuration système de l'appliance virtuelle

Nous vous recommandons de configurer l'appliance virtuelle avec 4 vCPU (4 vCPU monocœurs ou 2 vCPU bicœurs) et 8 Gio de RAM. Ces paramètres sont suffisants pour la plupart des opérations.

Pour améliorer les performances de la sauvegarde et éviter les défaillances liées à une mémoire RAM insuffisante, vous pouvez augmenter la mémoire RAM à 16 Gio dans les situations les plus exigeantes. Par exemple, augmentez ces ressources si vous vous attendez à un trafic de sauvegarde supérieur à 100 Mo par seconde (par exemple, sur les réseaux 10 Gigabits) ou si vous sauvegardez simultanément plusieurs machines virtuelles avec des disques durs de grande capacité (500 Gio ou plus).

© Acronis International GmbH, 2003-2026

La taille du disque virtuel de l'appliance est de 8 Gio.

Combien d'appliances virtuelles me faut-il ?

Une seule appliance virtuelle peut sauvegarder et restaurer toutes les machines virtuelles du cluster. Si vous souhaitez distribuer la charge de la bande passante du trafic de sauvegarde, vous pouvez utiliser plusieurs appliances virtuelles par cluster.

Si plusieurs appliances virtuelles sont déployées dans le cluster, les machines virtuelles sauvegardées sont redistribuées automatiquement lorsque le déséquilibre de charge entre les appliances atteint 20 %.

Lorsque vous déployez un autre appliance virtuelle, le serveur de gestion affecte les machines virtuelles les plus appropriées à la nouvelle appliance et la charge de l'appliance existante diminue. Lorsque vous supprimez un appliance virtuelle, les machines virtuelles sauvegardées sont redistribuées entre les appliances restantes. La redistribution se produit uniquement si vous supprimez l'appliance virtuelle de la console Cyber Protect. La redistribution ne démarrera pas si vous supprimez l'appliance virtuelle de la console Nutanix Prism Element ou si l'appliance est corrompue.

Limites

Les opérations suivantes ne sont pas prises en charge :

- Sauvegarde reconnaissant les applications
- Exécution d'une machine virtuelle à partir d'une sauvegarde
- Réplication de machines virtuelles
- Sauvegardes de groupes de volumes Nutanix

Déploiement du modèle QCOW2

Vous pouvez déployer l'appliance virtuelle Nutanix en créant une machine virtuelle dans le cluster Nutanix et en déployant le modèle QCOW que vous téléchargez à partir de la console Cyber Protect.

Vous devez déployer au moins une appliance virtuelle par cluster.

Pour déployer le modèle QCOW2

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur **Terminaux** > **Tous les terminaux** > **Ajouter** > **Nutanix AHV**.
   Une archive ZIP est téléchargée sur votre machine.
3. Décompressez l'archive ZIP et extrayez le fichier image QCOW2.
4. Connectez-vous à la console Nutanix Prism Element en tant qu'administrateur.
5. Téléchargez le fichier image QCOW2 sur la console Nutanix Prism Element.
   a. Accédez à **Paramètres**, puis, sous **Général**, sélectionnez **Configuration de l'image**.
   b. Cliquez sur **Transférer une image**.

© Acronis International GmbH, 2003-2026

c. Spécifiez un nom pour l'image.

d. Dans **Type d'image**, sélectionnez **Disque**.

e. Cliquez sur **Transférer un fichier**, puis sur **Choisir un fichier**.

f. Sélectionnez l'image QCOW2 que vous avez téléchargée à partir de la console Cyber Protect.

g. Cliquez sur **Enregistrer**.

6. Dans la console Nutanix Prism Element, créez une nouvelle machine virtuelle en utilisant l'image QCOW2.

   a. Accédez à **Machine virtuelle**, puis cliquez sur **Créer une machine virtuelle**.

   b. Spécifiez un nom pour la machine virtuelle.

   c. Dans **Détails du calcul**, spécifiez 4 vCPU (monocœurs) ou 2 vCPU bicœurs, et 8 Gio de mémoire.

   d. Dans **Disques**, cliquez sur **Ajouter un nouveau disque**.

   e. Dans **Opération**, sélectionnez **Cloner à partir du service d'image**.

   f. Dans **Image**, sélectionnez l'image que vous avez transférée sur la console Nutanix Prism Element.

   g. Cliquez sur **Ajouter**.

   h. Dans **Cartes réseau (NIC)**, cliquez sur **Ajouter une carte réseau**.

   i. Configurez les paramètres réseau, puis cliquez sur **Ajouter**.

   j. [Facultatif] Pour masquer l'appliance virtuelle dans la console Cyber Protect, spécifiez les informations suivantes dans **Description** :

   ```
   {AB53A0F1-AD54-480f-80BB-FC72DC41DF53}
   ```

   Cela évitera que vous appliquiez accidentellement des plans de protection à l'appliance proprement dite et que vous les incluyez dans des groupes dynamiques.

   k. Cliquez sur **Enregistrer**.

7. Dans **Machine virtuelle** > **Tableau**, cliquez avec le bouton droit sur la machine virtuelle que vous avez créée, puis sélectionnez **Mettre sous tension**.

   L'appliance virtuelle est déployée et mise sous tension.

   Configurez ensuite l'appliance virtuelle. Voir "Configuration de l'appliance virtuelle Nutanix" (p. 169).

Configuration de l'appliance virtuelle Nutanix

Après le déploiement de l'appliance virtuelle, vous devez configurer son accès au cluster Nutanix et à la console Cyber Protect.

Prérequis

- Vous avez déployé l'appliance virtuelle Nutanix et l'avez mise sous tension. Voir "Déploiement du modèle QCOW2" (p. 168).

© Acronis International GmbH, 2003-2026

Pour configurer l'appliance virtuelle Nutanix

1. Connectez-vous à la console Nutanix Prism Element en tant qu'administrateur.
2. Accédez à **Machine virtuelle** > **Tableau**.
3. Cliquez avec le bouton droit sur la machine virtuelle que vous avez déployée, puis sélectionnez **Lancer la console**.
4. Dans le champ **eth0**, configurez les interfaces réseau de l'appliance.
   Si des adresses DHCP sont attribuées automatiquement, assurez-vous qu'elles sont valides dans les réseaux qu'utilise votre machine virtuelle. Vous pouvez également les attribuer manuellement. Selon le nombre de réseaux que l'appliance utilise, vous aurez peut-être une ou plusieurs interfaces à configurer.
5. Spécifiez l'adresse IP du cluster Nutanix (Nutanix Prism Element) et les identifiants pour y accéder.

   Remarque
   Vous ne pouvez pas configurer l'agent pour Nutanix AHV avec l'adresse IP de Nutanix Prism Central. Même si vous gérez le cluster via Nutanix Prism Central, l'agent pour Nutanix AHV ne peut y accéder que via Nutanix Prism Element.

   a. Sous **Options de l'agent**, cliquez dans le champ **Nutanix** sur **Modifier**.
   b. Dans le champ **Nom/IP du serveur**, saisissez l'adresse IP du cluster.
   c. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants du compte administrateur Nutanix.
      Ce compte doit disposer des rôles **Administrateur utilisateur** et **Administrateur de cluster** dans le cluster Nutanix.
   d. Pour vérifier que les paramètres sont corrects, cliquez sur **Vérifier la connexion**.
   e. Cliquez sur **OK**.

   (missing or bad snippet)
6. [Facultatif] Modifiez le nom par défaut **localhost** de l'appliance virtuelle.
   Ce nom s'affiche dans la console Cyber Protect.
   a. Dans **Machine virtuelle**, cliquez dans le champ **Nom** sur **Modifier**.
   b. Modifiez le nom, puis cliquez sur **OK**.
7. [Facultatif] Configurer le fuseau horaire de l'appliance virtuelle.
   a. Sous **Machine virtuelle**, dans le champ **Fuseau horaire**, cliquez sur **Changer**.
   b. Pour vous assurer que les opérations de planification s'exécutent à l'heure correcte, sélectionnez le fuseau horaire de votre emplacement.
8. [Si un serveur proxy est activé sur votre réseau] Configurez le serveur proxy.
   a. Appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
   b. Ouvrez le fichier `/opt/acronis/etc/aakore.yaml` dans un éditeur de texte.
   c. Localisez la section **env** ou créez-la et ajoutez les lignes suivantes :

© Acronis International GmbH, 2003-2026

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

d. Remplacez `proxy_login` et `proxy_password` par les identifiants de connexion au serveur proxy, et `proxy_address:port` par l'adresse et le numéro de port du serveur proxy.

e. Exécutez la commande `reboot`.

Remarque

Pour pouvoir mettre à jour une appliance virtuelle déployée derrière un proxy, modifiez le fichier `config.yaml` de l'appliance (`/opt/acronis/etc/va-updater/config.yaml`) en ajoutant la ligne suivante à la fin du fichier et en saisissant les valeurs propres à votre environnement :

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Par exemple :

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Sauvegarde des machines virtuelles Nutanix

Prérequis

- Vous avez déployé et configuré l'appliance virtuelle Nutanix.

Pour protéger les machines virtuelles Nutanix

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Terminaux** > **Nutanix** > <your cluster>.
3. Sélectionnez les machines virtuelles et appliquez-leur un plan de protection.

Déploiement de l'agent pour Synology

Avant de commencer

Avec l'agent pour Synology, vous pouvez sauvegarder des fichiers et des dossiers depuis et vers un NAS Synology. Les propriétés du NAS et les autorisations d'accès des partages, dossiers et fichiers sont conservées.

L'agent pour Synology s'exécute sur le NAS. Par conséquent, vous pouvez utiliser les ressources du terminal pour les opérations de traitement des données hors hôte, comme la réplication de sauvegarde, la validation et le nettoyage. Pour en savoir plus sur ces opérations, reportez-vous à "Plans de protection des données hors hôte" (p. 255).

© Acronis International GmbH, 2003-2026

Remarque
L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge. Voir le centre de connaissances Synology.

Vous pouvez restaurer une sauvegarde dans son emplacement d'origine ou dans un nouvel emplacement sur le NAS, et dans un dossier réseau accessible par ce terminal. Les sauvegardes dans le stockage dans le cloud peuvent également être restaurées sur un NAS non d'origine sur lequel est installé l'agent pour Synology.

Le tableau ci-dessous récapitule les sources et destinations de sauvegarde disponibles.

Que sauvegarder	Éléments à sauvegarder (Source de sauvegarde)	Où sauvegarder (Destination de sauvegarde)
Fichiers/dossiers	Dossier local*	Stockage dans le Cloud
		Dossier local*
	Dossier réseau (SMB)**	Dossier réseau (SMB)**
		Dossier NFS
		Clouds publics***

* Comprend les clés USB insérées dans le NAS.

Remarque
Les dossiers chiffrés ne sont pas pris en charge. Ces dossiers ne sont pas affichés dans l'interface graphique Cyber Protection.

** L'utilisation de partages réseau externes en tant que source ou destination de la sauvegarde par l'intermédiaire du protocole SMB n'est disponible que pour les agents qui s'exécutent sur Synology DiskStation Manager 6.2.3 et les versions ultérieures. Les données hébergées sur le NAS Synology proprement dit, y compris dans les partages réseau hébergés, peuvent être sauvegardées sans limites.

*** La sauvegarde dans les clouds publics, tels que Microsoft Azure, Amazon ou les stockages compatibles S3, n'est prise en charge que par l'agent pour Synology 7.x. L'agent pour Synology 6.x ne prend pas en charge cette destination de sauvegarde en raison des limitations du noyau Linux de Synology DSM 6.x.

Limites

- L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge. Voir le centre de connaissances Synology.
- Les partages chiffrés et sauvegardés sont restaurés comme partages non chiffrés.

© Acronis International GmbH, 2003-2026

- Les partages sauvegardés pour lesquels l'option **Compression de fichier** est activée sont restaurés avec cette option désactivée.
- Vous ne pouvez restaurer sur un terminal Synology NAS que les sauvegardes créées par l'Agent for Synology.

Téléchargement du programme d'installation

Le programme d'installation de l'agent pour Synology est disponible sous forme de fichier SPK.

Agent pour Synology 7.x

Pour télécharger le programme d'installation

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans l'angle supérieur droit, cliquez sur **Ajouter**.
3. Dans **Périphériques de stockage en réseau (NAS)**, cliquez sur **Synology**.
   Le programme d'installation est téléchargé sur votre ordinateur.

Agent pour Synology 6.x

Pour télécharger le programme d'installation

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans l'angle supérieur droit, cliquez sur **Ajouter**.
3. Dans **Périphériques de stockage en réseau (NAS)**, cliquez sur **Synology**.
   Le programme d'installation de l'agent pour Synology 7.x est téléchargé sur votre ordinateur.
   Vous pouvez arrêter en toute sécurité le processus de téléchargement ou ignorer le fichier téléchargé.
4. Cliquez sur **Télécharger l'agent pour Synology 6.x**.
   Le programme d'installation de l'agent pour Synology 6.x est téléchargé sur votre ordinateur.

Installation de l'agent pour Synology

Pour installer l'agent pour Synology, exécutez le fichier SPK dans Synology DiskStation Manager.

Remarque
L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge. Voir le centre de connaissances Synology.

Agent pour Synology 7.x

Prérequis

- Le terminal NAS exécute DiskStation Manager 7.x.
- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace

© Acronis International GmbH, 2003-2026

libre.

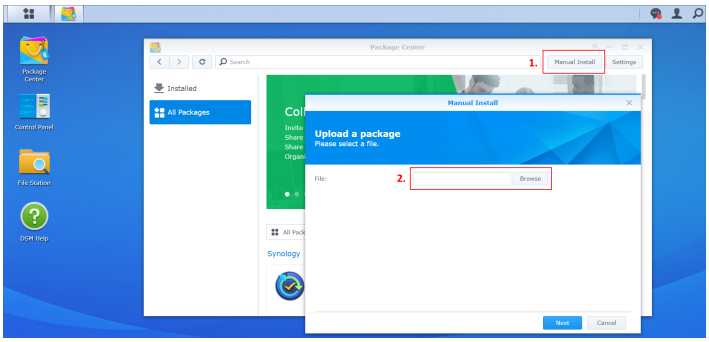
- Un client SSH est disponible sur votre ordinateur. Ce document utilise Putty comme exemple.

Limites

- Vous ne pouvez pas enregistrer l'agent pour Synology via QuickConnect. Pour enregistrer l'agent, accédez directement au terminal NAS.

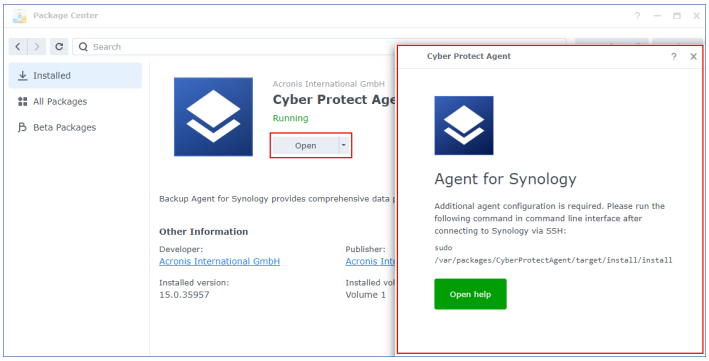
Pour installer l'agent pour Synology

1. Connectez-vous à Synology DiskStation Manager.
2. Ouvrez le **Package Center**.
3. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.



4. Sélectionnez le fichier SPK que vous avez téléchargé à partir de la console Cyber Protect, puis cliquez sur **Suivant**.

   Un avertissement s'affiche pour indiquer que vous allez installer un package logiciel tiers. Ce message fait partie de la procédure d'installation standard.
5. Pour confirmer que vous souhaitez installer le package, cliquez sur **Accepter**.
6. Sélectionnez le volume sur lequel vous souhaitez installer l'agent, puis cliquez sur **Suivant**.
7. Vérifiez les paramètres, puis cliquez sur **Terminé**.
8. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology, puis vérifiez que vous voyez l'écran suivant.

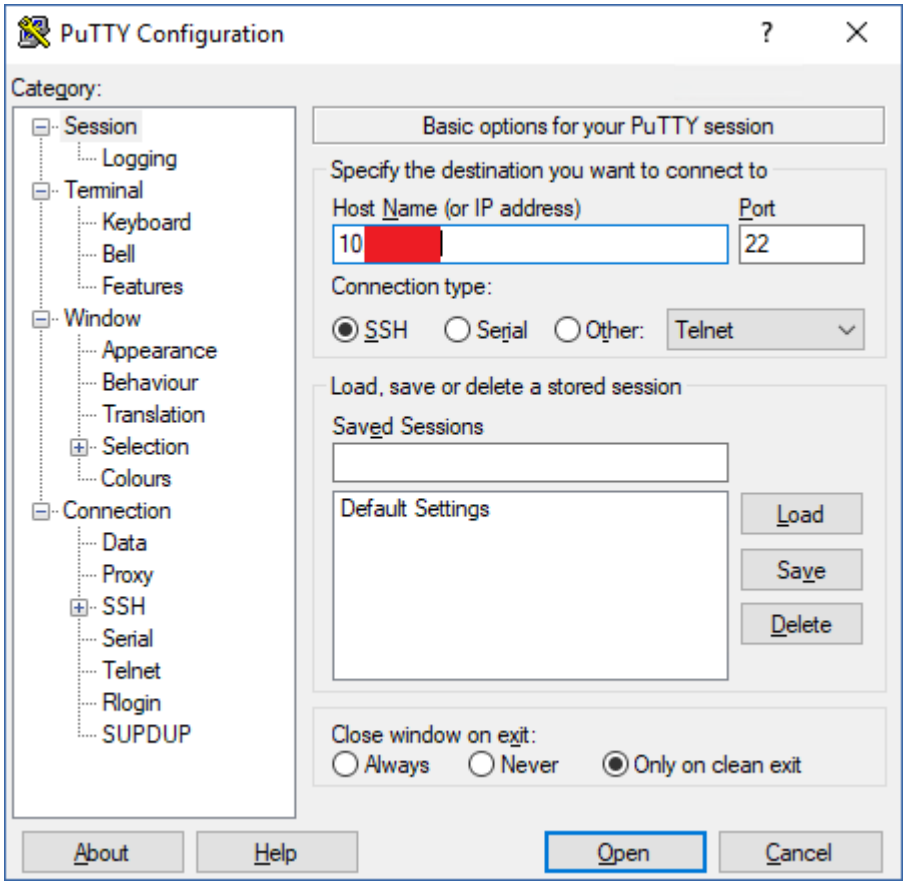


9. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis activez l'accès SSH au terminal NAS.
10. Exécutez le script `install` sur le terminal NAS à l'aide d'un client SSH (dans cet exemple, Putty).

© Acronis International GmbH, 2003-2026

Le script permet l'accès root (superutilisateur) à DSM 7.0 ou à une version ultérieure, qui est l'accès nécessaire à la configuration de l'agent.

a. Démarrez Putty, puis spécifiez l'adresse IP ou le nom d'hôte du terminal Synology NAS.



b. Cliquez sur **Ouvrir**, puis connectez-vous en tant qu'administrateur Synology DSM.

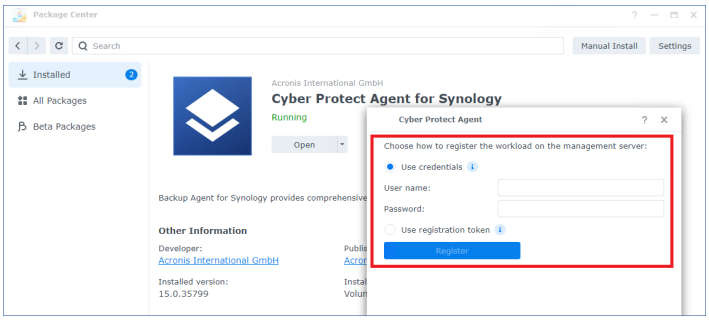
c. Exécutez la commande suivante.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

Après le démarrage du script, attendez 15 secondes pendant lesquelles les services Cyber Protection s'initialisent.

11. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis désactivez l'accès SSH au terminal NAS. L'accès SSH n'est plus nécessaire.
12. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology.
13. Sélectionnez la méthode d'inscription.

© Acronis International GmbH, 2003-2026



- [Pour enregistrer l'agent en utilisant les informations d'identification].
  - Dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel l'agent sera enregistré. Ce compte ne peut pas être un compte administrateur partenaire.
- [Pour enregistrer l'agent à l'aide d'un jeton d'enregistrement]
  - Dans **Adresse d'enregistrement**, indiquez l'adresse exacte du centre de données. L'adresse exacte du centre de données correspond à l'URL que vous voyez après vous être connecté à la console Cyber Protect. Par exemple, `https://us5.acronis.cloud`.

    Remarque
    N'utilisez pas de format d'URL sans l'adresse du centre de données. Par exemple, n'utilisez pas `https://acronis.cloud`.

  - Dans le champ **Jeton**, indiquez le jeton d'enregistrement.
    Pour plus d'informations sur la génération d'un jeton d'enregistrement, voir "Génération d'un jeton d'enregistrement" (p. 112).

14. Cliquez sur **Enregistrer**.

Agent pour Synology 6.x

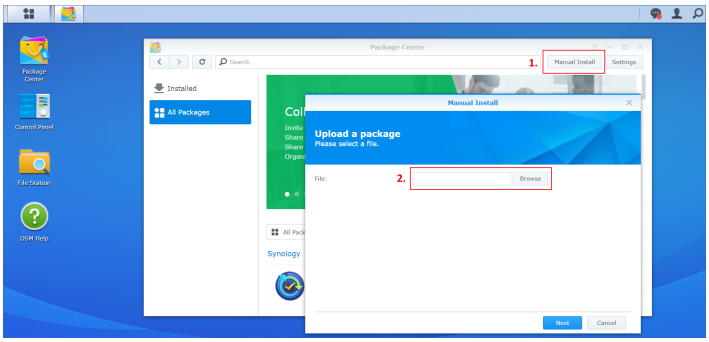
Prérequis

- Le terminal NAS exécute DiskStation Manager 6.2.x.
- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.

Pour installer l'agent pour Synology

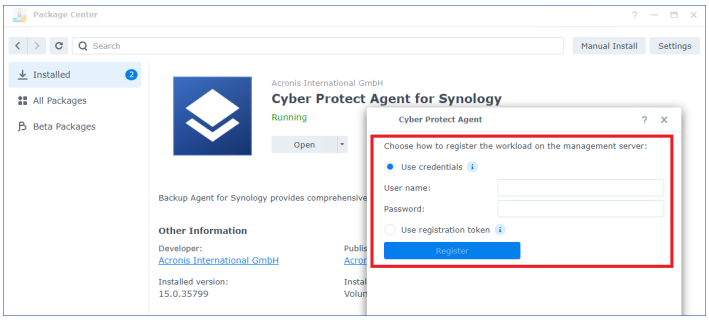
1. Connectez-vous à Synology DiskStation Manager.
2. Ouvrez le **Package Center**.
3. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.

© Acronis International GmbH, 2003-2026



4. Sélectionnez le fichier SPK que vous avez téléchargé à partir de la console Cyber Protect, puis cliquez sur **Suivant**.

   Un avertissement s'affiche pour indiquer que vous allez installer un package sans signature numérique. Ce message fait partie de la procédure d'installation standard.
5. Pour confirmer que vous souhaitez installer le package, cliquez sur **Oui**.
6. Sélectionnez le volume sur lequel vous souhaitez installer l'agent, puis cliquez sur **Suivant**.
7. Vérifiez les paramètres, puis cliquez sur **Appliquer**.
8. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology.
9. Sélectionnez la méthode d'inscription.



- [Pour enregistrer l'agent en utilisant les informations d'identification].
  - Dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel l'agent sera enregistré. Ce compte ne peut pas être un compte administrateur partenaire.
- [Pour enregistrer l'agent à l'aide d'un jeton d'enregistrement]
  - Dans **Adresse d'enregistrement**, indiquez l'adresse exacte du centre de données.

    L'adresse exacte du centre de données correspond à l'URL que vous voyez après vous être connecté à la console Cyber Protect. Par exemple, `https://us5.acronis.cloud`.

    Remarque

    N'utilisez pas de format d'URL sans l'adresse du centre de données. Par exemple, n'utilisez pas `https://acronis.cloud`.
  - Dans le champ **Jeton**, indiquez le jeton d'enregistrement.

© Acronis International GmbH, 2003-2026

Pour plus d'informations sur la génération d'un jeton d'enregistrement, voir "Génération d'un jeton d'enregistrement" (p. 112).

10. Cliquez sur **Enregistrer**.

Après l'inscription, le terminal NAS Synology apparaît dans la console Cyber Protect, dans l'onglet **Terminaux** > **NAS**.

Pour sauvegarder les données sur ce terminal NAS, appliquez un plan de protection.

Mise à jour de l'agent pour Synology

Vous pouvez mettre à jour l'agent pour Synology 6.x vers une nouvelle version de l'agent pour Synology 6.x. De la même manière, vous pouvez mettre à jour l'agent pour Synology 7.x vers une nouvelle version de l'agent pour Synology 7.x.

Pour mettre à jour l'agent, exécutez la dernière version du programme d'installation dans Synology DiskStation Manager. L'inscription d'origine de l'agent, ses paramètres et les plans appliqués aux ressources protégées seront conservés.

Remarque
Vous ne pouvez pas mettre l'agent à jour depuis la console Cyber Protect.

La mise à niveau de l'agent pour Synology 6.x vers l'agent pour Synology 7.x n'est prise en charge que par la désinstallation de l'ancien agent et l'installation du nouvel agent. Dans ce cas, tous les plans de protection sont révoqués et vous devez les réappliquer manuellement.

Agent pour Synology 7.x

Prérequis

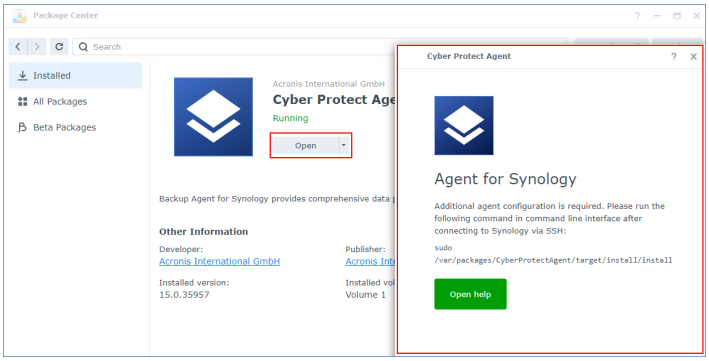
- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.
- Un client SSH est disponible sur votre ordinateur. Ce document utilise Putty comme exemple.

Pour mettre à jour l'agent pour Synology

1. Dans DiskStation Manager, ouvrez le **Package Center**.
2. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.
3. Sélectionnez le dernier fichier SPK de l'agent pour Synology 7.x que vous avez téléchargé depuis la console Cyber Protect, puis cliquez sur **Suivant**.
   Un avertissement s'affiche pour indiquer que vous allez installer un package logiciel tiers. Ce message fait partie de la procédure d'installation standard.
4. Pour confirmer que vous souhaitez installer le package, cliquez sur **Accepter**.
5. Vérifiez les paramètres, puis cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

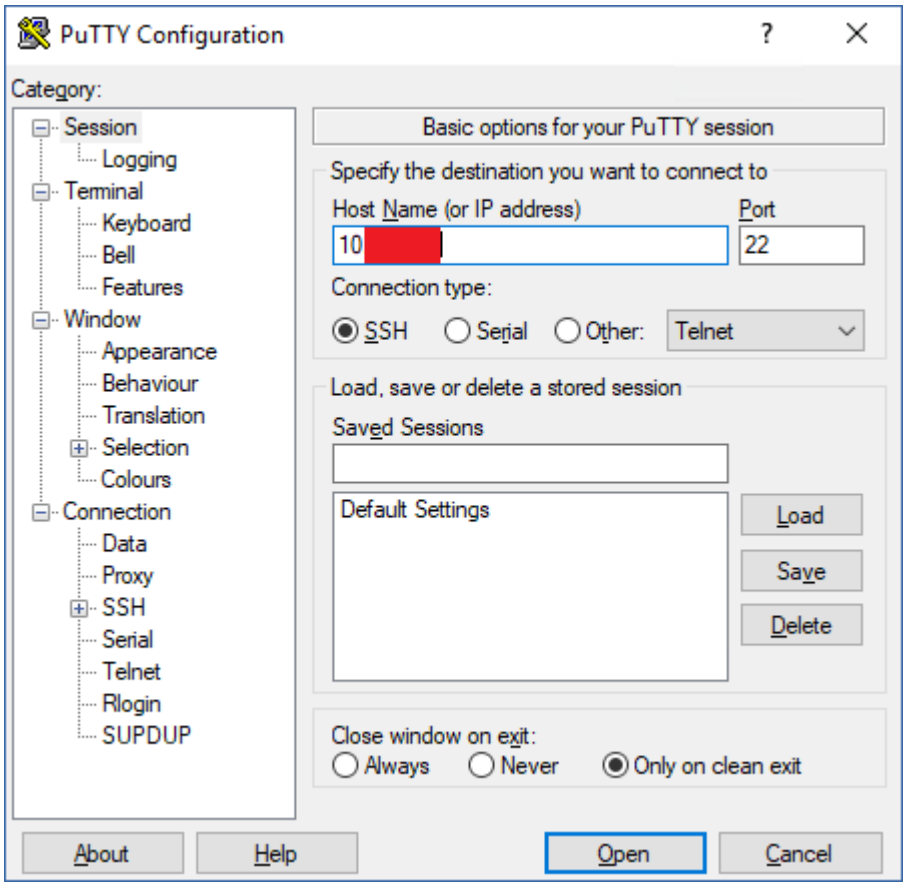
6. Dans le **Package Center** de Synology DiskStation Manager, ouvrez l'agent Cyber Protect pour Synology, puis vérifiez que vous voyez l'écran suivant.



7. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis activez l'accès SSH au terminal NAS.
8. Exécutez le script `install` sur le terminal NAS à l'aide d'un client SSH (dans cet exemple, Putty).

   Le script permet l'accès root (superutilisateur) à DSM 7.0 ou à une version ultérieure, qui est l'accès nécessaire à la configuration de l'agent.

   a. Démarrez Putty, puis spécifiez l'adresse IP ou le nom d'hôte du terminal Synology NAS.



   b. Cliquez sur **Ouvrir**, puis connectez-vous en tant qu'administrateur Synology DSM.

   c. Exécutez la commande suivante.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```


© Acronis International GmbH, 2003-2026

9. Dans le **Panneau de configuration** de Synology DiskStation Manager, accédez à **Terminal & SNMP**, puis désactivez l'accès SSH au terminal NAS. L'accès SSH n'est plus nécessaire.

Agent pour Synology 6.x

Prérequis

- Vous êtes membre du groupe d'**administrateurs** sur le terminal NAS.
- Le volume du NAS sur lequel vous souhaitez installer l'agent dispose d'au moins 200 Mo d'espace libre.

Pour mettre à jour l'agent pour Synology

1. Dans DiskStation Manager, ouvrez le **Package Center**.
2. Cliquez sur **Installation manuelle**, puis sur **Parcourir**.
3. Sélectionnez le dernier fichier SPK de l'agent pour Synology 6.x que vous avez téléchargé depuis la console Cyber Protect, puis cliquez sur **Suivant**.
   Un avertissement s'affiche pour indiquer que vous allez installer un package sans signature numérique. Ce message fait partie de la procédure d'installation standard.
4. Pour confirmer que vous souhaitez installer le package, cliquez sur **Oui**.
5. Vérifiez les paramètres, puis cliquez sur **Appliquer**.

Connexions SSH à une appliance virtuelle

Utilisez une connexion SSH (Secure Socket Shell) lorsque vous accédez à distance à une appliance virtuelle à des fins de maintenance.

Démarrage du démon Secure Shell

Pour permettre les connexions SSH à une appliance virtuelle, démarrez le démon Secure Shell (sshd) sur l'appliance.

Pour démarrer le démon Secure Shell

1. Dans le logiciel hyperviseur, ouvrez la console de l'appliance virtuelle.
2. Dans l'interface graphique de l'appliance, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
3. Exécuter la commande suivante :

   ```
   /bin/sshd
   ```

4. [Uniquement lors de la première connexion à l'appliance] Définissez le mot de passe de l'utilisateur `root` (superutilisateur).
   Pour savoir comment définir le mot de passe, voir "Définition du mot de passe root sur une appliance virtuelle" (p. 181).

 © Acronis International GmbH, 2003-2026

Remarque
Nous vous recommandons d'arrêter le démon Secure Shell lorsque vous n'utilisez pas la connexion SSH.

Définition du mot de passe root sur une appliance virtuelle

Avant d'établir la première connexion SSH à une appliance virtuelle, vous devez définir le mot de passe root sur l'appliance.

Pour définir le mot de passe root (superutilisateur)

1. Dans le logiciel hyperviseur, ouvrez la console de l'appliance virtuelle.
2. Dans l'interface graphique de l'appliance, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
3. Exécuter la commande suivante :

   ```
   passwd
   ```

4. Spécifiez un mot de passe, puis appuyez sur Entrée.
   Le mot de passe doit contenir au moins neuf caractères et doit avoir un score de complexité d'au moins trois. Le score de complexité est calculé automatiquement. Pour atteindre un score plus élevé, utilisez une combinaison de caractères spéciaux, de caractères en majuscules et en minuscules, et de chiffres.
5. Confirmez le mot de passe, puis appuyez sur Entrée.

Accéder à une appliance virtuelle via un client SSH

Prérequis

- Un client SSH doit être disponible sur la machine distante. La procédure ci-dessous utilise le client WinSCP comme exemple. Vous pouvez utiliser n'importe quel client SSH, en adaptant les étapes en conséquence.
- Le démon Secure Shell (sshd) doit être démarré sur l'appliance virtuelle. Pour plus d'informations, voir "Démarrage du démon Secure Shell" (p. 180).

Pour accéder à une appliance virtuelle via WinSCP

1. Sur la machine distante, ouvrez WinSCP.
2. Cliquez sur **Session** > **Nouvelle session**.
3. Dans **Protocole de fichier**, sélectionnez **SCP**.
4. Dans **Nom d'hôte**, spécifiez l'adresse IP de votre appliance virtuelle.
5. Dans **Nom d'utilisateur** et **Mot de passe**, spécifiez `root` et le mot de passe de l'`root`.
6. Cliquez sur **Connexion**.

La liste de tous les répertoires de l'appliance virtuelle s'affiche.

© Acronis International GmbH, 2003-2026

Détection des terminaux

Grâce à la fonctionnalité de découverte de terminaux, vous pouvez :

- Bénéficiez d'une visibilité complète des terminaux réseau disponibles dans les réseaux de l'organisation.
- Grâce à la synchronisation avec Active Directory, facilitez le provisionnement de ressources et la gestion des ordinateurs dans un domaine Active Directory important.
- Automatiser l'installation des agents de protection ainsi que l'inscription des ordinateurs en détectant les ordinateurs dans votre domaine Active Directory ou votre réseau local.
- Installer des agents de protection sur plusieurs ressources.

Vous pouvez utiliser l'une des méthodes suivantes pour effectuer la découverte de terminaux :

- Découverte Active Directory.

  Lors d'une découverte Active Directory, l'agent de découverte collecte des informations concernant l'unité d'organisation (UO) des ordinateurs, ainsi que des informations détaillées concernant leur nom et leur système d'exploitation. Les adresses IP et MAC ne sont pas collectées.
- Découverte du réseau local à l'aide de Device Sense ™. Pour plus d'informations, voir "Découverte de terminaux à l'aide de Device Sense ™" (p. 189).
- Découverte manuelle : par l'utilisation de l'adresse IP ou du nom d'hôte d'un ordinateur, ou par l'importation d'une liste d'ordinateurs à partir d'un fichier.

  Lors d'une découverte manuelle, les agents de protection existants sont mis à jour et réinscrits. Si vous exécutez la découverte automatique en utilisant le même compte que celui sur lequel un agent est inscrit, l'agent ne sera mis à jour que vers la version la plus récente. Si vous utilisez la découverte automatique à l'aide d'un autre compte, l'agent sera mis à jour vers la dernière version et réinscrit sous le tenant auquel le compte appartient.

Vous pouvez également configurer la découverte passive des terminaux à l'aide de Device Sense ™ et afficher des informations détaillées sur les terminaux disponibles dans les réseaux locaux de votre organisation. Pour plus d'informations, voir "Découverte passive de terminaux à l'aide de Device Sense ™" (p. 191).

Découverte de plusieurs terminaux

Le processus de découverte de plusieurs terminaux peut se résumer par les étapes suivantes :

1. Sélectionnez la méthode de découverte :
   - Découverte Active Directory : par l'utilisation d'un contrôleur de domaine pour le flux automatisé complet ou d'un agent de découverte pour le flux avec préconfiguration manuelle.
   - Découverte du réseau local par l'utilisation de Device Sense ™.
   - Découverte manuelle : par l'utilisation de l'adresse IP ou du nom d'hôte d'un ordinateur, ou par l'importation d'une liste d'ordinateurs à partir d'un fichier.

© Acronis International GmbH, 2003-2026

2. [Pour les découvertes Active Directory (flux avec préconfiguration manuelle) et manuelle] Sélectionnez les ordinateurs que vous souhaitez ajouter à votre tenant.
3. [Pour les découvertes Active Directory et manuelle] Sélectionnez le mode d'ajout de ces ordinateurs :
   - Installez un agent de protection et des composants supplémentaires sur les ordinateurs, et inscrivez-les dans la console Cyber Protect.
   - Inscrivez les ordinateurs dans la console Cyber Protect (si un agent de protection était déjà installé).
   - Ajoutez les ordinateurs à la console Cyber Protect en tant que terminaux non gérés, sans installer d'agent de protection.

   Vous pouvez également appliquer un plan de protection existant aux ordinateurs sur lesquels vous installez un agent de protection ou que vous inscrivez dans la console Cyber Protect.
4. [Pour les découvertes Active Directory (flux avec préconfiguration manuelle) et manuelle] Fourniture d'identifiants d'administrateur pour les ordinateurs sélectionnés.
5. [Pour les découvertes Active Directory (flux avec préconfiguration manuelle) et manuelle] Vérification que vous pouvez vous connecter aux ordinateurs à l'aide des identifiants fournis.

Les ordinateurs qui s'affichent dans la console Cyber Protect entrent dans les catégories suivantes :

- **Terminaux découverts** : ordinateurs découverts, mais sur lesquels l'agent de protection n'est pas installé.
- **Ordinateurs avec agents** : ordinateurs sur lesquels un agent de protection est installé.
- **Terminaux découverts/Terminaux sans agent** : ordinateurs sur lesquels un agent de protection peut être installé.
- **Terminaux découverts/Réseau local** : ordinateurs et terminaux réseau découverts par analyse des réseaux locaux à l'aide de Device Sense ™.
- **Terminaux découverts/Active Directory** : ordinateurs découverts par la recherche dans Active Directory.
- **Terminaux découverts/Manuel/À partir d'un fichier texte** : ordinateurs ajoutés manuellement ou à partir d'un fichier texte.

Exigences de découverte de terminaux

Avant d'utiliser la fonctionnalité de découverte de terminaux, assurez-vous que les exigences suivantes sont respectées :

- Pour le flux **Intégration automatique complète via Active Directory**, au moins un contrôleur de domaine avec un agent de protection installé doit être disponible dans votre réseau local ou votre domaine Active Directory.
- Pour le flux **Préconfiguration manuelle et intégration automatique**, au moins un ordinateur avec un agent de protection installé doit être disponible dans votre réseau local ou votre domaine Active Directory. Cet agent sera utilisé comme agent de découverte.
- L'un des rôles suivants doit vous être attribué pour le service Cyber Protection : cyberadministrateur ou administrateur.

© Acronis International GmbH, 2003-2026

Important
Seuls les agents installés sur des ordinateurs Windows peuvent être des agents de découverte. S'il n'existe aucun agent de découverte dans votre environnement, vous ne pourrez pas utiliser l'option **Terminaux multiples** du panneau **Ajouter des terminaux**.

L'installation à distance des agents est prise en charge uniquement pour les ordinateurs exécutant Windows (Windows XP n'est pas pris en charge). Pour l'installation à distance sur une machine exécutant Windows Server 2012 R2, vous devez avoir la mise à jour Windows KB2999226 installée sur cet ordinateur.

Ajout de plusieurs terminaux

Avant d'ajouter plusieurs terminaux, assurez-vous que les exigences sont remplies. Pour plus d'informations, voir "Exigences de découverte de terminaux" (p. 183).

Remarque
La découverte automatique n'est pas prise en charge pour l'ajout de contrôleurs de domaine en raison des autorisations supplémentaires requises pour l'exécution du service de l'agent.

Rechercher dans Active Directory

Pour ajouter plusieurs terminaux depuis Active Directory

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Découvrir des terminaux**.
   L'assistant de découverte s'ouvre.
4. Sélectionnez l'agent de découverte qui exécutera l'analyse pour détecter les machines.

   Remarque
   Un agent de découverte est une ressource sur laquelle un agent de protection est installé.
   L'agent de découverte doit être un membre du domaine Active Directory.
   Vous pouvez sélectionner un agent associé à l'unité sélectionnée ou à ses unités enfants.

5. Sélectionnez **Rechercher dans Active Directory**, puis cliquez sur **Suivant**.
6. Dans la fenêtre **Rechercher dans Active Directory**, sélectionnez le mode de recherche des ordinateurs, puis cliquez sur **OK**.

Option	Description
Dans une liste d'unités organisationnelles	Sélectionnez le groupe de machines à ajouter.
Par demande de	Servez-vous d'une demande de dialecte LDAP pour sélectionner les machines.

© Acronis International GmbH, 2003-2026

Option	Description
dialecte LDAP.	**Base de recherche** définit où chercher, alors que **Filtre** vous permet de spécifier les critères pour la sélection de la machine.

7. Dans la liste des ordinateurs découverts, sélectionnez les ordinateurs que vous souhaitez ajouter, puis cliquez sur **Suivant**.
   L'onglet **Sélectionner une option d'intégration** s'ouvre. Les options d'intégration suivantes sont disponibles.

Option	Description
Intégration automatique complète via Active Directory	Cette option utilise un contrôleur de domaine dans lequel un agent de découverte est installé pour intégrer des terminaux découverts à partir d'Active Directory. Aucune préconfiguration manuelle des terminaux n'est requise.
Préconfiguration manuelle et intégration automatique	Cette option nécessite la préconfiguration manuelle des terminaux et utilise un agent de découverte pour intégrer les terminaux découverts.
Ajouter en tant que machines non gérées	Cette option ajoute les terminaux découverts à la console en tant que terminaux non gérés, sans installer d'agent de protection sur ces terminaux.

8. En fonction de l'option d'intégration que vous sélectionnez, effectuez les opérations suivantes :
   - Si vous avez sélectionné **Intégration automatique complète via Active Directory**, effectuez les étapes 4 à 13 de la procédure correspondante.
   - Si vous avez sélectionné **Préconfiguration manuelle et intégration automatique**, suivez les étapes 4 à 11 de la procédure correspondante.
   - Si vous avez sélectionné **Ajouter en tant que machines non gérées**, sélectionnez le compte utilisateur sous lequel vous souhaitez enregistrer les terminaux, puis cliquez sur **Ajouter**.

Analyser le réseau local

Pour découvrir plusieurs terminaux en analysant le réseau local

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Découvrir des terminaux**.
   L'assistant de découverte s'ouvre.
4. Cliquez sur **Analyser**.
   La découverte active de terminaux démarre. Vous êtes redirigé vers l'écran **Terminaux découverts** > **Réseau local**. Lorsque l'analyse est terminée, une notification s'affiche ; elle indique le nombre de terminaux découverts lors de l'analyse et inclut un lien vers la liste des terminaux où vous pouvez voir des détails supplémentaires à leur sujet.

© Acronis International GmbH, 2003-2026

Que faire ensuite :

- Vous pouvez cliquer sur le lien **Afficher les nouveaux terminaux découverts** dans la notification, puis afficher les terminaux et les détails à leur sujet dans l'onglet **Réseau local**.
- Vous pouvez installer à distance un agent de protection sur les terminaux découverts et les enregistrer. Pour plus d'informations, voir "Installation d'agents à distance" (p. 200).
- Vous pouvez exclure des terminaux de la découverte. Pour plus d'informations, voir "Exclusion des terminaux de la découverte" (p. 205).

Manuellement ou par importation d'un fichier

Pour ajouter plusieurs terminaux manuellement ou par importation d'un fichier

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Découvrir des terminaux**.
   L'assistant de découverte s'ouvre.
4. Cliquez sur **Spécifier manuellement ou importer à partir d'un fichier**.
5. Ajoutez des ordinateurs en utilisant l'une des options suivantes.
   - Pour ajouter des ordinateurs manuellement :
     a. Dans le champ **Ajouter un ordinateur**, saisissez l'adresse IPv4 ou le nom d'hôte de l'ordinateur.
     b. Répétez l'étape précédente pour chaque ordinateur à ajouter.
   - Pour ajouter des ordinateurs par importation d'un fichier :
     a. Cliquez sur **Importer la liste des ordinateurs depuis un fichier**.
     b. Dans la fenêtre **Importer la liste des ordinateurs depuis un fichier**, déposez le fichier texte contenant la liste des ordinateurs ou cliquez sur **Parcourir**, accédez au fichier, sélectionnez-le, puis cliquez sur **Ouvrir**.
     Le fichier doit contenir des adresses IP ou des noms d'hôte, un par ligne. Voici un exemple du contenu du fichier :

     ```
     156.85.34.10
     156.85.53.32
     156.85.53.12
     EN-L00000100
     EN-L00000101
     ```

   Après l'ajout manuel ou l'importation d'ordinateurs à partir d'un fichier, l'agent essaie d'envoyer une commande ping aux ordinateurs ajoutés et de définir leur disponibilité.
6. Cliquez sur **Suivant**.
   L'onglet **Sélectionner une option d'intégration** s'ouvre. Les options d'intégration suivantes sont disponibles.

© Acronis International GmbH, 2003-2026

Option	Description
Intégration automatique complète via Active Directory	Cette option utilise un contrôleur de domaine dans lequel un agent de découverte est installé pour intégrer des terminaux découverts à partir d'Active Directory. Aucune préconfiguration manuelle des terminaux n'est requise.
Préconfiguration manuelle et intégration automatique	Cette option nécessite la préconfiguration manuelle des terminaux et utilise un agent de découverte pour intégrer les terminaux découverts.
Ajouter en tant que machines non gérées	Cette option ajoute les terminaux découverts à la console en tant que terminaux non gérés, sans installer d'agent de protection sur ces terminaux.

7. En fonction de l'option d'intégration que vous sélectionnez, effectuez les opérations suivantes :
   - Si vous avez sélectionné **Intégration automatique complète via Active Directory**, effectuez les étapes 4 à 13 de la procédure correspondante.
   - Si vous avez sélectionné **Préconfiguration manuelle et intégration automatique**, suivez les étapes 4 à 11 de la procédure correspondante.
   - Si vous avez sélectionné **Ajouter en tant que machines non gérées**, sélectionnez le compte utilisateur sous lequel vous souhaitez enregistrer les terminaux, puis cliquez sur **Ajouter**.

Exigences pour le contrôle de compte d'utilisateur (UAC)

Sur un ordinateur qui exécute Windows 7 ou une version ultérieure et qui n'est pas membre d'un domaine Active Directory, les opérations de gestion centralisée (y compris l'installation à distance) nécessitent que le contrôle de compte utilisateur (UAC) et ses restrictions à distance soient désactivés.

Pour désactiver l'UAC

Effectuez l'une des opérations suivantes en fonction du système d'exploitation :

- **Pour un système d'exploitation Windows antérieur à Windows 8 :**
  Accédez à **Panneau de configuration** > **Afficher par : Petites icônes** > **Comptes d'utilisateur** > **Modifier les paramètres du Contrôle de compte d'utilisateur**, puis déplacez le curseur sur **Ne jamais m'avertir**. Ensuite, redémarrez la machine.
- **Pour tout système d'exploitation Windows** :
  1. Ouvrez l'Éditeur du Registre
  2. Localisez la clé de registre suivante : **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Pour la valeur **EnableLUA**, modifiez la valeur du paramètre à **0**.
  4. Redémarrez la machine.

Pour désactiver les restrictions à distance UAC

© Acronis International GmbH, 2003-2026

1. Ouvrez l'Éditeur du Registre
2. Localisez la clé de registre suivante : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Pour la valeur **LocalAccountTokenFilterPolicy**, modifiez la valeur du paramètre sur **1**.

   Si la valeur **LocalAccountTokenFilterPolicy** n'existe pas, créez-en une en DWORD (32 bits). Pour plus d'informations sur cette valeur, reportez-vous à la documentation de Microsoft : https://support.microsoft.com/fr-fr/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Remarque
Pour des raisons de sécurité, nous vous recommandons de rétablir l'état d'origine des deux paramètres après la fin d'une opération de gestion (par exemple, une installation à distance) : **EnableLUA**=**1** et **LocalAccountTokenFilterPolicy** = **0**

Composants d'agent

Lorsque vous ajoutez plusieurs terminaux découverts par une recherche dans Active Directory, vous pouvez choisir d'installer les composants supplémentaires.

Le tableau suivant fournit des informations supplémentaires sur les composants d'agent que vous pouvez installer.

Composant	Description
Composant obligatoire	
Agent pour Windows	Cet agent sauvegarde des disques, volumes et fichiers, et sera installé sur des machines Windows. Il sera toujours installé. Vous ne pouvez pas le sélectionner.
Composants supplémentaires	
Agent pour empêcher les pertes de données	Cet agent vous permet de limiter l'accès des utilisateurs à des périphériques, ports et presse-papiers locaux et redirigés sur des ordinateurs sur lesquels des plans de protection sont appliqués. Il sera installé s'il est sélectionné.
Protection antimalware et filtrage d'URL Antimalware	Ce composant active la protection antivirus et antimalware et le module de filtrage d'URL dans les plans de protection. Même si vous choisissez de ne pas l'installer, il sera automatiquement installé ultérieurement si l'un de ces modules est activé dans un plan de protection pour l'ordinateur. Ce composant active le module de protection contre les virus et les malwares dans les plans de protection. Même si vous choisissez de ne pas l'installer, il sera automatiquement installé ultérieurement si ce module est activé dans un plan de protection pour l'ordinateur.
Agent pour Hyper-V	Cet agent sauvegarde des machines virtuelles Hyper-V et est installé sur des hôtes Hyper-V. Il est installé s'il est sélectionné et si un rôle Hyper-V est détecté sur une machine.

© Acronis International GmbH, 2003-2026

Agent pour SQL	Cet agent sauvegarde des bases de données SQL Server et est installé sur des machines exécutant Microsoft SQL Server. Il est installé s'il est sélectionné et si une application est détectée sur une machine.
Agent pour Exchange	Cet agent sauvegarde des bases de données et boîtes aux lettres Exchange, et est installé sur des machines exécutant le rôle de boîte aux lettres de Microsoft Exchange Server. Il est installé s'il est sélectionné et si une application est détectée sur une machine.
Agent pour Active Directory	Cet agent sauvegarde les données des services de domaine Active Directory et est installé sur des contrôleurs de domaine. Il est installé s'il est sélectionné et si une application est détectée sur une machine.
Agent pour VMware (Windows)	Cet agent sauvegarde des machine virtuelles VMware et est installé sur des machines Windows ayant un accès réseau à vCenter Server. Il est installé s'il est sélectionné.
Agent pour Microsoft 365	Cet agent sauvegarde des boîtes aux lettres Microsoft 365 vers une destination locale et est installé sur des machines Windows. Il est installé s'il est sélectionné.
Agent pour Oracle	Cet agent sauvegarde des bases de données Oracle et est installé sur des machines exécutant Oracle Database. Il est installé s'il est sélectionné.
Cyber Protection Monitor	Ce composant permet à un utilisateur de contrôler l'exécution des tâches en cours dans la zone de notification, et est installé sur des machines Windows. Il est installé s'il est sélectionné. Pris en charge sur Windows 7 Service Pack 1 et versions ultérieures et Windows Server 2008 R2 Service Pack 1 et versions ultérieures.
Outil de ligne de commande	Prend en charge l'interface de ligne de commande avec l'utilitaire **acrocmd**. **acrocmd** ne contient aucun outil exécutant physiquement les commandes. Il ne fait que fournir l'interface de ligne de commande aux composants de Cyber Protect — agents et serveur de gestion.
Bootable Media Builder	Crée un support de démarrage. Compatible avec Windows et Linux.

Découverte de terminaux à l'aide de Device Sense ™

Device Sense ™ utilise une combinaison sophistiquée de techniques pour analyser les réseaux locaux des organisations, et découvrir et identifier les terminaux. Outre la découverte des ordinateurs et tablettes physiques et virtuels, Device Sense ™ découvre également d'autres terminaux réseau tels que les routeurs, les commutateurs, les imprimantes, les smartphones et les caméras IP.

Grâce à Device Sense ™, vous pouvez obtenir :

© Acronis International GmbH, 2003-2026

- Une visibilité réseau complète : identification de chaque terminal connecté au réseau d'un client. Cela vous aide à gérer un inventaire des ressources précis et à gérer et prendre en charge efficacement votre infrastructure informatique. C'est essentiel pour le suivi des ressources et la gestion du cycle de vie, et garantit également la conformité avec les contrats de licence.
- La sécurité et la conformité : détection des terminaux non autorisés ou malveillants qui pourraient créer des risques de sécurité. Device Sense ™ vous aide à garantir que chaque terminal du réseau est conforme aux stratégies de sécurité et aux exigences réglementaires.
- L'allocation efficace des ressources : compréhension du champ d'application et de la taille du réseau d'un client, ce qui permet d'allouer les ressources plus efficacement et de mieux planifier les services.

La détection de terminaux à l'aide de Device Sense ™ inclut les fonctionnalités suivantes :

- Sélection automatique et intelligente des agents et des réseaux à analyser
- Blocage de la découverte de terminaux dans les réseaux de particuliers ou non professionnels

Remarque
La découverte passive à l'aide de Device Sense ™ n'analyse pas les réseaux dont le nombre d'agents est inférieur au nombre spécifié dans le paramètre **Empêcher la découverte de terminaux dans les réseaux non professionnels**. Au niveau du centre de données, la valeur préconfigurée pour ce paramètre est 3, mais la valeur est héritée du tenant de valeur supérieure et peut différer. Pour vous assurer que la découverte passive analyse tous les réseaux d'entreprise, vous pouvez mettre à jour le paramètre en fonction de votre organisation. Pour plus d'informations, voir "Configuration de la découverte passive de terminaux" (p. 191).

- Découverte active de terminaux à la demande
- Catégorisation des terminaux par type
- Options avancées de recherche et de filtrage pour parcourir les terminaux découverts
- Détails complets sur les terminaux découverts
- Installation à distance de l'agent de protection sur les terminaux découverts, avec application de différents types de plans
- Rapport étendu sur les terminaux découverts

Vous pouvez utiliser Device Sense ™ pour effectuer une découverte passive ou active de terminaux. Pour plus d'informations, voir "Découverte passive de terminaux à l'aide de Device Sense ™" (p. 191) et "Découverte active de terminaux à l'aide de Device Sense ™" (p. 192).

Remarque
La période de rétention dans la base de données des informations sur les terminaux découverts est de 3 mois.

© Acronis International GmbH, 2003-2026

Découverte passive de terminaux à l'aide de Device Sense ™

La découverte passive de terminaux est une méthode non intrusive qui permet d'identifier et de cataloguer des terminaux dans un environnement réseau, sans sonder activement ni envoyer des demandes à ces terminaux du réseau d'entreprise.

La découverte passive de terminaux collecte les données suivantes :

- Nom du terminal
- Type de terminal
- Famille de système d'exploitation
- Fabricant
- Modèle
- Adresse MAC
- Adresse IP

Les paramètres de découverte passive sont préconfigurés au niveau du centre de données. Un administrateur d'entreprise peut personnaliser ces paramètres pour tous les terminaux d'une entreprise ou d'une unité. Si aucun paramètre personnalisé n'est appliqué, les paramètres du niveau supérieur sont utilisés, dans l'ordre suivant :

1. Centre de données Cyber Protection
2. Entreprise (tenant client)
3. Unité

Par exemple, un administrateur d'unité peut configurer des paramètres de découverte personnalisée de terminaux pour l'unité qui peuvent différer du paramètre appliqué au niveau de l'entreprise.

Configuration de la découverte passive de terminaux

La découverte passive de terminaux analyse en continu les réseaux d'entreprise à la recherche de terminaux. Grâce à la découverte passive des terminaux :

- Les partenaires peuvent avoir une visibilité sur les réseaux des clients, et sur le nombre et le type de terminaux disponibles dans ces réseaux.
- Les clients peuvent avoir une visibilité sur les réseaux de leur organisation et le nombre et le type de terminaux disponibles sur ces réseaux.

Pour configurer les paramètres de découverte de terminaux passifs

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Gestion**.
2. Cliquez sur l'onglet **Découverte de terminaux passifs**.
3. Vérifiez que le paramètre **Activer la découverte passive des terminaux** est activé.

© Acronis International GmbH, 2003-2026

Le système affecte automatiquement des agents Windows en tant qu'agents de découverte.

4. [Facultatif] Modifiez les paramètres par défaut.

Paramètre	Description
Sélection automatique intelligente des agents de découverte	Nombre d'agents qui seront sélectionnés automatiquement pour effectuer la recherche passive des terminaux dans le réseau local. La valeur par défaut est 1.* La valeur maximale est 3.
Empêcher la découverte de terminaux dans les réseaux non professionnels	Nombre minimum d'agents devant être présents dans un réseau pour le classifier comme environnement professionnel et activer son analyse. La valeur par défaut est 3.* La valeur maximale est 1000.
Identification améliorée des terminaux dans un réseau	Activez ou désactivez l'utilisation de signaux multidiffusion, pour une identification plus précise des types de terminaux intégrant le réseau local. Par défaut, le paramètre est désactivé.*

* La valeur par défaut peut différer en fonction de la configuration d'un tenant de niveau supérieur. Les valeurs par défaut sont héritées et sont identiques à celles définies pour le tenant de niveau supérieur. Vous pouvez néanmoins les modifier en fonction des besoins de votre organisation.

5. Cliquez sur **Enregistrer**.

Découverte active de terminaux à l'aide de Device Sense ™

La découverte active de terminaux est une méthode utilisée dans la gestion de réseau, dans laquelle un système sonde activement les terminaux d'un réseau et établit la communication avec eux pour les identifier et recueillir des informations les concernant.

Vous pouvez récupérer des données complètes et précises sur les terminaux des réseaux, ce qui garantit que toutes les informations sur les terminaux sont claires et visibles.

La découverte de terminaux actifs collecte les données suivantes concernant les terminaux :

- Nom du terminal
- Type de terminal
- Famille de système d'exploitation
- Fabricant
- Modèle
- Adresse IP
- Adresse MAC

Exécution d'une analyse active à la recherche de terminaux à l'aide de Device Sense ™

Vous pouvez exécuter une analyse active pour une collecte de données complète et l'identification des terminaux connectés au réseau local.

© Acronis International GmbH, 2003-2026

Pour exécuter une analyse active

1. Dans la console Protection, accédez à **Terminaux** >**Terminaux détectés**.
2. Cliquez sur l'onglet **Réseau local**.
3. Cliquez sur **Exécuter une analyse active**.
4. Sélectionnez le réseau dans lequel exécuter l'analyse active, puis cliquez sur **Exécuter**.
5. Dans le champ **Tenant**, sélectionnez le tenant.
6. Dans le champ **Agent de découverte**, sélectionnez une ressource enregistrée dans le tenant. L'agent de protection installé sur cette ressource sera utilisé comme agent de découverte.
7. Cliquez sur **Exécuter**.

   La découverte de terminaux actifs démarre. Lorsque l'analyse est terminée, une notification s'affiche. Elle indique le nombre de terminaux découverts lors de l'analyse et inclut un lien vers la liste des terminaux où vous pouvez voir des détails supplémentaires à leur sujet.

Remarque
Vous ne pouvez pas exécuter plusieurs analyses actives simultanément. Si une analyse active est en cours, vous devez l'annuler ou attendre qu'elle soit terminée avant de pouvoir démarrer une nouvelle analyse.

Ports utilisés par Device Sense ™

Cette rubrique répertorie les ports utilisés par Device Sense ™.

La découverte passive des terminaux utilise les ports suivants.

Nom	Port	Commentaire
DHCP	udp/67	Écoute les REQUEST messages
NBNS	udp/137	Écoute les NAME REGISTRATION REQUEST et NAME REFRESH REQUEST paquets
NBDS (Browser)	udp/138	Écoute les messages d'annonce
SSDP	udp/1900	Écoute les M-SEARCH et NOTIFY messages
WSD	udp/3702	Écoute les wsd:Probe messages
MDNS	udp/5353	Écoute diverses annonces d'informations sur les services
LLMNR	udp/5355	Écoute les requêtes
TUYA	udp/6668	Écoute les paquets de découverte

Lorsque l'option **Identification améliorée des terminaux sur un réseau** est activée, Device Sense ™ utilise les ports suivants.

© Acronis International GmbH, 2003-2026

Nom	Ports	Commentaire
SSDP	udp/1900	Envoie M-SEARCH requêtes
WSD	udp/3702	Envoie wsd:Probe requêtes

La découverte des terminaux actifs (flux d'analyse à la demande) utilise les ports suivants.

Nom	Ports	Commentaire
FTP	tcp/21	Lit les bannières de service
SSH	tcp/22	Lit les bannières de service
TELNET	tcp/23	Lit les bannières
SMTP	tcp/25 , tcp/587	Lit EHLO messages
RDNS	udp/53	Effectue une requête DNS inversée `*.in-addr.arpa`
HTTP	tcp/80 , tcp/8080 et d'autres ports HTTP courants	Envoie GET requêtes
NBNS	udp/135	Envoie NBSTAT requêtes
SNMP	udp/161	Lit MIBs : Versions : v1, v2c ; Communautés : publique
HTTPS	tcp/443 , tcp/8443	Envoie GET requêtes
SMB	tcp/445	Extrait les données de NTLMv2 auth messages
RTSP	tcp/554	Envoie OPTIONS requêtes
SSDP	udp/1900	Envoie M-SEARCH
ARD	udp/3283	Envoie Start paquets
RDP	tcp/3389	Envoie Connection Request et lit Connection Confirm
WSD	udp/3702	Envoie wsd:Probe messages
AirPlay	tcp/5000 , tcp/7000	Envoie wsd:Probe messages
MDNS	udp/5353	Envoie PTR messages
iRobot	udp/5678	Envoie iRobot paquets de découverte irobotmsc
VNC	udp/5900	Envoie RFB ProtocolVersion et messages de sécurité

© Acronis International GmbH, 2003-2026

Nom	Ports	Commentaire
MIIO	udp/54321	Envoie Hello paquets

Affichage des informations sur les terminaux découverts

Vous pouvez utiliser les filtres intégrés dans la page **Terminaux découverts** pour trouver rapidement des terminaux spécifiques dans la liste et afficher leurs détails.

Pour trouver un terminal découvert et afficher ses détails

1. Dans la console Protection, cliquez sur **Terminaux découverts**.
   Par défaut, l'onglet **Terminaux sans agent** s'ouvre.
2. [Facultatif] Pour rechercher des terminaux d'une catégorie spécifique, cliquez sur l'onglet correspondant.

Onglet	Description
Terminaux sans agent	Cet onglet répertorie tous les ordinateurs découverts sur lesquels un agent de protection peut être installé, quelle que soit la méthode de découverte utilisée.
Active Directory	Cet onglet répertorie les ordinateurs découverts par analyse d'Active Directory.
Réseau local	Cet onglet répertorie les terminaux (ordinateurs ou autres terminaux réseau) découverts par analyse des réseaux d'entreprise locaux à l'aide de Device Sense ™.
Manuel/Depuis un fichier texte	Cet onglet répertorie les ordinateurs découverts manuellement ou à partir d'un fichier texte.
Exclusions	Cet onglet répertorie les terminaux exclus de la découverte.

3. [Facultatif] Pour effectuer une recherche par nom de terminal, saisissez le nom du terminal dans le champ **Recherche**.
   Les résultats de la liste sont filtrés dynamiquement.
4. [Facultatif] Pour rechercher les résultats à l'aide de filtres, cliquez sur **Filtre**, sélectionnez un ou plusieurs filtres, puis cliquez sur **Appliquer**.

Filtre	Description
Type de terminal	Pour rechercher un ou plusieurs types de terminaux, cliquez sur le champ, puis sélectionnez les types de terminaux pertinents dans la liste. Ce filtre n'est pas disponible dans l'onglet **Manuel/Depuis un fichier texte**.
Type de	Pour filtrer les résultats en fonction de la méthode de découverte,

© Acronis International GmbH, 2003-2026

Filtre	Description
découverte	cliquez sur le champ, puis sélectionnez l'une des méthodes suivantes. • **Active Directory** • **Manuel** • **Réseau local passif** • **Réseau local actif** Ce filtre est disponible uniquement dans l'onglet **Terminaux sans agent**.
Adresse MAC	Pour rechercher un terminal disposant d'une adresse MAC spécifique, entrez cette adresse MAC dans ce champ. Ce filtre n'est pas disponible dans l'onglet **Manuel/Depuis un fichier texte**.
Plage d'adresses IP	Pour filtrer les résultats en fonction de l'adresse IP du terminal, entrez l'adresse IP de début dans le premier champ et l'adresse IP de fin dans le second champ.
Première découverte	Pour filtrer les résultats en fonction de la date à laquelle le terminal a été découvert initialement, cliquez dans le champ, puis utilisez une plage prédéfinie ou personnalisée.
Dernière découverte	Pour filtrer les résultats en fonction de la date à laquelle le terminal a été découvert pour la dernière fois, cliquez dans le champ, puis utilisez une plage prédéfinie ou personnalisée.
Unité d'organisation	Unité d'organisation Active Directory à laquelle le terminal appartient. Ce filtre est disponible uniquement dans l'onglet **Active Directory**.

5. Cliquez sur le terminal, puis sur **Détails**.
6. Dans le volet **Données brutes**, cliquez sur l'icône en forme de flèche.
7. Pour télécharger les données brutes dans un fichier JSON, cliquez sur **Télécharger**.
   Le fichier est enregistré dans le répertoire de téléchargement par défaut sur l'ordinateur partir duquel vous vous êtes connecté à la console Protection.

Installation à distance des agents

Après le processus de découverte des terminaux, vous pouvez effectuer l'installation à distance des agents sur les terminaux Windows découverts.

L'installation à distance des agents s'effectue de la manière suivante :

1. L'agent de découverte se connecte aux ordinateurs cibles à l'aide du nom d'hôte, de l'adresse IP et des identifiants administrateur indiqués dans l'assistant de découverte, puis transfère le fichier `web_installer.exe` vers ces ordinateurs.
2. Le fichier `web_installer.exe` s'exécute sur l'ordinateur cible en mode sans assistance.

© Acronis International GmbH, 2003-2026

3. Le programme d'installation Web récupère des packages d'installation supplémentaires depuis le cloud, puis les installe sur les machines cibles via la commande `msiexec`.
4. Une fois l'installation terminée, les composants sont inscrits dans le cloud.

Remarque
L'installation à distance des agents n'est pas prise en charge pour les contrôleurs de domaine en raison des autorisations supplémentaires requises pour l'exécution du service de l'agent.

Préparation des ordinateurs pour l'installation à distance manuelle

- Pour une installation réussie sur une machine distante exécutant Windows 7 ou version ultérieure, l'option **Panneau de configuration** > **Options des dossiers** > **Affichage** > **Utiliser l'assistant de partage** doit être *désactivée* sur cet ordinateur.
- Pour une installation réussie sur un ordinateur distant *non membre* d'un domaine Active Directory, le contrôle de compte utilisateur (CCU) doit être *désactivé* sur cet ordinateur. Pour plus d'informations sur sa désactivation, consultez Exigences pour le contrôle de compte utilisateur (UAC) > Pour désactiver l'UAC.
- Par défaut, les identifiants du compte administrateur intégré sont requis pour l'installation à distance sur toute machine Windows. Pour effectuer l'installation à distance en utilisant les identifiants d'un autre compte administrateur, les restrictions à distance de contrôle de compte utilisateur (UAC) doivent être *désactivées*. Pour plus d'informations sur leur désactivation, voir Exigences pour le contrôle de compte utilisateur (UAC) > Pour désactiver les restrictions à distance UAC.
- Le partage des fichiers et d'imprimantes doit être *activé* sur la machine distante. Pour accéder à cette option :
  - Sur un ordinateur exécutant Windows 2003 Server : accédez au **Panneau de configuration** > **Pare-feu Windows** > **Exceptions** > **Partage de fichiers et d'imprimantes**.
  - Sur un ordinateur exécutant Windows Server 2008, Windows 7 ou une version ultérieure : accédez au **Panneau de configuration** > **Pare-feu Windows** > **Centre de réseau et de partage** > **Modifier les paramètres de partage avancés**.
- Cyber Protection utilise les ports TCP 445, 25001 et 43234 pour l'installation à distance.
  Le port 445 s'ouvre automatiquement lorsque vous activez le partage de fichiers et d'imprimantes. Les ports 43234 et 25001 s'ouvrent automatiquement dans le pare-feu Windows. Si vous utilisez un autre pare-feu, assurez-vous que ces trois ports sont ouverts (ajoutés aux exceptions) pour les demandes entrantes et sortantes.
  Une fois l'installation à distance terminée, le port 25001 est fermé automatiquement par le pare-feu Windows. Les ports 445 et 43234 doivent rester ouverts si vous souhaitez mettre à jour l'agent à distance à l'avenir. Le port 25001 est ouvert et fermé automatiquement par le pare-feu Windows lors de chaque mise à jour. Si vous utilisez un pare-feu différent, laissez les trois ports ouverts.

© Acronis International GmbH, 2003-2026

Préparation des ordinateurs pour une installation à distance à l'aide d'un objet de stratégie de groupe (GPO)

Vous pouvez configurer et appliquer un objet de stratégie de groupe (GPO) Active Directory pour préparer un ensemble d'ordinateurs membres d'Active Directory à l'installation à distance des agents Protection.

Prérequis

- Votre utilisateur est membre du groupe des administrateurs de domaine ou est administrateur de domaine.
- La **console de gestion des stratégies de groupe** (GPMC) est installée sur l'ordinateur sur lequel vous êtes connecté pour créer l'objet de stratégie de groupe (GPO).

Pour préparer des ordinateurs à l'installation à distance à l'aide d'un objet de stratégie de groupe (GPO)

1. Pour ouvrir GPMC, appuyez sur **Win** + **R**, tapez `gpmc.msc`, puis appuyez sur **Entrée**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur le domaine ou l'unité d'organisation (OU) auquel vous voulez appliquer un objet de stratégie de groupe (GPO).
3. Cliquez sur **Créer un GPO dans ce domaine et le lier ici...**
4. Dans la fenêtre contextuelle **Nouveau GPO**, saisissez un nom pour le GPO, puis cliquez sur **OK**.
5. Dans l'arborescence de la console, cliquez avec le bouton droit sur le GPO que vous avez créé à l'étape précédente, puis cliquez sur **Modifier...**
6. Désactivez **Utiliser l'assistant de partage** en suivant les étapes ci-dessous.
   a. Dans l'arborescence de la console, accédez à **Configuration utilisateur** > **Préférences** > **Paramètres Windows** > **Registre**.
   b. Cliquez avec le bouton droit sur **Registre**, puis cliquez sur **Nouveau** > **Élément de registre**.
   c. Dans la fenêtre **Nouvelles propriétés du registre**, onglet **Général**, configurez l'élément du registre comme suit.

Paramètre	Valeur
Action	Mise à jour
Hive	`HKEY_CURRENT_USER`
Chemin d'accès de la clé	Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Nom de la valeur	SharingWizardOn
Type de valeur	`REG_DWORD`
Données de la valeur	0

© Acronis International GmbH, 2003-2026

d. Cliquez sur **Appliquer**, puis sur **OK**.

7. [Pour Windows Vista et les versions ultérieures] Désactivez le contrôle de compte d'utilisateur (UAC) en suivant les étapes ci-dessous.
   a. Dans l'arborescence de la console, accédez à **Configuration de l'ordinateur** > **Préférences** > **Paramètres Windows** > **Registre**.
   b. Cliquez avec le bouton droit sur **Registre**, puis cliquez sur **Nouveau** > **Élément de registre**.
   c. Dans la fenêtre **Nouvelles propriétés du registre**, onglet **Général**, configurez l'élément du registre comme suit.

Paramètre	Valeur
Action	Mise à jour
Hive	HKEY_LOCAL_MACHINE
Chemin d'accès de la clé	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
Nom de la valeur	EnableLUA
Type de valeur	REG_DWORD
Données de la valeur	0

   d. Cliquez sur **Appliquer**, puis sur **OK**.

8. [Pour Windows Vista et les versions ultérieures] Désactivez les restrictions à distance du contrôle de compte d'utilisateur (UAC) en suivant les étapes ci-dessous.
   a. Dans l'arborescence de la console, accédez à **Configuration de l'ordinateur** > **Préférences** > **Paramètres Windows** > **Registre**.
   b. Cliquez avec le bouton droit sur **Registre**, puis cliquez sur **Nouveau** > **Élément de registre**.
   c. Dans la fenêtre **Nouvelles propriétés du registre**, onglet **Général**, configurez l'élément du registre comme suit.

Paramètre	Valeur
Action	Mise à jour
Hive	HKEY_LOCAL_MACHINE
Chemin d'accès de la clé	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Nom de la valeur	LocalAccountTokenFilterPolicy
Type de valeur	REG_DWORD
Données de la valeur	1

   d. Cliquez sur **Appliquer**, puis sur **OK**.

© Acronis International GmbH, 2003-2026

9. Activez le **partage de fichiers et d'imprimantes** en suivant les étapes ci-dessous.
   a. Dans l'arborescence de la console, accédez à **Configuration de l'ordinateur** > **Stratégies** > **Paramètres Windows** > **Paramètres de sécurité** > **Pare-feu Windows Defender avec sécurité avancée** > **Règles de trafic entrant**.
   b. Cliquez avec le bouton droit sur **Règles de trafic entrant**, puis cliquez sur **Nouvelle règle**.
   c. Dans l'**Assistant Nouvelle règle entrante**, configurez la règle comme suit.
   d. Dans l'onglet **Type de règle**, sélectionnez **Prédéfini** et **Partage de fichiers et d'imprimantes**, puis cliquez sur **Suivant**.
   e. Dans l'onglet **Règles prédéfinies**, cliquez sur **Suivant**.
   f. Dans l'onglet **Action**, sélectionnez **Autoriser la connexion**, puis cliquez sur **Terminer**.
   g. Dans l'arborescence de la console, accédez à **Configuration de l'ordinateur** > **Stratégies** > **Paramètres Windows** > **Paramètres de sécurité** > **Pare-feu Windows Defender avec sécurité avancée** > **Règles de sortie**.
   h. Cliquez avec le bouton droit sur **Règles de sortie**, puis sélectionnez **Nouvelle règle**.
   i. Dans l'**Assistant Nouvelle règle de sortie**, configurez la règle en effectuant les mêmes actions qu'aux étapes d à f.
10. Liez l'objet de stratégie de groupe (GPO) au domaine ou à l'OU, en suivant les étapes ci-dessous.
   a. Dans l'arborescence de la console, cliquez avec le bouton droit sur le domaine ou l'OU cible, puis cliquez sur **Lier un GPO existant...**
   b. Dans l'écran **Sélectionner un GPO**, sélectionnez l'objet de stratégie de groupe (GPO) que vous avez créé, puis cliquez sur **OK**.
11. Sur les machines cibles que vous souhaitez préparer pour une installation d'agent à distance, forcez la mise à jour de la stratégie de groupe en suivant les étapes ci-dessous.
   a. Exécutez l'**invite de commandes** en tant qu'administrateur.
   b. Exécuter la commande suivante :
      ```
      gpupdate /force
      ```

Installation d'agents à distance

Remarque
L'installation à distance d'agents est prise en charge pour les terminaux Windows uniquement.

L'installation d'un agent sur plusieurs terminaux n'est disponible que pour les terminaux d'un même réseau et découverts par la même méthode de découverte.

Vous pouvez intégrer simultanément et à distance plusieurs terminaux découverts. Le processus d'intégration consiste à installer l'agent, à appliquer des plans et à procéder à l'inscription du terminal.

Intégration automatique complète via Active Directory

Prérequis

© Acronis International GmbH, 2003-2026

Au moins un contrôleur de domaine sur lequel un agent de protection est installé doit être disponible dans Active Directory.

Pour ajouter plusieurs terminaux en utilisant l'intégration automatisée complète via Active Directory

1. Dans la console Protection, accédez à **Terminaux** > **Terminaux découverts** > **Terminaux sans agent**.
2. Sélectionnez les terminaux que vous souhaitez protéger.
3. Cliquez sur **Installer l'agent**.
4. Dans l'onglet **Sélectionner l'option d'intégration**, cliquez sur **Intégration automatique complète via Active Directory**.
5. Dans le champ **Contrôleur de domaine**, sélectionnez le contrôleur de domaine.
6. Dans le champ **Identifiants de l'administrateur de domaine**, cliquez sur **Sélectionner**.
7. Dans l'écran **Liste des identifiants**, sélectionnez les identifiants du compte d'administrateur du contrôleur de domaine, puis cliquez sur **Sélectionner les identifiants**.
   Le contrôleur de domaine analyse Active Directory pour les terminaux et les affiche dans une liste. Par défaut, tous les terminaux découverts sont présélectionnés, mais vous pouvez désélectionner ceux que vous ne souhaitez pas enregistrer ni protéger.
8. Dans la liste des terminaux, assurez-vous que les terminaux que vous souhaitez intégrer sont sélectionnés.
9. Cliquez sur **Suivant**.
10. Dans l'onglet **Sélectionner les composants de l'agent**, effectuez les opérations suivantes :
    a. Pour sélectionner les composants à installer, cliquez sur **Composants à installer**, puis sélectionnez-les. Pour plus d'informations sur les composants disponibles, voir "Composants d'agent" (p. 188).
    b. Dans le volet **Paramètres**, configurez les options d'installation.

Option	Description
Compte d'ouverture de session du service	Compte sous lequel les services s'exécuteront. Par défaut, l'option **Utiliser les comptes d'utilisateurs de service** est sélectionnée. Pour modifier la valeur par défaut, cliquez sur **Modifier**. Pour en savoir plus sur toutes les options, voir "Changer le compte de connexion sur les machines Windows" (p. 66).
Redémarrer le terminal si nécessaire	Sélectionnez cette option si vous souhaitez que le terminal redémarre lorsque l'installation d'un composant le nécessite.
Ne pas redémarrer le terminal si un utilisateur est connecté	Sélectionnez cette option si vous ne souhaitez pas que le terminal soit redémarré lorsqu'un utilisateur y est connecté.

© Acronis International GmbH, 2003-2026

c. Sélectionnez un compte utilisateur sous lequel vous souhaitez enregistrer les terminaux.

d. Cliquez sur **Suivant**.

11. [Facultatif] Pour sélectionner les plans qui seront appliqués automatiquement aux ordinateurs, cliquez dans l'onglet **Sélectionner des plans** sur l'option **Modifier** du champ de sélection du type de plan correspondant, sélectionnez le plan, puis cliquez une nouvelle fois sur **Modifier**.

Remarque
La sélection de plan est autorisée uniquement si l'authentification à deux facteurs (2FA) est configurée pour le tenant. Si cette authentification n'est pas configurée, vous devez d'abord le faire, puis vous connecter à la console Cyber Protect et démarrer cette procédure depuis le début.

12. Cliquez sur **Suivant**.
13. Dans l'écran **Examiner et enregistrer**, vérifiez les quotas requis, puis effectuez l'une des opérations suivantes :
    - Pour sélectionner différents plans, accédez à l'onglet **Sélectionner des plans**, suivez la procédure à l'étape 11, puis cliquez sur **Suivant** jusqu'à ce que vous reveniez à l'écran **Examiner et enregistrer**.
    - Pour enregistrer les ressources, cliquez sur **Enregistrer**.
      - Si vous êtes connecté en tant qu'administrateur partenaire, tous les packs Advanced requis seront automatiquement activés pour le tenant dans lequel vous enregistrez la ressource.
      - Si vous n'êtes pas connecté en tant qu'administrateur partenaire, aucun pack Advanced requis ne sera activé automatiquement. Vous pouvez toujours appliquer les plans sélectionnés, mais ils peuvent ne pas fonctionner correctement. Pour résoudre ce problème, demandez à votre administrateur partenaire d'activer les packs Advanced requis ou de modifier les plans présélectionnés.

Préconfiguration manuelle et intégration automatique

Prérequis

Les terminaux que vous souhaitez ajouter sont configurés pour l'installation de l'agent à distance, comme le décrit "Préparation des ordinateurs pour une installation à distance à l'aide d'un objet de stratégie de groupe (GPO)" (p. 198).

Pour ajouter plusieurs terminaux en utilisant la préconfiguration manuelle et l'intégration automatique

1. Dans la console Protection, accédez à **Terminaux** > **Terminaux découverts** > **Terminaux sans agent**.
2. Sélectionnez les terminaux que vous souhaitez protéger.
3. Cliquez sur **Installer l'agent**.
4. Dans l'onglet **Sélectionner l'option d'intégration**, cliquez sur **Préconfiguration manuelle et intégration automatique**, puis sur **Suivant**.

© Acronis International GmbH, 2003-2026

5. Dans l'onglet **Sélectionner les composants de l'agent**, effectuez les opérations suivantes :
   a. Dans le champ **Agent de découverte**, sélectionnez la ressource qui sera utilisée pour l'installation à distance de l'agent et l'inscription des ordinateurs.

      Remarque
      Un agent de découverte est une ressource sur laquelle un agent de protection est installé.
      Au niveau du client, vous pouvez sélectionner un agent associé à la division sélectionnée.
      Au niveau du partenaire, vous pouvez sélectionner un agent associé au client sélectionné.

   b. Pour sélectionner les composants à installer, cliquez sur **Composants à installer**, puis sélectionnez-les. Pour plus d'informations sur les composants disponibles, voir "Composants d'agent" (p. 188).
   c. Dans le volet **Paramètres**, configurez les options d'installation.

Option	Description
Compte d'ouverture de session du service	Compte sous lequel les services s'exécuteront. Par défaut, l'option **Utiliser les comptes d'utilisateurs de service** est sélectionnée. Pour modifier la valeur par défaut, cliquez sur **Modifier**. Pour en savoir plus sur toutes les options, voir "Changer le compte de connexion sur les machines Windows" (p. 66).
Redémarrer le terminal si nécessaire	Sélectionnez cette option si vous souhaitez que le terminal redémarre lorsque l'installation d'un composant le nécessite.
Ne pas redémarrer le terminal si un utilisateur est connecté	Sélectionnez cette option si vous ne souhaitez pas que le terminal soit redémarré lorsqu'un utilisateur y est connecté.

   d. Sélectionnez un compte utilisateur sous lequel vous souhaitez enregistrer les terminaux.
   e. Cliquez sur **Suivant**.
6. [Facultatif] Pour sélectionner les plans qui seront appliqués automatiquement aux ordinateurs, cliquez dans l'onglet **Sélectionner des plans** sur l'option **Modifier** du champ de sélection du type de plan correspondant, sélectionnez le plan, puis cliquez une nouvelle fois sur **Modifier**.

   Remarque
   La sélection de plan est autorisée uniquement si l'authentification à deux facteurs (2FA) est configurée pour le tenant. Si cette authentification n'est pas configurée, vous devez d'abord le faire, puis vous connecter à la console Cyber Protect et démarrer cette procédure depuis le début.

7. Cliquez sur **Suivant**.
8. Dans l'onglet **Identifiants**, procédez comme suit :

© Acronis International GmbH, 2003-2026

a. Cliquez sur **Ajouter les identifiants**.

b. Sélectionnez les identifiants d'un utilisateur disposant des droits d'administrateur sur les terminaux sélectionnés, puis cliquez sur **Sélectionner les identifiants**.

Important
L'installation à distance d'agents fonctionne sans aucune préparation uniquement si vous spécifiez les identifiants du compte d'administrateur intégré (le premier compte créé lors de l'installation du système d'exploitation). Si vous souhaitez définir des identifiants d'administrateur personnalisés, vous devez effectuer d'autres opérations préparatoires. Pour plus d'informations, voir "Préparation des ordinateurs pour l'installation à distance manuelle" (p. 197).

c. Cliquez sur **Suivant**.

Le système effectue des vérifications préliminaires sur les terminaux sélectionnés pour s'assurer qu'ils sont appropriés et qu'ils disposent de la configuration correcte pour l'installation à distance de l'agent et des composants sélectionnés.

9. Dans l'onglet **Connectivité**, effectuez l'une des opérations suivantes :
   - Si des problèmes de connectivité se posent, résolvez-les en cliquant sur **Changer les identifiants pour tous les terminaux**, puis sur Suivant.
   - Si aucun problème de connectivité n'est identifié, cliquez sur **Suivant**.
10. Dans l'écran **Examiner et enregistrer**, vérifiez les quotas requis, puis effectuez l'une des opérations suivantes :
    - Pour sélectionner différents plans, accédez à l'onglet **Sélectionner des plans**, suivez la procédure à l'étape 6, puis cliquez sur **Suivant** jusqu'à ce que vous reveniez à l'écran **Examiner et enregistrer**.
    - Pour enregistrer les ressources, cliquez sur **Enregistrer**.
      - Si vous êtes connecté en tant qu'administrateur partenaire, tous les packs Advanced requis seront automatiquement activés pour le tenant dans lequel vous enregistrez la ressource.
      - Si vous n'êtes pas connecté en tant qu'administrateur partenaire, aucun pack Advanced requis ne sera activé automatiquement. Vous pouvez toujours appliquer les plans sélectionnés, mais ils peuvent ne pas fonctionner correctement. Pour résoudre ce problème, demandez à votre administrateur partenaire d'activer les packs Advanced requis ou de modifier les plans présélectionnés.

Remarque
Un fichier nommé `RemoteInstallEntryPoint.bat` est déployé sur chaque ressource enregistrée sur le réseau. Ce fichier installe les composants nécessaires pour déployer les agents de protection.

À de rares occasions, les analyses de sécurité peuvent signaler ce fichier comme suspect ou malveillant. Si cela se produit, ajoutez-le à la liste d'autorisation/liste blanche pour que l'installation puisse se terminer avec succès.

© Acronis International GmbH, 2003-2026

Exclusion des terminaux de la découverte

Lorsque vous excluez des terminaux de la découverte, ils ne sont pas répertoriés dans les résultats des terminaux découverts lors de l'exécution d'une découverte de terminaux.

Pour exclure un terminal de la découverte

1. Dans la console Protection, allez dans **Terminaux découverts**.
2. Cliquez sur le terminal que vous voulez exclure de la recherche, puis cliquez sur **Exclure de la recherche**.
   Le terminal est exclu de la recherche et est ajouté à la liste des terminaux dans la page **Exclusions**.

Connexion aux terminaux découverts à distance

Vous pouvez vous connecter à distance aux terminaux Windows ou macOS découverts et fournir une assistance ponctuelle.

Prérequis

- [Pour les connexions RDP] RDP est activé sur le terminal Windows.
- [Pour les connexions Apple Screen Sharing] Apple Screen Sharing est activé sur le terminal macOS.

Pour vous connecter à distance à un terminal découvert

1. Dans la console Cyber Protect, accédez à **Terminaux** >**Terminaux détectés**.
2. Cliquez sur le terminal auquel vous souhaitez vous connecter à distance.
3. Cliquez sur **Bureau à distance**, puis, selon le système d'exploitation du terminal, cliquez sur le mode d'affichage.

Système d'exploitation	Protocole de connexion	Mode d'affichage
Windows	RDP	**Contrôle** - Dans ce mode, vous pourrez observer et effectuer des opérations sur le terminal distant.
macOS	Partage d'écran Apple	**Contrôle** - Dans ce mode, vous pourrez observer et effectuer des opérations sur le terminal distant. **Visualisation uniquement** - Dans ce mode, vous ne pourrez observer que le terminal distant. **Rideau** – disponible uniquement pour les terminaux macOS. Si vous vous connectez au terminal distant en mode rideau, l'écran du terminal distant sera assombri et l'utilisateur distant ne pourra pas voir vos actions sur le terminal.

© Acronis International GmbH, 2003-2026

4. [Si Connect Client n'est pas installé sur votre terminal] Dans la boîte de dialogue **Se connecter à la ressource**, cliquez sur **Télécharger Connect Client**, téléchargez et installez le client sur votre terminal, puis cliquez sur **Connexion**.
5. [Si une fenêtre contextuelle de confirmation apparaît] Cliquez sur **Ouvrir Connect Client**.
6. [Pour les terminaux Windows] Dans la **fenêtre pop-up d'authentification RDP**, entrez le nom d'utilisateur, le mot de passe et le domaine, puis cliquez sur **Connexion**.
7. [Pour les terminaux macOS] Dans la **fenêtre d'authentification**, sélectionnez une option d'authentification, fournissez les identifiants requis selon l'option que vous avez sélectionnée, puis cliquez sur **Connexion**.

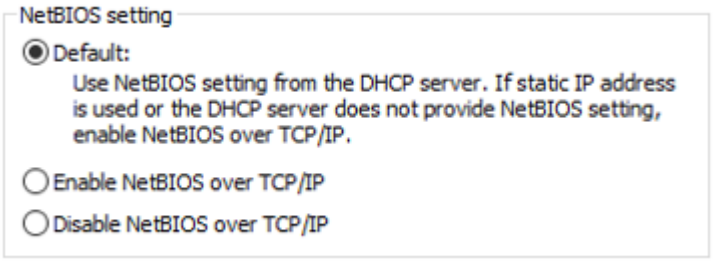
Option d'authentification	Description
Avec les identifiants macOS	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur administrateur du terminal distant.
en demandant à observer	Vous pourrez établir la connexion à distance en mode d'observation lorsque l'utilisateur connecté sur le terminal distant l'ait autorisé.
avec mot de passe VNC	Vous serez autorisé à établir la connexion à distance après avoir fourni le mot de passe VNC.

Remarque
Les options d'authentification que vous verrez dépendent des options de partage d'écran configurées sur le terminal macOS distant.

Dépannage de la découverte de terminaux

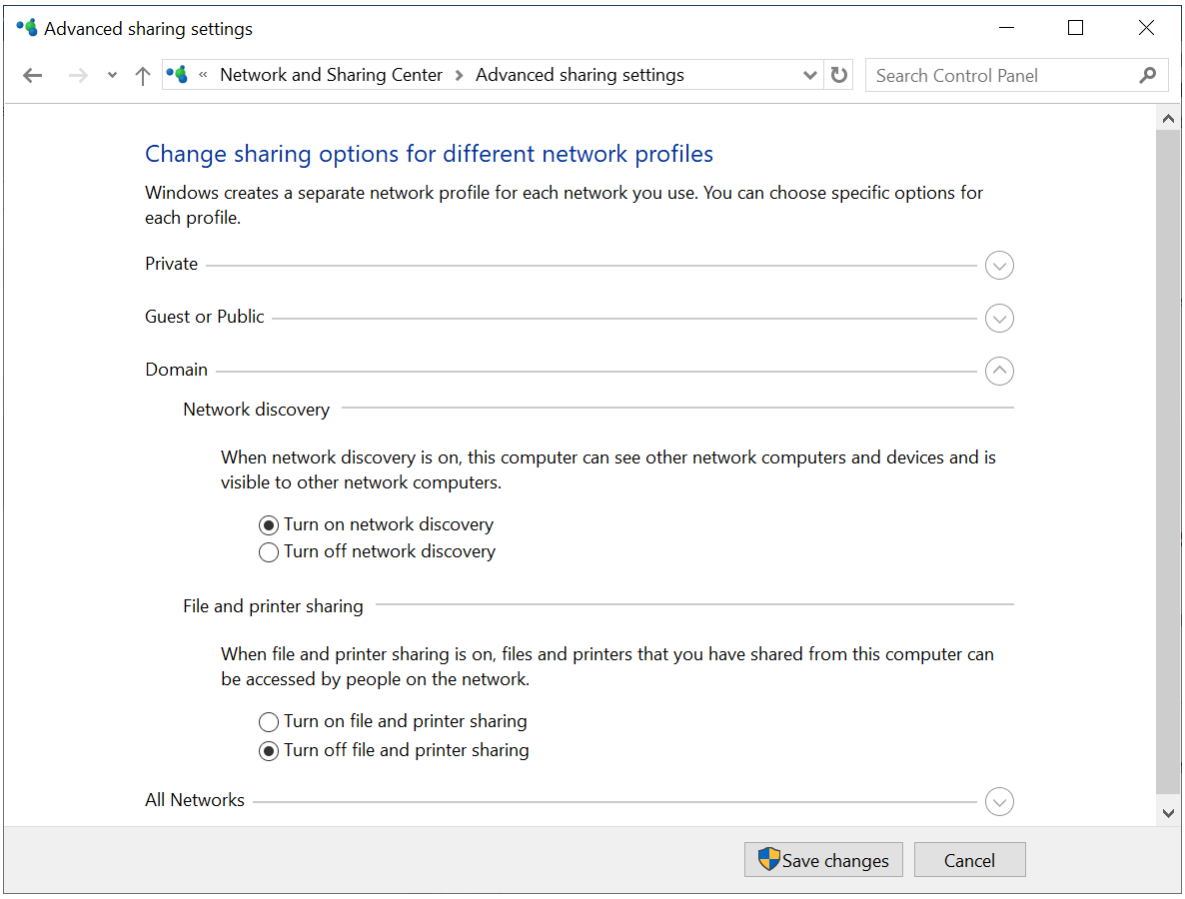
Si vous rencontrez le moindre problème avec la fonctionnalité de découverte automatique de terminaux, essayez de procéder aux vérifications suivantes :

- Vérifiez que l'option NetBIOS sur TCP/IP est activée ou configurée par défaut.



- Dans Panneau de configuration\Centre Réseau et partage\Paramètres de partage avancés, activez la découverte du réseau.

© Acronis International GmbH, 2003-2026



- Vérifiez que le service hôte du fournisseur de découverte de fonctions est en cours d'exécution sur la machine qui effectue la découverte, ainsi que sur les machines à découvrir.
- Vérifiez que le service Publication des ressources de découverte de fonctions est en cours d'exécution sur les machines à découvrir.

Empêcher la désinstallation ou la modification non autorisée d'agents

L'agent Cyber Protection pour Windows est protégé contre la désinstallation ou la modification non autorisée via l'option **Protection contre la désinstallation de l'agent** dans les plans de protection. Pour tous les plans de protection créés après novembre 2024, cette option est activée par défaut. Dans les plans de protection hérités, vous devez l'activer manuellement pour renforcer la sécurité de vos ressources.

Remarque
Cette option est disponible uniquement si le paramètre **Autoprotection** est activé.

Pour activer la protection de désinstallation de l'agent

1. Dans un plan de protection, développez le module **Protection contre les virus et les malwares** (module **Active Protection** pour les éditions Cyber Backup).

© Acronis International GmbH, 2003-2026

2. Assurez-vous que le commutateur **Autoprotection** est activé.
3. Cochez la case **Protection contre la désinstallation de l'agent**.
4. Dans le volet **Autoprotection**, cliquez sur **Terminé**.
5. Enregistrez le plan de protection.

La protection contre la désinstallation de l'agent sera activée pour les ordinateurs Windows auxquels ce plan de protection est appliqué. Toutes les modifications seront interdites, sauf si un administrateur les autorise. Voir "Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée" (p. 208).

Vous pouvez appliquer un plan de protection avec l'option **Protection contre la désinstallation de l'agent** activée à un ordinateur exécutant macOS ou Linux, mais aucune protection ne sera fournie.

Par ailleurs, vous ne pouvez appliquer à un ordinateur Windows qu'un seul plan de protection avec l'option Protection contre la désinstallation de l'agent activée. Pour en savoir plus sur la résolution d'un conflit potentiel, consultez la section Résolution des problèmes de compatibilité.

Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée

1. Après une tentative infructueuse de modification de l'agent de protection, accédez à l'onglet **Alertes**.
2. Recherchez l'alerte liée à la tentative de modification/désinstallation ayant échoué.
   Gravité de l'alerte : Avertissement
   Titre de l'alerte : Tentative de désinstallation/mise à jour de l'agent empêchée
3. Cliquez sur l'alerte, puis sélectionnez une mesure d'intervention dans le menu déroulant :
   - **Autoriser les modifications de l'agent pendant 1 heure** : permet d'autoriser les modifications de l'agent de protection au cours de l'heure suivante.
   - **Accéder aux paramètres de mise à jour de l'agent** : permet de configurer une fenêtre de maintenance plus longue.
     La durée peut être comprise entre 1 heure et 7 jours à partir du moment présent.
     Les modifications ou la désinstallation de l'agent ne seront autorisées que pendant cette période, sauf si vous activez les mises à jour automatiques pour l'agent de protection.
4. [Uniquement si vous avez choisi d'accéder aux paramètres de mise à jour de l'agent] Dans la boîte de dialogue de configuration de l'agent, sélectionnez la durée de la période de maintenance pour les mises à jour manuelles ou activez l'option **Mettre à jour automatiquement les agents**.
   - Si vous configurez une période de maintenance sans activer les mises à jour automatiques, seules les modifications manuelles seront autorisées pendant la période de maintenance que vous avez configurée.
   - Si vous activez les mises à jour automatiques sans configurer de fenêtre de maintenance, les mises à jour automatiques peuvent se produire à n'importe quel moment.

© Acronis International GmbH, 2003-2026

- Si vous configurez une fenêtre de maintenance et des mises à jour automatiques, les mises à jour automatiques et manuelles ne peuvent se produire que pendant cette fenêtre de maintenance.

5. Cliquez sur **Appliquer**.

Pour désactiver la protection contre la désinstallation de l'agent

Avertissement !
La désactivation de la **Protection contre la désinstallation de l'agent** expose les ressources protégées à des risques de sécurité.

1. Ouvrez le plan de protection pour le modifier et développez le module **Protection contre les virus et les malwares** (module **Active Protection** pour les éditions Cyber Backup).
2. Développez la section **Autoprotection**.
3. Désélectionnez la case **Protection contre la désinstallation de l'agent**.
4. Dans le volet **Autoprotection**, cliquez sur **Terminé**.
5. Enregistrez le plan de protection.

Modifier le quota du service pour les ressources

Un quota de service est automatiquement affecté lorsqu'un plan de protection est appliqué à une ressource pour la première fois.

Le quota le plus approprié est affecté en fonction du type de ressource protégée, de son système d'exploitation, du niveau de protection requis et de la disponibilité des quotas. Si le quota le plus approprié n'est pas disponible dans votre organisation, le second meilleur quota est affecté. Par exemple, si le quota le plus approprié est **Serveurs d'hébergement Web** mais qu'il n'est pas disponible, le quota **Serveurs** est affecté.

Exemples d'affectation de quota :

- Une machine physique exécutant Windows Server ou un système d'exploitation Linux se voit affecter le quota **Serveurs**.
- Une machine physique exécutant un système d'exploitation Windows pour bureau se voit affecter le quota **Postes de travail**.
- Une machine physique exécutant Windows 10 avec le rôle Hyper-V activé se voit affecter le quota **Postes de travail**.
- Un ordinateur de bureau fonctionnant sur une infrastructure de bureau virtuel et dont l'agent de protection est installé dans le système d'exploitation invité (par exemple, Agent pour Windows) se voit affecter le quota **Machines virtuelles**. Ce type d'ordinateur peut également utiliser le quota **Postes de travail** si le quota **Machines virtuelles** n'est pas disponible.
- Un ordinateur de bureau fonctionnant sur une infrastructure de bureau virtuel et sauvegardé en mode sans agent (par exemple, par Agent pour VMware ou Agent pour Hyper-V) se voit affecter le quota **Machines virtuelles**.

© Acronis International GmbH, 2003-2026

- Un serveur Hyper-V ou vSphere se voit affecter le quota **Serveurs**.
- Un serveur avec cPanel ou Plesk se voit affecter le quota **Serveurs d'hébergement Web**. Il peut également utiliser le quota **Machines virtuelles** ou le quota **Serveurs**, selon le type d'ordinateur sur lequel le serveur web fonctionne, si le quota **Serveurs d'hébergement Web** n'est pas disponible.
- La sauvegarde reconnaissant les applications nécessite le quota **Serveurs**, même pour un poste de travail.

Vous pouvez modifier manuellement l'attribution initiale ultérieurement. Par exemple, pour appliquer un plan de protection plus avancé à la même ressource, vous pourriez avoir besoin de mettre à niveau le quota de service de la ressource. Si les fonctionnalités requises par ce plan de protection ne sont pas prises en charge par le quota de service actuellement affecté, le plan de protection échouera.

Alternativement, vous pouvez changer le quota de service si vous achetez un quota plus approprié après l'attribution initiale. Par exemple, le quota **Postes de travail** est attribué à une machine virtuelle. Après l'achat d'un quota **Machines virtuelles**, vous pouvez affecter manuellement ce quota à la ressource, au lieu du quota **Postes de travail** initial.

Vous pouvez également libérer le quota de service actuellement attribué, puis l'affecter à une autre ressource.

Vous pouvez modifier le quota de service d'une ressource individuelle ou d'un groupe de ressources.

Pour modifier le quota de service d'une ressource individuelle

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez une ressource, puis cliquez sur **Détails**.
3. Dans la section **Quota de service**, cliquez sur **Modifier**.
4. Dans la fenêtre **Modifier le quota**, sélectionnez le quota de service ou **Aucun quota**, puis cliquez sur **Modifier**.

Pour modifier le quota de service d'un groupe de ressources

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez plusieurs ressources, puis cliquez sur **Attribuer un quota**.
3. Dans la fenêtre **Modifier le quota**, sélectionnez le quota de service ou **Aucun quota**, puis cliquez sur **Modifier**.

Paramètres de protection

Pour configurer les paramètres généraux de protection pour Cyber Protection, accédez depuis la console Cyber Protect à **Paramètres** > **Protection**.

© Acronis International GmbH, 2003-2026

Mises à jour automatiques pour les composants

Par défaut, tous les agents peuvent se connecter à Internet et télécharger les mises à jour.

Un administrateur peut réduire le trafic sur la bande passante réseau en sélectionnant un ou plusieurs agents dans l'environnement et en leur attribuant le rôle Responsable de la mise à jour. Les agents dédiés se connecteront donc à Internet et téléchargeront les mises à jour. Tous les autres agents se connecteront aux agents dédiés responsables de la mise à jour à l'aide d'une technologie de pair à pair, et téléchargeront les mises à jour auprès d'eux.

Les agents ne disposant pas du rôle Responsable de la mise à jour se connecteront à Internet s'il n'y a pas d'autre agent dédié responsable de la mise à jour dans l'environnement, ou si aucune connexion à un tel agent ne peut être établie au bout de cinq minutes.

L'agent responsable de la mise à jour distribue les mises à jour et les correctifs pour la protection antivirus et antimalware, l'évaluation des vulnérabilités et la gestion des correctifs, mais il n'inclut pas les mises à jour de la version de l'agent.

Remarque
Un agent avec le rôle Responsable de la mise à jour ne peut télécharger et distribuer des correctifs que pour les produits tiers Windows. Pour les produits Microsoft, la distribution des correctifs n'est pas prise en charge par l'agent Responsable de la mise à jour.

Avant d'attribuer le rôle Responsable de la mise à jour à un agent, vérifiez que l'ordinateur sur lequel l'agent est exécuté est assez puissant et dispose d'une connexion Internet haute vitesse et d'assez d'espace disque.

Pour préparer un ordinateur pour le rôle Responsable de la mise à jour

1. Sur l'ordinateur agent sur lequel vous prévoyez d'activer le rôle Responsable de la mise à jour, appliquez les règles de pare-feu suivantes :
   - Entrant «updater_incoming_tcp_ports» : autoriser la connexion aux ports TCP 18018 et 6888 pour tous les profils de pare-feu (public, privé et domaine).
   - Entrant «updater_incoming_udp_ports» : autoriser la connexion aux ports UDP 6888 pour tous les profils de pare-feu (public, privé et domaine).
2. Redémarrez Acronis Agent Core Service.
3. Redémarrez le service de pare-feu.

Si vous n'appliquez pas ces règles et que le pare-feu est activé, les autres agents téléchargeront les mises à jour depuis le Cloud.

Attribuer le rôle Responsable de la mise à jour à un agent de protection

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur comportant l'agent auquel vous souhaitez attribuer le rôle Responsable de la mise à jour.

© Acronis International GmbH, 2003-2026

3. Cliquez sur **Détails**, puis activez l'interrupteur **Utilisez cet agent pour télécharger et distribuer des correctifs et des mises à jour**.

La mise à jour de pair à pair fonctionne comme suit.

1. De façon planifiée, l'agent possédant le rôle Responsable de la mise à jour vérifie le fichier d'index mis à disposition par le fournisseur de services afin de mettre à jour les principaux composants.
2. L'agent possédant le rôle Responsable de la mise à jour commence à télécharger et à distribuer les mises à jour à tous les agents.

Vous pouvez attribuer le rôle Responsable de la mise à jour à plusieurs agents dans l'environnement. Ainsi, si un agent avec le rôle Responsable de la mise à jour est hors ligne, d'autres agents possédant ce rôle peuvent servir de source pour les mises à jour des définitions.

Collecte automatique de données de performances

Sur les ordinateurs protégés exécutant Microsoft Windows, les administrateurs d'entreprise peuvent activer ou désactiver la collecte automatique des journaux de performances. La collecte de données démarre si les performances du système chutent en dessous des seuils attendus pendant une période définie allant jusqu'à 3 600 secondes. La période définie est spécifiée sur la plate-forme et les seuils de performances sont configurés sur l'ordinateur sur lequel s'exécute l'agent de protection.

La collecte automatique des journaux de performances est désactivée par défaut.

Pour activer la collecte automatique de données de performances

Rôle requis : administrateur d'entreprise

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur sur lequel vous souhaitez activer la surveillance des performances.
3. Cliquez sur **Détails**, puis activez le commutateur **Autoriser cet agent à collecter automatiquement les journaux de performances**.

Le moniteur de performances fonctionne comme suit.

1. L'agent de protection surveille sur l'ordinateur plusieurs indicateurs de performances (comme l'utilisation de la mémoire et la charge du processeur).
2. Si les indicateurs passent sous un certain seuil pendant une certaine période, l'agent collecte une trace ETL.
3. Une alerte (info) indique que la collecte de données de performances a démarré.
   La collecte automatique dure 1 heure (3 600 secondes) et cette période ne peut pas être modifiée.
4. Une alerte (info) indique que la collecte de données de performances est terminée.
   Les données collectées automatiquement sont stockées sur le disque local de l'ordinateur protégé, dans le dossier `C:\ProgramData\Acronis\ETLTool\ETL\`

© Acronis International GmbH, 2003-2026

Mise à jour des définitions de Cyber Protection de façon planifiée

Dans l'onglet **Planification**, vous pouvez configurer le planning de mise à jour automatique des définitions de Cyber Protection pour chacun des composants suivants :

- Antimalware
- Évaluation des vulnérabilités
- Gestion des correctifs

Pour modifier le paramètre de mise à jour des définitions, naviguez vers **Paramètres** > **Protection** > **Mise à jour des définitions de protection** > **Planification**.

Type de planification :

- **Par jour** : définissez les jours de la semaine pour la mise à jour des définitions.
  Débuter à : sélectionnez l'heure à laquelle mettre à jour les définitions.
- **Par heure** : définissez un planning horaire plus granulaire pour les mises à jour.
  Exécution chaque : définissez la périodicité des mises à jour.
  À partir de... **Jusqu'à** : définissez une plage de temps spécifique pour les mises à jour.

Mise à jour des définitions de Cyber Protection à la demande

Pour mettre à jour les définitions de Cyber Protection à la demande, pour un ordinateur en particulier

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez les machines sur lesquelles vous souhaitez mettre à jour les définitions de protection, puis cliquez sur **Mettre les définitions à jour**.

Mémoire en cache

L'emplacement des données en cache est le suivant :

- Sur les machines Windows : `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Sur les machines Linux : `/opt/acronis/var/atp-downloader/Cache`
- Sur les ordinateurs macOS : `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Pour modifier le paramètre de stockage du cache, accédez à **Paramètres** > **Protection** > **Mise à jour des définitions de protection** > **Stockage du cache**.

Dans **Fichiers de mise à jour et données de gestion des correctifs obsolètes**, indiquez au bout de combien de temps supprimer les données en cache.

Taille maximum de la mémoire en cache (Go) pour les agents :

© Acronis International GmbH, 2003-2026

- **Rôle Responsable de la mise à jour :** définissez la taille du stockage pour le cache sur les machines ayant le rôle Responsable de la mise à jour.
- **Autres rôles :** définissez la taille du stockage pour le cache sur les autres machines.

Remarque
Cyber Protection collecte des échantillons de malware détectés en vue d'une analyse supplémentaire qui nous permettra d'améliorer notre logiciel. Vous pouvez modifier ce paramètre à tout moment dans l'onglet **Protection**, en désactivant l'option **Collecter et transférer des échantillons de malware vers le CPOC**.

Services Cyber Protection installés dans votre environnement

Cyber Protection installe certains des services suivants, en fonction des options Cyber Protection que vous utilisez.

Services installés sous Windows

Nom du service	Objectif
Acronis Managed Machine Service	Fonctionnalités de sauvegarde, restauration, réplication, rétention, validation
Acronis Scheduler2 Service	Exécute les tâches planifiées pour certains événements
Acronis Active Protection Service	Offre une protection contre les ransomware
Acronis Cyber Protection Service	Offre une protection antimalware

Services installés sous macOS

Nom du service et emplacement	Objectif
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Sert à la communication entre l'agent et les composants de gestion
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Permet de détecter les malwares
`/Library/LaunchDaemons/com.acronis.mms.plist`	Offre une fonctionnalité de sauvegarde et de restauration
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Exécute les tâches planifiées

© Acronis International GmbH, 2003-2026

Collecte des informations système

Vous pouvez enregistrer un journal d'agent dans un fichier .zip. Si une sauvegarde échoue pour une raison inconnue, ce fichier aidera le personnel du support technique à identifier le problème.

Par défaut, les informations contenues dans le journal sont optimisées pour les trois derniers jours, mais vous pouvez modifier cette période.

Collecter depuis la console Cyber Protect

Pour collecter les journaux des agents

1. Effectuez l'une des actions suivantes :
   - Dans **Terminaux**, sélectionnez la ressource dont vous souhaitez collecter les journaux, puis cliquez sur **Activités**.
   - Dans **Paramètres** > **Agents**, sélectionnez la ressource dont vous souhaitez collecter les journaux, puis cliquez sur **Détails**.
2. [Facultatif] Pour modifier la période par défaut pour laquelle les informations système sont incluses, cliquez sur la flèche située à côté du bouton **Collecter les informations système**, puis sélectionnez la période.
3. Cliquez sur **Collecter les informations système**.
4. Si vous y êtes invité par votre navigateur Web, indiquez où enregistrer le fichier.

Collecter localement

Cette procédure est applicable aux ressources hors ligne ainsi qu'aux supports de démarrage.

Pour collecter les journaux des agents

- Suivez les étapes de cet article de la base de connaissances.

Gestion des licences pour les serveurs de gestion sur site

Pour obtenir des informations détaillées sur l'activation d'un serveur de gestion sur site ou sur l'allocation de licences, reportez-vous à la section Gestion des licences du Guide de l'utilisateur Cyber Protect.

© Acronis International GmbH, 2003-2026

Utilisation de plans

Présentation des plans

Remarque
La disponibilité de certaines fonctionnalités dépend des éléments de l'offre activés pour votre compte, ainsi que du niveau d'administration dans la console Cyber Protect.

Un plan est un ensemble de configurations et de règles que vous pouvez appliquer à une ou plusieurs ressources pour atteindre différents objectifs tels que la sauvegarde d'une ressource, la protection d'une ressource contre les malware, la surveillance des performances de la ressource, etc.

Un plan se compose de modules que vous pouvez activer ou désactiver. Chaque module contient des paramètres liés à une fonctionnalité spécifique.

Tous les plans que vous avez créés sont visibles dans l'onglet **Gestion**.

Plan	Description	Disponible au niveau de l'administrateur		
		Partenaire (Tous les clients)	**Client**	**Unité**
Plan de protection	Protège les données de la ressource. Au niveau du partenaire, un plan de protection comprend les modules suivants : • Protection contre les virus et les malwares Des limitations s'appliquent. Pour plus d'informations, voir "Utilisation de caractères génériques pour définir des exclusions" (p. 395). • Évaluation des vulnérabilités Pour plus d'informations, voir "Évaluation des vulnérabilités et gestion des correctifs au niveau partenaire" (p. 1421). • Gestion des correctifs Pour plus d'informations, voir "Évaluation des vulnérabilités et gestion des correctifs au niveau partenaire" (p. 1421). Au niveau du client et de l'unité, un plan de protection comprend les modules suivants :	Oui, avec des limitations	Oui	Oui

© Acronis International GmbH, 2003-2026

Plan	Description	Disponible au niveau de l'administrateur		
		Partenaire (Tous les clients)	Client	Unité
	• Sauvegarde • "Implémentation de la reprise d'activité après sinistre" (p. 1016) • EDR (Endpoint Detection and Response) • Protection contre les virus et les malwares • Filtrage d'URL • Antivirus Windows Defender • Microsoft Security Essentials • Évaluation des vulnérabilités • Gestion des correctifs • Carte de la protection des données • Contrôle des terminaux • Prévention de la perte de données Pour plus d'informations sur les plans de protection, voir "Plans et modules de protection" (p. 243).			
Plan de gestion à distance	Active la fonctionnalité d'assistance et de bureau à distance sur vos ressources gérées. Pour plus d'informations, voir "Plans de gestion à distance" (p. 1467).	Oui	Oui	Oui
Plan de création de script	Permet l'exécution de scripts sur plusieurs ressources, l'exécution programmée de scripts et la configuration de paramètres de scripts supplémentaires. Pour plus d'informations, voir "Plans de création de scripts" (p. 503).	Oui	Oui	Oui
Plan de surveillance	Surveille les performances, le matériel, les logiciels, le système et les paramètres de sécurité de vos ressources gérées. Pour plus d'informations, voir "Plans de surveillance" (p. 1561).	Oui	Oui	Oui
Plan de déploiement logiciel	Automatise le processus de déploiement des logiciels et garantit que la distribution des logiciels sur vos ressources gérées est cohérente.	Oui	Oui	Oui

© Acronis International GmbH, 2003-2026

Plan	Description	Disponible au niveau de l'administrateur		
		Partenaire (Tous les clients)	Client	Unité
Sauvegarde d'applications dans le Cloud	Sauvegarde des applications exécutées dans le cloud au moyen d'agents qui s'exécutent dans le cloud et utilise le stockage dans le cloud comme emplacement de sauvegarde. Pour plus d'informations, voir "Plans de sauvegarde pour les applications dans le Cloud" (p. 273)	Non	Oui	Oui
Plan d'archivage	Avec l'archivage des e-mails, tous les e-mails d'une organisation Microsoft 365 sont conservés dans une archive externe qui est stockée dans le cloud. De nouveaux e-mails sont ajoutés à l'archive en continu, au fur et à mesure de leur envoi ou de leur réception. Pour plus d'informations, voir "Archivage d'e-mails" (p. 771).	Oui	Oui	Non
Plan d'analyse de la sauvegarde	Recherche des malwares (y compris les ransomware) dans les sauvegardes. Pour plus d'informations, voir "Plan d'analyse des sauvegardes" (p. 272).	Non	Oui	Oui
Plan de transfert SIEM	Configure comment les alertes Acronis, les événements, les tâches et les informations du journal d'audit sont transférés pour être consommés par des plate-formes de gestion des incidents et des événements de sécurité (SIEM) de tiers. Pour plus d'informations, voir plans de transfert SIEM.	Oui	Non	Non
Réplication de sauvegarde	Réplique une sauvegarde vers un autre emplacement. Pour plus d'informations, voir "Réplication de sauvegarde" (p. 255).	Non	Oui	Oui
Validation	Valide une sauvegarde et vérifie que les données de la sauvegarde peuvent être restaurées. Pour plus d'informations, voir "Validation" (p. 259).	Non	Oui	Oui
Nettoyage	Supprime les sauvegardes obsolètes conformément aux règles de rétention. Ce	Non	Oui	Oui

© Acronis International GmbH, 2003-2026

Plan	Description	Disponible au niveau de l'administrateur		
		Partenaire (Tous les clients)	Client	Unité
	plan s'applique uniquement aux agents et aux ressources, et non aux sauvegardes de cloud à cloud. Pour plus d'informations, voir "Nettoyage" (p. 266).			
Conversion en MV	Ce plan ne s'applique qu'aux sauvegardes de niveau disque. Vérifie si une sauvegarde inclut le volume système et contient toutes les informations nécessaires au démarrage du système d'exploitation afin que la machine virtuelle résultante puisse démarrer seule. Pour plus d'informations, voir "Conversion en une machine virtuelle" (p. 267).	Non	Oui	Oui
Réplication de MV	Recherche des malwares (y compris les ransomware) dans les sauvegardes. Pour plus d'informations, voir "Réplication de machines virtuelles" (p. 961).	Non	Oui	Oui

Plans intégrés

Les plans intégrés sont préconfigurés avec certains des paramètres les plus utilisés ou recommandés. Les plans intégrés peuvent être sélectionnés immédiatement, sans aucune configuration. Vous ne pouvez pas modifier les plans intégrés, mais vous pouvez modifier les paramètres d'un plan intégré appliqué à une ressource.

Des plans intégrés sont disponibles pour les types de plans suivants : plans de protection, plans de surveillance et plans de gestion à distance.

Plans de protection intégrés

Le tableau suivant fournit plus d'informations sur les plans de protection intégrés.

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
Sauvegarde	Activée	Activée	Activée	Activée
Quoi sauvegarder Éléments à sauvegarder	Toute la machine	Toute la machine	Toute la machine	Toute la machine
Protection continue des données (CDP)	Désactivé	Désactivé	Activé	Activé
Où sauvegarder	Stockage dans le Cloud	Stockage dans le Cloud	Stockage dans le Cloud	Stockage dans le Cloud
Planification	Du lundi au vendredi, à midi En plus, options activées et conditions de démarrage : • Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine	Du lundi au vendredi, à 00 h En plus, options activées et conditions de démarrage : • Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine	Du lundi au vendredi, à 00 h En plus, options activées et conditions de démarrage : • Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine	Du lundi au vendredi, à 00 h En plus, options activées et conditions de démarrage : • Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
	• Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée • Économiser de la batterie : Ne pas démarrer lors d'une alimentation sur batterie • Ne pas démarrer pendant une connexion mesurée	• Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée • Économiser de la batterie : Ne pas démarrer lors d'une alimentation sur batterie • Ne pas démarrer pendant une connexion mesurée	• Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée • Économiser de la batterie : Ne pas démarrer lors d'une alimentation sur batterie • Ne pas démarrer pendant une connexion mesurée	• Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée • Économiser de la batterie : Ne pas démarrer lors d'une alimentation sur batterie • Ne pas démarrer pendant une connexion mesurée
Modèle de sauvegarde	Toujours incrémentielle	Toujours incrémentielle	Toujours incrémentielle	Toujours incrémentielle

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
Durée de conservation	Conserver toutes les sauvegardes pendant 90 jours	Conserver toutes les sauvegardes pendant 90 jours	Conserver toutes les sauvegardes pendant 90 jours	Conserver toutes les sauvegardes pendant 90 jours
Options de sauvegarde	Options par défaut	Options par défaut, plus : • Performance et créneau de sauvegarde (l'ensemble vert) : Priorité de CPU : Faible Vitesse de sortie : 50 %	Options par défaut, plus : • Performance et créneau de sauvegarde (l'ensemble vert) : Priorité de CPU : Faible Vitesse de sortie : 50 %	Options par défaut, plus : • Performance et créneau de sauvegarde (l'ensemble vert) : Priorité de CPU : Faible Vitesse de sortie : 50 %
EDR	Désactivée	Désactivée	Activée	
Protection contre les virus et les malwares	Activée	Activée	Activée	
Active Protection	Activée	Activée	Activée	
Protection Antimalware Advanced	Activée	Activée	Activée	

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
Protection du dossier réseau	Activée	Activée	Activée	
Protection côté serveur	Désactivée	Désactivée	Désactivée	
Autoprotection	Activée	Activée	Activée	
Détection d'un processus de cryptominage	Activée	Activée	Activée	
Quarantaine	Supprimer les fichiers mis en quarantaine après 30 jours	Supprimer les fichiers mis en quarantaine après 30 jours	Supprimer les fichiers mis en quarantaine après 30 jours	
Moteur de comportement	Quarantaine	Quarantaine	Quarantaine	
Prévention des failles	Notifier et stopper le processus	Notifier et stopper le processus	Notifier et stopper le processus	
Protection en temps réel	Quarantaine	Quarantaine	Quarantaine	
Planifier l'analyse	Analyse rapide : Quarantaine	Analyse rapide : Quarantaine	Analyse rapide : Quarantaine	

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
	À 20 heures, du dimanche au samedi Analyse complète : Quarantaine À 21 heures, le mercredi et le vendredi En plus, options activées et conditions de démarrage : Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée	À 20 heures, du dimanche au samedi Analyse complète : Quarantaine À 21 heures, le mercredi et le vendredi En plus, options activées et conditions de démarrage : Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée	À 20 heures, du dimanche au samedi Analyse complète : Quarantaine À 21 heures, le mercredi et le vendredi En plus, options activées et conditions de démarrage : Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée	
Exclusions	Aucun	Aucun	Aucun	

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
Filtrage d'URL	Désactivée	Activée	Activée	
Accès à un site Web malveillant	Bloquer	Bloquer	Bloquer	
Catégories à filtrer	Options par défaut	Options par défaut	Options par défaut	
Exclusions	Aucun	Aucun	Aucun	
Antivirus Microsoft Defender	Désactivée	Désactivée	Désactivée	
Gestion du pare-feu	Désactivée	Activée	Activée	
Microsoft Security Essentials	Désactivée	Désactivée	Désactivée	
Évaluation des vulnérabilités	Activée	Activée	Activée	
Portée d'évaluation des vulnérabilités	Produits Microsoft, produits tiers Windows, produits Apple,	Produits Microsoft, produits tiers Windows, produits Apple,	Produits Microsoft, produits tiers Windows, produits Apple,	

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
	produits tiers macOS, package d'analyse Linux	produits tiers macOS, package d'analyse Linux	produits tiers macOS, package d'analyse Linux	
Planification	A 11 h 00, uniquement le mercredi et le vendredi	A 11 h 00, uniquement le mercredi et le vendredi	A 11 h 00, uniquement le mercredi et le vendredi	
Gestion des correctifs	Activée	Activée	Activée	
Produits Microsoft	Toutes les mises à jour	Toutes les mises à jour	Toutes les mises à jour	
Produits Windows tiers	Toutes les mises à jour	Toutes les mises à jour	Toutes les mises à jour	
Planification	À 12 h 30, uniquement le mercredi et le vendredi	À 12 h 30, uniquement le mercredi et le vendredi	À 12 h 30, uniquement le mercredi et le vendredi	
Sauvegarde pré-mise à jour	Activée	Activée	Activée	

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
Carte de la protection des données	Désactivée	Désactivée	Activée	
Extensions et règles d'exception	–	–	Options par défaut (66 extensions à détecter)	
Planification	–	–	À 15 h 40, du lundi au vendredi	
Contrôle des terminaux	Désactivée	Désactivée	Désactivée	
Paramètres d'accès	Autorisé : Tout	Autorisé : Tout	Autorisé : Tout	
Liste d'autorisation des types de terminaux	1 HID USD autorisé (souris, clavier, etc.)	1 HID USD autorisé (souris, clavier, etc.)	1 HID USD autorisé (souris, clavier, etc.)	
Liste d'autorisation des périphériques USB	Vide	Vide	Vide	
Exclusion	Aucun	Aucun	Aucun	

© Acronis International GmbH, 2003-2026

Modules et paramètres	Plans de protection intégrés			
	Protection essentielle	**Protection étendue**	**Protection exhaustive**	**Sauvegarde de l'intégralité de la ressource**
	Temps d'arrêt et perte de données réduits au minimum, restauration sans effort avec objectif de point de restauration (RPO) court et maintenance aisée	**Deuxième niveau de protection : continuité des activités, atténuation proactive des risques de sécurité et conformité**	**Troisième niveau de protection : continuité des activités, objectif de point de restauration (RTO) proche de zéro, atténuation proactive des risques de sécurité, prévention des fuites de données et conformité**	**Sauvegarde l'intégralité de la ressource dans le cloud**
Prévention de la perte de données	Désactivée	Désactivée	Désactivée	
Mode	–	–	–	
Paramètres avancés	–	–	–	
Disaster Recovery	Désactivée	Désactivée	Désactivée	

Pour plus d'informations sur les plans de protection, voir "Plans et modules de protection" (p. 243).

Plans de surveillance intégrés

Le tableau suivant fournit de plus amples informations sur les plans de surveillance intégrés.

Nom	Description	Moniteurs activés
Surveillance recommandée pour Windows	Surveille l'intégrité et les performances des ordinateurs Windows	Les 13 moniteurs suivants sont activés dans ce plan : • État du logiciel antimalware • État de la fonctionnalité d'exécution automatique • Température du processeur • Utilisation du processeur • Espace disque

© Acronis International GmbH, 2003-2026

Nom	Description	Moniteurs activés
		• Vitesse de transfert du disque • Échecs de connexion • État du pare-feu • Température du processeur graphique • Dernier redémarrage du système • Utilisation de la mémoire • Utilisation du réseau • État de Windows Update
Surveillance recommandée pour macOS	Surveille l'intégrité et les performances des ordinateurs macOS	Les 10 moniteurs suivants sont activés dans ce plan : • État du logiciel antimalware • Température du processeur • Utilisation du processeur • Espace disque • Vitesse de transfert du disque • État du pare-feu • Température du processeur graphique • Dernier redémarrage du système • Utilisation de la mémoire • Utilisation du réseau
Surveillance recommandée pour les serveurs	Surveille l'intégrité et les performances des serveurs Windows	Les 20 moniteurs suivants sont activés dans ce plan : • État du logiciel antimalware • Température du processeur, 2 moniteurs : 80 degrés, 10 min, avertissement 90 degrés, 10 min, critique • Utilisation du processeur, 3 moniteurs : Moins de 20 %, 10 min, informations Plus de 80 %, 10 min, avertissement Plus de 90 %, 10 min, critique

© Acronis International GmbH, 2003-2026

Nom	Description	Moniteurs activés
		• Espace disque, 2 moniteurs : Moins de 20 %, 30 min, avertissement Moins de 10 %, 30 min, critique • Vitesse de transfert du disque • Échec des connexions, 3 moniteurs : 5 tentatives, 1 heure, informations 10 tentatives, 1 heure, avertissement 20 tentatives, 1 heure, critique • État du pare-feu • Modifications apportées au matériel • Logiciel installé • Utilisation de la mémoire, 3 moniteurs : Moins de 20 %, 10 min, informations Plus de 80 %, 10 min, avertissement Plus de 90 %, 10 min, critique • Utilisation du réseau • État de Windows Update

Pour plus d'informations sur les plans de surveillance, voir "Plans de surveillance" (p. 1561).

Plans de gestion à distance intégrés

Le tableau suivant fournit plus d'informations sur le plan de gestion à distance intégré.

Nom	Description	Paramètres
Bureau à distance essentiel	Active les fonctionnalités de bureau à distance et de transfert de fichiers	Protocoles de connexion **Autoriser les connexions via NEAR** : option activée Paramètres de sécurité NEAR • **Verrouiller la ressource lorsque l'utilisateur se déconnecte d'une session de console** : option désactivée

© Acronis International GmbH, 2003-2026

Nom	Description	Paramètres
		• **Autoriser un seul utilisateur à la fois à se connecter avec NEAR ou à effectuer un transfert de fichiers** : option désactivée • **Autoriser l'administrateur de la ressource à se connecter à une session** : option activée • **Autoriser la création d'une session système** : option désactivée • **Autoriser la synchronisation du Presse-papiers** : option activée **Autoriser les connexions via RDP** : option activée **Autoriser les connexions via le partage d'écran Apple** : option désactivée Paramètres de sécurité • **Indiquer si la ressource est contrôlée à distance** : option activée • **Demander l'autorisation de l'utilisateur à effectuer des captures d'écran de la ressource** : option activée Gestion des ressources • **Transfert de fichiers** : option activée • **Transmission de captures d'écran** : option désactivée Paramètres d'affichage • **Utiliser la déduplication de bureau pour effectuer la capture d'un bureau** : option activée • **Utiliser l'accélération OpenCL** : option activée • **Utiliser le codage matériel H.264** : option activée Boîte à outils **Afficher les derniers utilisateurs connectés** : option désactivée

Pour plus d'informations sur les plans de gestion à distance, voir "Plans de gestion à distance" (p. 1467).

Plans par défaut

Le plan par défaut est un plan présélectionné qui s'affiche en premier dans les listes de plans et dans les champs de sélection de plan. Vous ne pouvez avoir qu'un seul plan par défaut, par tenant et par type de plan pris en charge à la fois.

© Acronis International GmbH, 2003-2026

La liste des plans et le plan par défaut que vous verrez dépendent du niveau auquel vous utilisez la console Protection.

Par exemple, si vous utilisez la console au niveau du partenaire, vous verrez les plans créés aux niveaux partenaire, client et unité ; les plans par défaut seront les plans définis comme tels au niveau du partenaire. Si vous utilisez la console au niveau du client, vous ne verrez aucun plan créé au niveau partenaire, pas même les plans par défaut au niveau partenaire. De la même manière, si vous utilisez la console au niveau de l'unité, vous ne verrez aucun plan créé aux niveaux partenaire ou client, pas même les plans par défaut à ces niveaux.

Les plans par défaut sont pris en charge pour les types de plans suivants : plans de protection, plans de surveillance et plans de gestion à distance.

Définition des plans par défaut

Vous pouvez définir comme plan par défaut l'un des plans parmi les types pris en charge (plan de protection, de surveillance ou de gestion à distance).

Remarque
La fonctionnalité n'est pas disponible pour les utilisateurs auxquels le rôle **Administrateur en lecture seule** a été attribué pour le service de protection.

Plans de protection

Prérequis

Au moins un plan de protection est créé pour votre tenant. Pour plus d'informations, voir "Création d'un plan de protection" (p. 244).

Pour définir un plan de protection par défaut

1. Dans l'écran **Plans de protection**, sélectionnez le plan que vous souhaitez définir par défaut, puis cliquez sur **Détails**.
2. Cliquez sur l'icône représentant des points de suspension, puis cliquez sur **Définir par défaut**.
3. Dans la fenêtre de confirmation, cliquez sur **Définir**.
   Dans l'écran **Plans de protection**, la balise **Défaut** apparaît à côté du nom du plan.

Plans de gestion à distance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Au moins un plan de gestion à distance est créé pour votre tenant. Pour plus d'informations, voir "Création d'un plan de gestion à distance" (p. 1467).

Pour définir un plan de gestion à distance par défaut

1. Dans l'écran **Plans de gestion à distance**, recherchez le plan que vous souhaitez définir par défaut.

© Acronis International GmbH, 2003-2026

2. Dans la même ligne, cliquez sur l'icône **Autres actions**.
3. Cliquez sur **Définir par défaut**.
4. Dans la fenêtre de confirmation, cliquez sur **Définir**.
   Dans l'écran **Plans de gestion à distance**, la balise **Par défaut** apparaît à côté du nom du plan.

Plans de surveillance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Au moins un plan de surveillance est créé pour votre tenant. Pour plus d'informations, voir "Création d'un plan de surveillance" (p. 1561).

Pour définir un plan de surveillance par défaut

1. Dans l'écran **Plans de surveillance**, recherchez le plan que vous souhaitez définir par défaut.
2. Dans la même ligne, cliquez sur l'icône **Autres actions**.
3. Cliquez sur **Définir par défaut**.
4. Dans la fenêtre de confirmation, cliquez sur **Définir**.
   Dans l'écran **Plans de surveillance**, la balise **Défaut** apparaît à côté du nom du plan.

Suppression des plans par défaut

Vous pouvez supprimer le plan de protection par défaut. Il ne sera plus présélectionné dans les champs de sélection de plan.

Remarque
La fonctionnalité n'est pas disponible pour les utilisateurs auxquels le rôle **Administrateur en lecture seule** a été attribué pour le service de protection.

Plans de protection

Prérequis

Un plan de protection est créé pour votre tenant et défini par défaut. Pour plus d'informations, voir "Création d'un plan de protection" (p. 244).

Pour supprimer un plan de protection par défaut

1. Dans l'écran **Plans de protection**, sélectionnez le plan par défaut, puis cliquez sur **Détails**.
2. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Effacer la valeur par défaut**.
3. Dans la fenêtre de confirmation, cliquez sur **Effacer**.
   Sur l'écran **Plans de protection**, la balise **Par défaut** située à côté du nom du plan disparaît.

Plans de gestion à distance

Prérequis

© Acronis International GmbH, 2003-2026

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Un plan de gestion à distance est créé pour votre tenant et défini par défaut. Pour plus d'informations, voir "Création d'un plan de gestion à distance" (p. 1467).

Pour supprimer un plan de protection par défaut

1. Sur l'écran **Plans de gestion à distance**, repérez le plan par défaut que vous souhaitez effacer.
2. Dans la même ligne, cliquez sur l'icône représentant des points de suspension (...).
3. Cliquez sur **Effacer la valeur par défaut**.
4. Dans la fenêtre de confirmation, cliquez sur **Effacer**.
   Sur l'écran **Plans de gestion à distance**, la balise **Défaut** qui se trouvait à côté du nom du plan disparaît.

Plans de surveillance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Un plan de surveillance est créé pour votre tenant et défini par défaut. Pour plus d'informations, voir "Création d'un plan de surveillance" (p. 1561).

Pour supprimer un plan de protection par défaut

1. Sur l'écran **Plans de surveillance**, repérez le plan par défaut que vous souhaitez effacer.
2. Dans la même ligne, cliquez sur l'icône représentant des points de suspension (...).
3. Cliquez sur **Effacer la valeur par défaut**.
4. Dans la fenêtre de confirmation, cliquez sur **Effacer**.
   Sur l'écran **Plans de surveillance**, la balise **Défaut** qui se trouvait à côté du nom du plan disparaît.

Plans favoris

Les plans favoris apparaissent en haut de la liste des plans, après les plans par défaut. Vous pouvez ajouter un plan à vos favoris si vous souhaitez qu'il est visible et facile à trouver, même lorsque votre organisation dispose de nombreux plans.

La liste des plans et les plans favoris que vous verrez dépendent du niveau auquel vous utilisez la console Protection.

Par exemple, si vous utilisez la console au niveau du partenaire, vous verrez les plans créés à tous les niveaux (partenaire, client et unité), mais les plans favoris seront les plans ajoutés aux favoris au niveau partenaire. Si vous utilisez la console au niveau client, vous ne verrez pas les plans créés au niveau partenaire, pas même les plans favoris au niveau partenaire. De la même manière, si vous utilisez la console au niveau unité, vous ne verrez pas les plans créés aux niveaux partenaire ou client, pas même les plans favoris à ces niveaux.

© Acronis International GmbH, 2003-2026

Les plans favoris sont pris en charge pour les types de plans suivants : plans de protection, plans de surveillance et plans de gestion à distance.

Définition de plans en tant que favori

Vous pouvez définir jusqu'à 10 plans favoris par type de plan pris en charge (plan de protection, de surveillance ou de gestion à distance) par tenant.

Remarque
La fonctionnalité n'est pas disponible pour les utilisateurs auxquels le rôle **Administrateur en lecture seule** a été attribué pour le service de protection.

Plans de protection

Prérequis

Au moins un plan de protection est créé pour votre tenant. Pour plus d'informations, voir "Création d'un plan de protection" (p. 244).

Pour définir un plan de protection comme favori

1. Dans l'écran **Plans de protection**, recherchez le plan que vous souhaitez définir par défaut, puis cliquez sur **Détails**.
2. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Ajouter aux favoris**.
   Dans l'écran **Plans de protection**, une icône en forme d'étoile apparaît à côté du nom du plan.

Plans de gestion à distance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Au moins un plan de gestion à distance est créé pour votre tenant. Pour plus d'informations, voir "Création d'un plan de surveillance" (p. 1561).

Pour définir un plan de gestion à distance comme favori

1. Dans l'écran **Plans de gestion à distance**, localisez le plan que vous souhaitez ajouter en tant que favori.
2. Dans la ligne du plan, cliquez sur l'icône représentant des points de suspension (...).
3. Cliquez sur **Ajouter aux favoris**.
   Dans l'écran **Plans de gestion à distance**, une icône en forme d'étoile apparaît à côté du nom du plan.

Plans de surveillance

Prérequis

© Acronis International GmbH, 2003-2026

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Au moins un plan de gestion est créé pour votre tenant. Pour plus d'informations, voir "Création d'un plan de surveillance" (p. 1561).

Pour définir un plan de surveillance comme favori

1. Dans l'écran **Plans de surveillance**, localisez le plan que vous souhaitez définir comme favori.
2. Dans la ligne du plan, cliquez sur l'icône représentant des points de suspension (...).
3. Cliquez sur **Ajouter aux favoris**.
   Dans l'écran **Plans de surveillance**, une icône en forme d'étoile apparaît à côté du nom du plan.

Suppression de plans des favoris

Vous pouvez supprimer les plans de protection, les plans de surveillance et les plans de gestion à distance favoris de la liste des favoris.

Remarque
La fonctionnalité n'est pas disponible pour les utilisateurs auxquels le rôle **Administrateur en lecture seule** a été attribué pour le service de protection.

Plans de protection

Prérequis

Au moins un plan de protection est défini comme favori pour votre tenant.

Pour supprimer un plan de protection des favoris

1. Dans l'écran **Plans de protection**, cliquez sur le plan que vous souhaitez supprimer des favoris, puis cliquez sur **Détails**.
2. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Retirer des favoris**.
   Dans l'écran **Plans de protection**, une icône en forme d'étoile apparaît à côté du nom du plan.

Plans de gestion à distance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Au moins un plan de gestion à distance est défini comme favori pour votre tenant.

Pour supprimer un plan de gestion à distance des favoris

1. Dans l'écran **Plans de gestion à distance**, localisez le plan que vous souhaitez supprimer des favoris.
2. Dans la ligne du plan, cliquez sur l'icône représentant des points de suspension (...).
3. Cliquez sur **Supprimer des favoris**.

© Acronis International GmbH, 2003-2026

Sur l'écran **Plans de gestion à distance**, l'icône en forme d'étoile à côté du nom du plan disparaît.

Plans de surveillance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Au moins un plan de surveillance est défini comme favori pour votre tenant.

Pour supprimer un plan de surveillance des favoris

1. Dans l'écran **Plans de surveillance**, localisez le plan que vous souhaitez supprimer des favoris.
2. Dans la ligne du plan, cliquez sur l'icône représentant des points de suspension (...).
3. Cliquez sur **Supprimer des favoris**.
   Sur l'écran **Plans de surveillance**, l'icône en forme d'étoile à côté du nom du plan disparaît.

Définition de l'ordre des plans favoris

Vous pouvez définir l'ordre dans lequel les plans de protection favoris s'affichent dans les champs de sélection de plan.

Vous pouvez définir jusqu'à 10 plans favoris par type de plan pris en charge (plan de protection, de surveillance ou de gestion à distance) par tenant.

Remarque
La fonctionnalité n'est pas disponible pour les utilisateurs auxquels le rôle **Administrateur en lecture seule** a été attribué pour le service de protection.

Plans de protection

Prérequis

Deux plans au moins sont définis comme favoris.

Pour définir l'ordre des plans favoris

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Gérer les favoris**.
3. Glissez-déposez les plans pour définir l'ordre dans lequel ils apparaîtront dans les champs de sélection de plan.

   Remarque
   Pour pouvoir faire glisser un plan, cliquez sur la zone figurant avant le nom du plan.

4. Cliquez sur **Enregistrer**.

Plans de gestion à distance

Prérequis

© Acronis International GmbH, 2003-2026

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Deux plans au moins sont définis comme favoris.

Pour définir l'ordre des plans favoris

1. Dans l'écran des plans de la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Cliquez sur **Gérer les favoris**.
3. Glissez-déposez les plans pour définir l'ordre dans lequel ils apparaîtront dans les champs de sélection de plan.

   Remarque
   Pour pouvoir faire glisser un plan, cliquez sur la zone figurant avant le nom du plan.

4. Cliquez sur **Enregistrer**.

Plans de surveillance

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Deux plans au moins sont définis comme favoris.

Pour définir l'ordre des plans favoris

1. Dans l'écran des plans de la console Cyber Protect, accédez à **Gestion** > **Plans de surveillance**.
2. Cliquez sur **Gérer les favoris**.
3. Glissez-déposez les plans pour définir l'ordre dans lequel ils apparaîtront dans les champs de sélection de plan.

   Remarque
   Pour pouvoir faire glisser un plan, cliquez sur la zone figurant avant le nom du plan.

4. Cliquez sur **Enregistrer**.

Plans préselectionnés

Si l'authentification à deux facteurs (2FA) est activée pour votre compte, un plan de protection, un plan de surveillance et un plan de gestion à distance sont préselectionnés lorsque vous enregistrez une ressource dans la console Cyber Protect.

Vous pouvez modifier la sélection ou choisir de ne pas appliquer de plan à la ressource. Pour plus d'informations, voir "Enregistrement des ressources à l'aide de l'interface utilisateur graphique" (p. 110).

Les plans préselectionnés dépendent des éléments suivants :

© Acronis International GmbH, 2003-2026

- Rôle de l'utilisateur qui enregistre la ressource.
- Compte sous lequel la ressource sera enregistrée.
- Disponibilité du plan.

Le tableau suivant résume les options possibles, qui sont répertoriées de manière hiérarchique. Si une option n'est pas disponible, la suivante dans la liste est appliquée. Si toutes les options possibles ne sont pas disponibles, aucun plan ne sera présélectionné.

Rôle de l'utilisateur qui enregistre la ressource	**Compte sous lequel la ressource sera enregistrée**	
	Compte dans un tenant client	**Compte dans une unité**
Compte de niveau partenaire avec l'un des rôles suivants dans le service **Protection** : • **Administrateur d'entreprise** • **Cyberadministrateur** • **Administrateur**	1. Plan par défaut au niveau du client 2. Plan par défaut au niveau du partenaire 3. Premier plan favori au niveau du client 4. Premier plan favori au niveau du partenaire 5. Plan sélectionné au hasard au niveau du client 6. Plan sélectionné au hasard au niveau du partenaire 7. Plan intégré* (appliqué en tant que plan au niveau du client)	1. Plan par défaut au niveau de l'unité 2. Plan par défaut au niveau du client 3. Plan par défaut au niveau du partenaire 4. Premier plan favori au niveau de l'unité 5. Premier plan favori au niveau du client 6. Premier plan favori au niveau du partenaire 7. Plan sélectionné au hasard au niveau de l'unité 8. Plan sélectionné au hasard au niveau du client 9. Plan sélectionné au hasard au niveau du partenaire 10. Plan intégré* (appliqué en tant que plan au niveau du client)
Compte au niveau client avec l'un des rôles suivants dans le service **Protection** : • **Administrateur d'entreprise** • **Cyberadministrateur** • **Administrateur**	1. Plan par défaut au niveau du client 2. Premier plan favori au niveau du client 3. Plan sélectionné au hasard au niveau du client 4. Plan intégré*	1. Plan par défaut au niveau de l'unité 2. Plan par défaut au niveau du client 3. Premier plan favori au niveau de l'unité 4. Premier plan favori au niveau du client 5. Plan sélectionné au hasard au niveau de l'unité 6. Plan sélectionné au hasard au niveau du client 7. Plan intégré*

© Acronis International GmbH, 2003-2026

Rôle de l'utilisateur qui enregistre la ressource	Compte sous lequel la ressource sera enregistrée	
	Compte dans un tenant client	**Compte dans une unité**
Compte au niveau client avec le rôle **Utilisateur** dans le service **Protection**	1. Plan par défaut au niveau du client (si le plan est créé par cet utilisateur) 2. Premier plan favori au niveau du client (si le plan est créé par cet utilisateur) 3. Plan, créé par cet utilisateur au niveau du client, sélectionné au hasard 4. Plan intégré*	Sans Objet
Compte au niveau de l'unité avec l'un des rôles suivants dans le service **Protection** : • **Administrateur de l'unité** • **Cyberadministrateur** • **Administrateur**	Sans Objet	1. Plan par défaut au niveau de l'unité 2. Premier plan favori au niveau de l'unité 3. Plan sélectionné au hasard au niveau de l'unité 4. Plan intégré*
Compte au niveau de l'unité avec le rôle **Utilisateur** dans le service **Protection**	Sans Objet	1. Plan par défaut au niveau de l'unité (si le plan est créé par cet utilisateur) 2. Premier plan favori au niveau de l'unité (si le plan est créé par cet utilisateur) 3. Plan sélectionné au hasard créé par cet utilisateur au niveau de l'unité 4. Plan intégré*

* Disponible uniquement pour les plans de protection.

Plans à différents niveaux d'administration

En fonction de leur niveau hiérarchique, les administrateurs peuvent créer et gérer des plans aux niveaux suivants :

- Niveau de partenaire (**Tous les clients**)
- Niveau client
- Niveau unité

© Acronis International GmbH, 2003-2026

Pour plus d'informations, voir "Niveaux d'administration dans la console Cyber Protect" (p. 387).

Les administrateurs de niveau supérieur peuvent créer et appliquer des plans dans leur propre tenant et dans les tenants enfants qu'ils gèrent. Les administrateurs de niveau inférieur ont un accès en lecture seule aux plans appliqués par les administrateurs de niveau supérieur et ne peuvent pas supprimer, modifier ou révoquer ces plans.

Lorsqu'il travaille à un niveau d'administration inférieur, un administrateur de niveau supérieur dispose des droits de l'administrateur de niveau inférieur. Par exemple, lorsqu'un administrateur partenaire travaille au niveau du client, l'administrateur partenaire dispose des droits d'un administrateur client.

Le tableau suivant résume les plans à différents niveaux d'administration, selon la hiérarchie des administrateurs.

Hiérarchie des administrateurs	Niveau d'administration	Plans	Access
Compte de niveau partenaire avec l'un des rôles suivants dans le service **Protection** : • **Administrateur d'entreprise** • **Cyberadministrateur** • **Administrateur**	Niveau partenaire	Plans partenaires (propriétaire)*	Accès complet
		Plans clients, y compris les plans dans les unités	Accès complet
		Plans d'unité	Accès complet
	Niveau client (pour les clients gérés par le fournisseur de services)	Plans partenaires appliqués aux ressources de ce client	Lecture seule
		Plans clients, y compris les plans dans les unités (propriétaire)*	Accès complet
		Plans d'unité	Accès complet
	Niveau unité (pour les clients gérés par le fournisseur de services)	Plans partenaires appliqués aux ressources de cette unité	Lecture seule
		Plans clients appliqués aux ressources de cette unité	Lecture seule
		Plans d'unité (propriétaire)*	Accès complet
Compte au niveau client avec l'un des rôles suivants dans le service **Protection** : • **Administrateur d'entreprise** • **Cyberadministrateur**	Niveau client	Plans partenaires appliqués aux ressources de ce client ou de cette unité	Lecture seule

© Acronis International GmbH, 2003-2026

Hiérarchie des administrateurs	Niveau d'administration	Plans	Access
• **Administrateur**			
		Plans clients, y compris les plans dans les unités (propriétaire)*	Accès complet
		Plans d'unité	Accès complet
	Niveau unité	Plans partenaires appliqués aux ressources de cette unité	Lecture seule
		Plans clients appliqués aux ressources de cette unité	Lecture seule
		Plans d'unité (propriétaire)*	Accès complet
Compte au niveau de l'unité avec l'un des rôles suivants dans le service **Protection** : • **Administrateur de l'unité** • **Cyberadministrateur** • **Administrateur**	Niveau unité	Plans partenaires appliqués aux ressources de cette unité	Lecture seule
		Plans clients appliqués aux ressources de cette unité	Lecture seule
		Plans d'unité (propriétaire)*	Accès complet

* Le propriétaire d'un plan est le tenant dans lequel le plan a été créé. Par exemple, si un administrateur partenaire crée un plan au niveau du client, le tenant client est le propriétaire de ce plan. Si un administrateur partenaire crée un plan au niveau du partenaire (**Tous les clients**), le tenant partenaire est le propriétaire du plan.

Tous les types de plans ne sont pas disponibles à tous les niveaux d'administration. Pour plus d'informations, voir "Présentation des plans" (p. 216).

État du plan

Pour certains plans, tels que les plans de protection et les plans de réplication de machines virtuelles, une barre d'état cliquable à code couleur est disponible. Elle indique l'état du plan sur toutes les ressources auxquelles ce plan est appliqué, comme suit :

- OK (vert)
- Avertissement (orange)
- Erreur (rouge)
- Le plan est en cours d'exécution (bleu)
- Le plan est désactivé (gris)

© Acronis International GmbH, 2003-2026

Vous pouvez cliquer sur une section de la barre d'état pour voir le nombre de ressources ayant ce statut.

Remarque
L'état d'un plan appliqué à une ressource peut ne pas correspondre à l'état de la ressource. Par exemple, un plan de protection peut être appliqué avec succès à une ressource, ce qui fait que son état s'affiche comme **OK** (vert). Cependant, si la ressource est hors ligne, son état dans l'onglet **Terminaux** sera rouge.

Plans et modules de protection

Pour protéger vos données, vous devez créer des plans de protection, puis les appliquer à vos ressources.

Un plan de protection se compose de différents modules de protection. Activez les modules dont vous avez besoin et configurez leurs paramètres afin de créer des plans de protection correspondant à vos besoins.

Les modules suivants sont disponibles :

- Sauvegarde. Sauvegarde vos sources de données dans un stockage local ou dans le Cloud.
- "Implémentation de la reprise d'activité après sinistre" (p. 1016). Lance des copies exactes de vos ordinateurs dans le cloud et bascule la ressource des ordinateurs d'origine corrompus vers les serveurs de restauration dans le cloud.
- Protection antivirus et antimalware. Vérifie les ressources à l'aide d'une solution antimalware intégrée.
- Endpoint Detection and Response (EDR). Détecte toute activité suspecte sur la ressource, y compris les attaques qui n'ont pas été identifiées, et génère des incidents qui vous aident à comprendre comment une attaque s'est produite et comment éviter qu'elle se reproduise.
- Filtrage des URL. Protège vos ordinateurs des menaces provenant d'Internet en bloquant l'accès aux URL et aux contenus téléchargeables malveillants.
- Sécurité de l'intelligence artificielle générative. Vous permet de contrôler, surveiller et appliquer une utilisation sécurisée des applications d'intelligence artificielle générative prises en charge à travers les ressources protégées
- Antivirus Windows Defender. Gère les paramètres de l'antivirus Windows Defender afin de protéger votre environnement.
- Microsoft Security Essentials. Gère les paramètres de Microsoft Security Essentials afin de protéger votre environnement.
- Évaluation des vulnérabilités. Recherche la présence de vulnérabilités dans les solutions Windows, Linux, macOS, Microsoft tierces et macOS tierces installées sur vos ordinateurs, et vous prévient le cas échéant.
- Gestion des correctifs. Installe des correctifs et des mises à jour pour les solutions Windows, Linux, macOS, Microsoft tierces et macOS tierces sur vos ordinateurs afin de résoudre les vulnérabilités détectées.

© Acronis International GmbH, 2003-2026

- Carte de protection des données. Découvre les données afin de surveiller l'état de protection des fichiers importants.
- Contrôle des terminaux. Spécifie les terminaux que les utilisateurs sont autorisés ou ne sont pas autorisés à utiliser sur leurs ordinateurs.
- Data Loss Prevention. Empêche la fuite de données sensibles via des périphériques (tels que des imprimantes ou un stockage amovible) ou par des transferts réseau internes et externes, selon la stratégie de flux de données.

Remarque
La disponibilité des modules dépend des éléments de l'offre qui sont activés pour votre compte et du niveau d'administration dans la console Cyber Protect. Pour plus d'informations, voir "Présentation des plans" (p. 216).

Création d'un plan de protection

Vous pouvez créer un plan de protection de l'une des manières suivantes :

- Dans l'onglet **Terminaux**. Sélectionnez une ou plusieurs ressources à protéger, puis créez un plan de protection pour elles. Seuls les modules applicables aux types de ressources sélectionnés sont affichés.
- Dans l'onglet **Gestion** > **Plans de protection**. Créez un plan de protection, puis sélectionnez une ou plusieurs ressources auxquelles l'appliquer.

Vous pouvez appliquer un plan de protection à plusieurs ressources ou plusieurs plans de protection à une même ressource. Pour en savoir plus sur les conflits éventuels, reportez-vous à "Résolution des problèmes de compatibilité" (p. 253).

Lorsque vous créez un module de protection avec le module **Sauvegarde** activé, vous pouvez activer le chiffrement de sauvegarde. Pour plus d'informations, voir "Chiffrement" (p. 596).

Pour créer un plan de protection

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les ressources que vous souhaitez protéger, puis cliquez sur **Protection**.
3. [Si des plans sont déjà appliqués] Cliquez sur **Ajouter un plan**.
4. Cliquez sur **Création d'un plan** > **Protection**.
   Le tableau de bord du plan de protection s'ouvre.
5. [Facultatif] Pour modifier le nom du plan de protection, cliquez sur l'icône représentant un crayon, spécifiez un nouveau nom, puis cliquez sur **OK**.
6. [Facultatif] Pour activer ou désactiver un module du plan, utilisez l'interrupteur à côté du nom du module.
7. [Facultatif] Pour configurer un module, développez-le, puis modifiez les paramètres.
8. Cliquez sur **Créer**.

© Acronis International GmbH, 2003-2026

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Sélectionnez un modèle basé sur un plan intégré, ou sélectionnez **Créer votre propre plan** pour configurer un plan à partir de zéro, puis cliquez sur **Suivant**.
4. [Facultatif] Pour modifier le nom du plan, cliquez sur l'icône représentant un crayon, spécifiez un nouveau nom, puis cliquez sur **OK**.
5. [Facultatif] Pour activer ou désactiver un module du plan, utilisez l'interrupteur à côté du nom du module.
6. [Facultatif] Pour configurer un module, développez-le, puis modifiez les paramètres selon vos besoins.
7. [Facultatif] Pour ajouter des ressources au plan, cliquez sur **Ajouter des terminaux**, puis sélectionnez les ressources.

   Remarque
   Vous pouvez créer un plan sans ajouter de ressources. Pour ajouter des ressources plus tard, modifiez le plan. Pour plus d'informations, voir "Application d'un plan de protection à une ressource" (p. 246).

8. Cliquez sur **Créer**.

Pour exécuter un module à la demande (**Sauvegarde**, **Protection contre les virus et les malwares**, **Évaluation des vulnérabilités**, **Gestion des correctifs** ou **Carte de la protection des données**), cliquez sur **Exécuter maintenant**.

Regardez la vidéo pratique Création du premier plan de protection.

Pour plus d'informations sur le module de reprise d'activité après sinistre, voir "Création d'un plan de protection de reprise d'activité après sinistre" (p. 1022).

Pour plus d'informations sur le module de contrôle des terminaux, voir "Utilisation du module de contrôle des terminaux" (p. 448).

Actions avec plans de protection

Après avoir créé un plan de protection, vous pouvez l'utiliser pour exécuter les opérations suivantes :

- Appliquer un plan à une ressource ou à un groupe de terminaux.
- Renommer le plan.
- Modifier un plan.
  Vous pouvez activer et désactiver les modules d'un plan, et modifier ses paramètres.
- Activer ou désactiver un plan.
  Un plan désactivé ne sera pas exécuté sur les ressources auxquelles il est appliqué.

© Acronis International GmbH, 2003-2026

Cette action est utile pour les administrateurs qui prévoient de protéger ultérieurement la même ressource avec le même plan. Le plan n'est pas révoqué de la ressource et vous pouvez restaurer la protection en réactivant le plan.

- Révoquer un plan d'une ressource.

  Un plan révoqué n'est plus appliqué à la ressource.

  Cette action est utile pour les administrateurs qui n'ont pas besoin de protéger rapidement la même ressource avec le même plan. Pour restaurer la protection d'un plan révoqué, vous devez connaître le nom de ce plan, le sélectionner dans la liste des plans disponibles et le réappliquer à la ressource correspondante.
- Arrêter un plan

  Cette action arrête toutes les opérations de sauvegarde en cours d'exécution sur toutes les ressources auxquelles le plan est appliqué. Les sauvegardes redémarrent en fonction de la planification du plan.

  L'analyse antimalware n'est pas concernée par cette action et se poursuit conformément à la configuration de la planification.
- Cloner un plan.

  Vous pouvez créer une copie exacte d'un plan existant. Le nouveau plan n'est affecté à aucune ressource.
- Exporter et importer un plan.

  Vous pouvez exporter un plan sous forme de fichier JSON que vous pourrez réimporter ultérieurement. Par conséquent, vous n'avez pas besoin de créer un nouveau plan manuellement et de configurer ses paramètres.

Remarque
Cette fonctionnalité n'est pas disponible pour les plans au niveau partenaire. Pour plus d'informations sur ce niveau, voir "Niveaux d'administration dans la console Cyber Protect" (p. 387).

- Vérifier les détails d'un plan.
- Vérifiez les activités et les alertes relatives à un plan.
- Supprimer un plan.

Application d'un plan de protection à une ressource

Pour protéger une ressource, vous devez lui appliquer un plan de protection.

Vous pouvez appliquer un plan à partir de l'onglet **Terminaux** et de l'onglet **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez une ou plusieurs ressources à protéger.
2. Cliquez sur **Protection**.

© Acronis International GmbH, 2003-2026

3. [Si un autre plan de protection est déjà appliqué aux ressources sélectionnées] Cliquez sur **Ajouter un plan**.
   La liste des plans de protection disponibles s'affiche.
4. Sélectionnez le plan de protection que vous souhaitez appliquer, puis cliquez sur **Appliquer**.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez appliquer.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Gérer les terminaux**.
5. Dans la fenêtre **Terminaux**, cliquez sur **Ajouter**.
6. Sélectionnez les ressources auxquelles vous souhaitez appliquer le plan, puis cliquez sur **Ajouter**.
7. Dans la fenêtre **Terminaux**, cliquez sur **Terminé**.
8. Dans le tableau de bord du plan de protection, cliquez sur **Enregistrer**.

Pour savoir comment appliquer un plan de protection à un groupe de terminaux, voir "Application d'un plan à un groupe" (p. 446).

Modification d'un plan de protection

Lorsque vous modifiez un plan, vous pouvez activer et désactiver ses modules, et modifier leurs paramètres.

Vous pouvez modifier un plan de protection pour toutes les ressources auxquelles il est appliqué ou uniquement pour les ressources sélectionnées.

Vous pouvez modifier un plan à partir des onglets **Terminaux** et **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez une ou plusieurs ressources auxquelles le plan est appliqué.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez modifier.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan, puis sur **Modifier**.
5. Cliquez sur un module que vous souhaitez modifier, puis configurez ses paramètres en fonction de vos besoins.
6. Cliquez sur **Enregistrer**.
7. [Si vous n'avez pas sélectionné toutes les ressources auxquelles le plan est appliqué]
   Sélectionnez le champ d'application de la modification :
   - Pour modifier le plan pour toutes les ressources auxquelles il est appliqué, cliquez sur **Appliquer les modifications à ce plan (cela a une incidence sur d'autres terminaux)**.

© Acronis International GmbH, 2003-2026

- Pour ne modifier le plan que pour les ressources sélectionnées, cliquez sur **Créer un plan de protection pour les terminaux sélectionnés uniquement**.
  En conséquence, le plan existant sera révoqué des ressources sélectionnées. Un nouveau plan de protection avec les paramètres que vous avez configurés sera créé et appliqué à ces ressources.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Cliquez sur les modules que vous souhaitez modifier, puis configurez leurs paramètres en fonction de vos besoins.
5. Cliquez sur **Enregistrer**.

Remarque
La modification d'un plan à partir de l'onglet **Gestion** > **Plans de protection** a une incidence sur toutes les ressources auxquelles ce plan est appliqué.

Exporter un plan de protection

Vous pouvez exporter un plan de protection dans un fichier JSON.

Remarque
Cette fonctionnalité n'est pas disponible pour les plans au niveau partenaire. Pour plus d'informations sur ce niveau, voir "Niveaux d'administration dans la console Cyber Protect" (p. 387).

Prérequis

Au moins un plan de protection est disponible pour votre tenant.

Pour exporter un plan de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur le plan que vous souhaitez exporter, puis dans le menu **Actions**, cliquez sur **Exporter**.
   Un fichier JSON contenant la configuration est créé et enregistré dans le dossier de téléchargement par défaut de votre ordinateur.

Importer un plan de protection

Vous pouvez importer des plans de protection qui ont été exportés dans un fichier JSON. Vous pouvez ainsi gagner du temps et garantir la cohérence des paramètres entre les tenants.

© Acronis International GmbH, 2003-2026

Remarque
Cette fonctionnalité n'est pas disponible pour les plans au niveau partenaire. Pour plus d'informations sur ce niveau, voir "Niveaux d'administration dans la console Cyber Protect" (p. 387).

Prérequis

Un fichier JSON avec la configuration du plan est disponible sur l'ordinateur à partir duquel vous êtes connecté à la console.

Pour importer un plan de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Dans le menu **Actions**, cliquez sur **Importer**.
3. Dans la fenêtre qui s'ouvre, parcourez jusqu'au fichier JSON.
4. Cliquez sur le fichier, puis cliquez sur **Ouvrir**.
   Le plan de protection apparaît à l'écran. Vous pouvez maintenant l'appliquer aux ressources.

Révocation d'un plan de protection

Lorsque vous retirez un plan, vous le supprimez d'une ou de plusieurs ressources. Le plan continue à protéger les autres ressources auxquelles il est appliqué.

Vous pouvez révoquer un plan à partir des onglets **Terminaux** et **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez les ressources à partir desquelles vous voulez révoquer le plan.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez révoquer.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan, puis sur **Retirer**.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez révoquer.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Gérer les terminaux**.
5. Dans la fenêtre **Terminaux**, sélectionnez les ressources à partir desquelles vous souhaitez révoquer le plan.
6. Cliquez sur **Supprimer**.
7. Dans la fenêtre **Terminaux**, cliquez sur **Terminé**.
8. Dans le modèle de plan de protection, cliquez sur **Enregistrer**.

© Acronis International GmbH, 2003-2026

Activation ou désactivation d'un plan de protection

Un plan activé est actif et s'exécute sur les ressources auxquelles il est appliqué. Un plan désactivé est inactif : il est toujours appliqué aux ressources, mais il ne s'y exécute pas.

Lorsque vous activez ou désactivez un plan de protection depuis l'onglet **Terminaux**, votre action n'a une incidence que sur les ressources sélectionnées.

Lorsque vous activez ou désactivez un plan de protection à partir de l'onglet **Gestion** > **Plans de protection**, votre action a une incidence sur toutes les ressources auxquelles ce plan est appliqué. Par ailleurs, vous pouvez activer ou désactiver plusieurs plans de protection.

Terminaux

1. Sélectionnez la ressource que vous envisagez de désactiver.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez désactiver.
4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan, puis sur **Activer** ou sur **Désactiver** respectivement.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez un ou plusieurs plans de protection que vous souhaitez activer ou désactiver.
3. Cliquez sur **Modifier**.
4. Cliquez sur **Activer** ou **Désactiver** respectivement.

Remarque
Cette action n'a aucune incidence sur les plans de protection qui étaient déjà dans l'état cible. Par exemple, si votre sélection comprend des plans activés et désactivés, et que vous cliquiez sur **Activer**, tous les plans sélectionnés seront activés.

Suppression d'un plan de protection

Lorsque vous supprimez un plan, il est révoqué à partir de toutes les ressources et est supprimé de la console Cyber Protect.

Vous pouvez supprimer un plan à partir des onglets **Terminaux** et **Gestion** > **Plans de protection**.

Terminaux

1. Sélectionnez une ressource à laquelle le plan de protection que vous voulez supprimer est appliqué.
2. Cliquez sur **Protection**.
3. Sélectionnez le plan de protection que vous souhaitez supprimer.

© Acronis International GmbH, 2003-2026

4. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sur **Supprimer**.

Gestion > Plans de protection

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez votre choix en cochant la case **Je confirme la suppression du plan**, puis cliquez sur **Supprimer**.

Plans de protection individuels pour l'hébergement des intégrations du panneau de configuration

Lorsque vous activez l'hébergement des intégrations du panneau de configuration sur les serveurs d'hébergement Web qui utilisent DirectAdmin, cPanel ou Plesk, le service Cyber Protection crée automatiquement un plan de protection individuel sous le compte utilisateur pour chaque ressource. Ce plan de protection est associé à la ressource spécifique qui a lancé la création du plan de protection et il ne peut être ni révoqué ni affecté à d'autres ressources.

Pour ne plus utiliser un plan de protection individuel, vous pouvez le supprimer depuis la console Cyber Protect. Vous pouvez identifier les plans de protection individuels à l'aide du signe qui figure après leur nom.

Si vous souhaitez qu'un plan de protection protège plusieurs serveurs d'hébergement Web utilisant les intégrations du panneau de configuration, vous pouvez créer un plan de protection standard dans la console Cyber Protect et lui affecter ces ressources. Toutefois, les modifications apportées à un plan de protection partagé par plusieurs panneaux de configuration d'hébergement Web ne peuvent être effectuées que dans la console Cyber Protect, pas depuis les intégrations.

Problèmes de compatibilité avec les plans

Dans certains cas, l'application d'un plan sur une ressource peut provoquer des problèmes de compatibilité.

Vous pouvez observer les problèmes suivants :

- Plan en conflit : il existe un conflit entre le plan que vous appliquez et un plan déjà appliqué.
  Par exemple, certains paramètres du plan peuvent entrer en conflit avec les paramètres du plan déjà appliqué, ou la même ressource peut déjà avoir été protégée en tant que partie d'un groupe de terminaux.
- Système d'exploitation incompatible : le système d'exploitation de la ressource n'est pas pris en charge.
- Agent non pris en charge : la version de l'agent de protection sur la ressource est obsolète et ne prend pas en charge la fonctionnalité configurée.

© Acronis International GmbH, 2003-2026

- Quota insuffisant : le quota de service dans le tenant est insuffisant pour l'affectation à la ressource sélectionnée.
- Type de ressource incompatible : la fonctionnalité sélectionnée n'est pas disponible pour ce type de ressource.
- Pack Advanced manquant : la fonctionnalité sélectionnée n'est pas disponible, car un pack Advanced requis n'est pas activé pour ce client.

Le tableau suivant récapitule les problèmes de compatibilité possibles pour différents types de plans.

Problème/Type de plan	Plan de protection	Plan de création de script	Plan de surveillance	Plan de gestion à distance	Plan de déploiement logiciel
Plan en conflit	+*	-	-	+	-
Système d'exploitation incompatible	+	+	+	+	+
Agent non pris en charge	+	+	+	+	+
Quota insuffisant	+	+	+	+	-
Type de ressource incompatible	+	+	+	+	-
Pack Advanced manquant	+	-	-	-	-

* Aucun conflit n'est déclenché si des paramètres de sauvegarde différents sont configurés dans plusieurs plans de protection pour la même ressource.

Si le plan est appliqué à 150 ressources sélectionnées au maximum, vous serez invité à résoudre les conflits existants avant d'enregistrer le plan. Pour résoudre un conflit, supprimez sa cause première ou les ressources concernées du plan. Pour plus d'informations, voir "Résolution des problèmes de compatibilité" (p. 253). Si vous ne résolvez pas les conflits et selon du type de problème de compatibilité, le plan dans son intégralité ou certains de ses modules seront désactivés sur les ressources incompatibles, et des alertes s'afficheront.

Si le plan est appliqué à plus de 150 ressources ou à des groupes de terminaux, il sera d'abord enregistré, puis sa compatibilité sera vérifiée. Selon le type de problème de compatibilité, l'intégralité du plan ou certains de ses modules seront désactivés sur les ressources incompatibles, et des alertes seront affichées.

© Acronis International GmbH, 2003-2026

Résolution des problèmes de compatibilité

Selon la cause des problèmes de compatibilité, vous pouvez effectuer différentes actions afin de résoudre les problèmes de compatibilité dans le cadre du processus de création ou de modification d'un plan.

Pour résoudre les problèmes de compatibilité

Plan en conflit

1. Cliquez sur **Examiner les problèmes**.
2. [Pour résoudre le problème en supprimant les ressources du nouveau plan]
   a. Dans l'onglet **Plan en conflit**, sélectionnez les ressources que vous souhaitez supprimer.

      Remarque
      Vous ne pouvez pas supprimer les ressources qui font partie d'un groupe de terminaux.

   b. Cliquez sur **Supprimer les ressources sélectionnées du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
3. [Pour résoudre le problème en désactivant les plans déjà appliqués à la ressource]
   a. Cliquez sur **Désactiver les plans appliqués**.
   b. Cliquez sur **Désactiver**, puis sur **Fermer**.
4. [Pour résoudre le problème en désactivant les modules en conflit dans les plans déjà appliqués à la ressource]
   a. Cliquez sur **Désactiver les modules en conflit dans les plans appliqués**.
   b. Cliquez sur **Désactiver**, puis sur **Fermer**.

Système d'exploitation incompatible

1. Cliquez sur **Examiner les problèmes**.
2. [Pour résoudre le problème en supprimant les ressources du plan]
   a. Dans l'onglet **Système d'exploitation incompatible**, sélectionnez les ressources que vous souhaitez supprimer.
   b. Cliquez sur **Supprimer les ressources du plan**.
   c. Cliquez sur **Supprimer**, puis sur **Fermer**.
3. [Pour les plans de surveillance] [Pour résoudre le problème en désactivant un moniteur dans le plan]
   a. Dans l'onglet **Système d'exploitation incompatible**, sélectionnez les moniteurs que vous souhaitez supprimer.
   b. Cliquez sur **Désactiver le moniteur**.
   c. Cliquez sur **Désactiver**, puis sur **Fermer**.

© Acronis International GmbH, 2003-2026

4. [Pour les plans autres que les plans de surveillance] [Pour résoudre le problème en désactivant un module dans le plan]
   a. Dans l'onglet **Système d'exploitation incompatible**, développez le module en conflit.
   b. Cliquez sur **Désactiver le module dans le plan**.
   c. Cliquez sur **Désactiver**, puis sur **Fermer**.

Agent non pris en charge

1. Cliquez sur **Examiner les problèmes**.
2. Dans l'onglet **Agent non pris en charge**, sélectionnez les ressources que vous souhaitez supprimer.
3. Cliquez sur **Supprimer les ressources du plan**.
4. Cliquez sur **Supprimer**, puis sur **Fermer**.

Quota insuffisant

1. Cliquez sur **Examiner les problèmes**.
2. Dans l'onglet **Quota insuffisant**, sélectionnez les ressources que vous souhaitez supprimer.
3. Cliquez sur **Supprimer les ressources du plan**.
4. Cliquez sur **Supprimer**, puis sur **Fermer**.

Type de ressource incompatible

1. Cliquez sur **Examiner les problèmes**.
2. Dans l'onglet **Quota insuffisant**, sélectionnez les ressources que vous souhaitez supprimer.
3. Cliquez sur **Supprimer les ressources du plan**.
4. Cliquez sur **Supprimer**, puis sur **Fermer**.

Pack Advanced manquant

1. Cliquez sur **Examiner les problèmes**.
2. [Pour résoudre le problème en supprimant les ressources du nouveau plan] Dans l'onglet **Pack Advanced manquant**, sélectionnez les ressources que vous souhaitez supprimer.
   - Cliquez sur **Supprimer les ressources du plan**.
   - Cliquez sur **Supprimer**, puis sur **Fermer**.
3. [Pour résoudre le problème en activant le pack Advanced requis]
   - [Pour les administrateurs partenaires] Accédez au portail de gestion, puis activez le pack Advanced requis pour ce client.

© Acronis International GmbH, 2003-2026

Plans de protection des données hors hôte

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

La réplication, la validation et le nettoyage sont généralement effectués par l'agent de protection qui effectue la sauvegarde. Cela représente une charge supplémentaire pour l'ordinateur sur lequel l'agent s'exécute, même après la fin du processus de sauvegarde. Pour décharger l'ordinateur, vous pouvez créer des plans de protection des données hors hôte, c'est-à-dire des plans distincts pour la réplication, la validation, le nettoyage et la conversion en machine virtuelle.

Les plans de protection des données hors hôte permettent d'effectuer les opérations suivantes :

- Choisir des agents différents pour les opérations de sauvegarde et de protection des données hors hôte
- Programmez les opérations de traitement des données hors hôte pendant les heures creuses afin de minimiser la consommation de la bande passante du réseau.
- Si vous ne souhaitez pas installer un agent dédié au traitement des données hors hôte, planifiez les opérations de traitement des données hors hôte en dehors des heures de bureau.

Remarque
Les plans de traitement des données hors hôte s'exécutent en fonction des paramètres temporels (y compris le fuseau horaire) de l'ordinateur sur lequel l'agent de protection est installé. Pour une appliance virtuelle (par exemple, Agent for VMware ou Agent for Scale Computing HC3), vous pouvez configurer le fuseau horaire dans l'interface utilisateur graphique de l'agent.

Réplication de sauvegarde

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

La réplication de sauvegarde copie une sauvegarde vers un autre emplacement. En tant qu'opération de traitement des données hors hôte, elle est configurée dans un plan de réplication de sauvegarde.

La réplication de sauvegarde peut également faire partie d'un plan de protection. Pour plus d'informations sur cette option, reportez-vous à "Réplication" (p. 594).

Création d'un plan de réplication de sauvegarde

Pour répliquer les sauvegardes en tant qu'opération de traitement des données hors hôte, vous créez un plan de réplication des sauvegardes.

© Acronis International GmbH, 2003-2026

Pour créer un plan de réplication de sauvegarde

1. Dans la console Cyber Protect, cliquez sur **Gestion** > **Réplication des sauvegardes**.
2. Cliquez sur **Création d'un plan**.
3. Dans **Agent**, sélectionnez l'agent qui effectuera la réplication.
   Vous pouvez sélectionner n'importe quel agent ayant accès à la fois à l'emplacement source et aux emplacements de réplication.
4. Dans **Éléments à répliquer**, sélectionnez les archives ou les emplacements de sauvegarde à répliquer.
   Pour naviguer entre les archives et les emplacements, utilisez le commutateur **Emplacements** / **Sauvegardes** dans le coin supérieur droit.
   Si vous sélectionnez plusieurs archives chiffrées, leur mot de passe de cryptage doit être identique. Pour les archives qui utilisent des mots de passe de cryptage différents, créez des plans distincts.
5. Dans **Destination**, indiquez l'emplacement de réplication.
6. Dans **Comment répliquer**, sélectionnez les sauvegardes (également appelées points de restauration) à répliquer.
   Les options suivantes sont disponibles :
   - **Toutes les sauvegardes**
   - **Sauvegardes complètes uniquement**
   - **Dernière sauvegarde uniquement**

   Pour plus d'informations sur ces options, reportez-vous à "Que répliquer" (p. 257).
7. Dans **Planification**, configurez la planification de réplication.
   Lors de la configuration de la planification de la réplication des sauvegardes, assurez-vous que la dernière sauvegarde répliquée sera toujours disponible à son emplacement d'origine lorsque la réplication des sauvegardes commencera. Si cette sauvegarde n'est pas disponible à l'emplacement d'origine, par exemple parce qu'elle a été supprimée par une règle de conservation, l'archive entière sera répliquée en tant que sauvegarde complète. Cela peut prendre beaucoup de temps et utiliser de l'espace de stockage supplémentaire.
8. Dans **Règles de rétention**, spécifiez les règles de rétention pour l'emplacement cible.
   Les options suivantes sont disponibles :
   - **Par nombre de sauvegardes**
   - **Par âge des sauvegardes** (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires)
   - **Par volume total de sauvegardes**
   - **Conserver les sauvegardes indéfiniment**

     Remarque
     La sélection de cette option entraînera une augmentation de l'utilisation de l'espace de stockage. Vous devez supprimer manuellement les sauvegardes inutiles.

© Acronis International GmbH, 2003-2026

9. [Si vous avez sélectionné des archives cryptées dans les **Éléments à répliquer**] Activez le commutateur **Mot de passe de sauvegarde**, puis fournissez le mot de passe de chiffrement.
10. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône engrenage, puis configurez les options selon vos besoins.
11. Cliquez sur **Créer**.

Que répliquer

Remarque
Certaines opérations de réplication telles que la réplication d'un emplacement complet ou la réplication de toutes les sauvegardes d'un ensemble de sauvegardes peuvent être longues.

Vous pouvez répliquer des ensembles de sauvegardes ou des emplacements de sauvegarde complets. Lorsque vous répliquez un emplacement de sauvegarde, tous les ensembles de sauvegardes sont répliqués.

Les ensembles de sauvegardes sont composés de sauvegardes (appelés également points de restauration). Vous devez sélectionner les sauvegardes à répliquer.

Les options suivantes sont disponibles :

- **Toutes les sauvegardes**
  Toutes les sauvegardes de l'ensemble de sauvegardes sont répliquées à chaque exécution d'un plan de réplication.
- **Sauvegardes complètes uniquement**
  Seules les sauvegardes complètes de l'ensemble de sauvegardes sont répliquées.
- **Dernière sauvegarde uniquement**
  Seule la dernière sauvegarde de l'ensemble est répliquée, quel que soit son type (complète, différentielle ou incrémentielle).

Sélectionnez une option adaptée à vos besoins, ainsi que le modèle de sauvegarde que vous utilisez. Par exemple, si vous utilisez le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** et souhaitez répliquer uniquement la dernière sauvegarde incrémentielle, sélectionnez **Dernière sauvegarde uniquement** dans le plan de réplication de sauvegarde.

Le tableau suivant récapitule les sauvegardes qui seront répliquées en fonction des différents modèles de sauvegarde.

	Toujours incrémentielle (fichier unique)	**Toujours complète**	**Complète hebdomadaire, incrémentielle journalière**	**Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)**
Toutes les sauvegardes	Toutes les	Toutes les	Toutes les	Toutes les

© Acronis International GmbH, 2003-2026

	Toujours incrémentielle (fichier unique)	Toujours complète	Complète hebdomadaire, incrémentielle journalière	Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)
	sauvegardes de l'ensemble de sauvegarde	sauvegardes de l'ensemble de sauvegarde	sauvegardes de l'ensemble de sauvegarde	sauvegardes de l'ensemble de sauvegarde
Sauvegardes complètes uniquement	Uniquement la première sauvegarde complète	Toutes les sauvegardes	Une sauvegarde par semaine*	Une sauvegarde par mois*
Dernière sauvegarde uniquement	La dernière sauvegarde de l'ensemble de sauvegardes uniquement*	La dernière sauvegarde de l'ensemble de sauvegardes uniquement*	La dernière sauvegarde de l'ensemble de sauvegardes uniquement, quel que soit son type*	La dernière sauvegarde de l'ensemble de sauvegardes uniquement, quel que soit son type*

*Lors de la configuration de la planification de la réplication des sauvegardes, assurez-vous que la dernière sauvegarde répliquée sera toujours disponible à son emplacement d'origine lorsque la réplication des sauvegardes commencera. Si cette sauvegarde n'est pas disponible à l'emplacement d'origine, par exemple parce qu'elle a été supprimée par une règle de conservation, l'archive entière sera répliquée en tant que sauvegarde complète. Cela peut prendre beaucoup de temps et utiliser de l'espace de stockage supplémentaire.

Emplacements pris en charge pour le traitement des données hors hôte

Le tableau suivant récapitule les emplacements de sauvegarde pris en charge dans les plans de réplication de sauvegarde de traitement de données hors hôte.

Emplacement de sauvegarde	Pris en charge comme source	Pris en charge comme cible
Stockage dans le Cloud	+	+
Dossier local	+	+
Dossier réseau	+	+
Cloud public	+	+
Dossier NFS	–	–
Secure Zone	–	–

© Acronis International GmbH, 2003-2026

Validation

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

Vous pouvez valider une sauvegarde pour vérifier que vous pouvez restaurer les données.

Lorsque vous validez une sauvegarde, vous appliquez une méthode de validation à une archive de sauvegarde ou à un emplacement de sauvegarde. La validation d'un emplacement de sauvegarde valide toutes les archives de cet emplacement.

Pour valider une sauvegarde en tant que traitement des données hors hôte, vous devez créer un plan de validation. Pour plus d'informations, voir "Création d'un plan de validation" (p. 264).

Pour valider une sauvegarde sans créer de plan de validation, suivez la procédure figurant dans "Validation des sauvegardes" (p. 736).

Emplacements pris en charge pour la validation

Le tableau suivant répertorie les méthodes de validation et les emplacements de sauvegarde pris en charge.

Remarque
L'option de validation n'est pas disponible pour les sauvegardes dans le cloud public en raison des coûts prohibitifs de lecture d'une archive complète depuis un cloud public.

Emplacement de sauvegarde	Vérification de la somme de contrôle	Exécuter en tant que machine virtuelle	
		Pouls de la MV	Validation de l'instantané
Stockage dans le Cloud	+	+	+
Dossier local	+	+	+
Dossier réseau	+	+	+
Dossier NFS	–	–	–
Secure Zone	–	–	–

Méthodes de validation

Vous pouvez sélectionner une ou plusieurs méthodes de validation. Si plusieurs méthodes de validation sont sélectionnées, elles sont appliquées dans l'ordre suivant :

© Acronis International GmbH, 2003-2026

- Pouls de la VM (partie de l'option de validation **Exécuter en tant que machine virtuelle**)
- Validation de capture d'écran (partie de l'option de validation **Exécuter en tant que machine virtuelle**)
- Vérification de la somme de contrôle

L'option de validation **Exécuter en tant que machine virtuelle** est disponible uniquement pour les sauvegardes de disque qui contiennent un système d'exploitation. Vous pouvez l'utiliser sur des hôtes ESXi ou Hyper-V qui sont gérés par un agent de protection (agent pour VMware ou agent pour Hyper-V).

Pouls de la MV

Avec cette méthode de validation, l'agent exécute une machine virtuelle à partir de la sauvegarde, la connecte à des services d'intégration VMware Tools ou Hyper-V, puis vérifie la réponse de pouls afin de garantir que le système d'exploitation a démarré avec succès. Si la connexion échoue, l'agent essaie de se connecter toutes les deux minutes pour un total de cinq tentatives. Si aucune des tentatives n'est fructueuse, la validation échoue.

Quel que soit le nombre de plans de validation et de sauvegardes validées, l'agent qui effectue la validation exécute une seule machine virtuelle à la fois. Dès que le résultat de la validation est tangible, l'agent supprime la machine virtuelle, puis exécute la suivante.

Remarque
Utilisez cette méthode uniquement lorsque vous validez des sauvegardes de machines virtuelles VMware en exécutant ces sauvegardes sous forme de machines virtuelles sur un hôte ESXi, ainsi que des sauvegardes de machines virtuelles Hyper-V en les exécutant sous forme de machines virtuelles sur un hôte Hyper-V.

Validation de l'instantané

Avec cette méthode de validation, l'agent exécute une machine virtuelle à partir de la sauvegarde et, pendant le démarrage de la machine virtuelle, des captures d'écran sont prises pendant une période spécifique. Pour plus d'informations sur cette période, voir "Modification du délai d'expiration de la validation du pouls et des captures d'écran d'une machine virtuelle" (p. 262).

Un module d'intelligence machine (IM) vérifie les captures d'écran, et une capture d'écran est jointe à chaque sauvegarde validée (point de restauration).

Si une capture d'écran contient un écran de connexion, aucune autre capture d'écran n'est prise et cette capture d'écran est jointe. Si aucune capture d'écran ne contient un écran de connexion, des captures d'écran sont prises jusqu'à la fin de la période d'expiration, puis la dernière capture d'écran est jointe.

Dans la console Cyber Protect, vous pouvez télécharger la capture d'écran jointe dans l'année suivant la validation. Pour plus d'informations sur l'affichage de la capture d'écran, voir "Vérification du statut de validation" (p. 263).

© Acronis International GmbH, 2003-2026

Si les notifications sont activées pour votre compte utilisateur, vous recevrez un e-mail concernant le statut de validation de la sauvegarde. L'e-mail contient l'instantané en pièce jointe. Pour plus d'informations sur les notifications, voir Modification des paramètres de notification pour un utilisateur.

La validation d'instantané est prise en charge par l'agent des versions 15.0.30971 (sortie en novembre 2022) et ultérieures.

Remarque
La validation d'instantané est plus efficace avec les sauvegardes de systèmes Windows et Linux avec écran de connexion basé sur l'interface utilisateur graphique. Cette méthode n'est pas optimisée pour les systèmes Linux avec écran de connexion à la console.

Si les notifications sont activées pour votre compte utilisateur, vous recevrez un e-mail concernant le statut de validation de la sauvegarde. Pour plus d'informations sur les notifications, voir Modification des paramètres de notification pour un utilisateur.

Vérification de la somme de contrôle

La validation via la vérification de la somme de contrôle calcule une somme de contrôle pour chaque bloc de données restauré depuis la sauvegarde, puis la compare à la somme de contrôle d'origine pour ce bloc de données qui a été écrite pendant la sauvegarde. La seule exception concerne la validation des sauvegardes de niveau fichier se trouvant dans le stockage dans le cloud. Ces sauvegardes sont validées une fois que la cohérence des métadonnées enregistrées dans la sauvegarde a été vérifiée.

La validation via la vérification de la somme de contrôle est une opération qui prend du temps, même pour les sauvegardes incrémentielles ou différentielles, qui sont généralement de petite taille. L'opération de validation inclut toutes les données qui doivent être restaurées. Dans le cas de sauvegardes incrémentielles et différentielles, ces données peuvent être contenues dans plusieurs sauvegardes.

Une validation réussie par vérification de la somme de contrôle garantit une forte probabilité de restauration de données. Toutefois, la validation par cette méthode ne vérifie pas tous les facteurs qui influencent le processus de restauration.

Si les notifications sont activées pour votre compte utilisateur, vous recevrez un e-mail concernant le statut de validation de la sauvegarde. Pour plus d'informations sur les notifications, voir Modification des paramètres de notification pour un utilisateur.

Si vous sauvegardez un système d'exploitation, nous vous recommandons d'utiliser certaines des opérations supplémentaires suivantes :

- Testez la restauration du support de démarrage vers un disque dur de secours.
- Exécution d'une machine virtuelle à partir de la sauvegarde dans un environnement ESXi ou Hyper-V.
- Exécution d'un plan de validation dans lequel la méthode de validation **Exécuter en tant que machine virtuelle** est activée.

© Acronis International GmbH, 2003-2026

Modification du délai d'expiration de la validation du pouls et des captures d'écran d'une machine virtuelle

Lorsque vous validez une sauvegarde en l'exécutant en tant que machine virtuelle, vous pouvez configurer le délai d'expiration entre le démarrage de la machine virtuelle, et l'envoi de la demande de pouls ou la création d'une capture d'écran.

La période par défaut est la suivante :

- Une minute : pour les sauvegardes stockées dans un dossier local ou un partage réseau.
- Cinq minutes : pour les sauvegardes stockées dans le cloud.

Pour modifier le délai d'expiration

1. Ouvrez le fichier de configuration de l'agent pour VMware ou de l'agent pour Hyper-V pour le modifier.

   Le fichier de configuration est disponible dans les emplacements suivants :
   - [Pour l'agent pour VMware ou pour Hyper-V s'exécutant sous Windows] `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - [Pour l'agent pour VMware (appliance virtuelle)] `/bin/mms_settings.config`

     Pour plus d'informations sur l'accès au fichier de configuration sur une appliance virtuelle, voir "Connexions SSH à une appliance virtuelle" (p. 180).
2. Accédez à `<validation>`, puis modifiez les valeurs des sauvegardes locales et dans le cloud en fonction des besoins :

   ```
   <validation>
   <run_vm>
   <initial_timeout_minutes>
   <local_backups>1</local_backups>
   <cloud_backups>5</cloud_backups>
   </initial_timeout_minutes>
   </run_vm>
   </validation>
   ```
3. Enregistrez le fichier de configuration.
4. Redémarrez l'agent.
   - [Pour l'agent pour VMware ou pour Hyper-V s'exécutant sous Windows] Exécutez les commandes suivantes à l'invite de commandes :

     ```
     net stop mms
     ```

     ```
     net start mms
     ```
   - [Pour l'agent pour VMware (appliance virtuelle)] Redémarrez l'appliance virtuelle.

© Acronis International GmbH, 2003-2026

Configuration du nombre de nouvelles tentatives en cas d'erreur

Pour maximiser le nombre de validations réussies, vous pouvez configurer de nouvelles tentatives automatiques pour les validations qui aboutissent à une erreur.

Pour configurer des nouvelles tentatives automatiques

1. Lors de la création d'un plan de validation, cliquez sur l'icône en forme d'engrenage.
2. Dans le panneau **Options**, sélectionnez **Gestion erreurs**.
3. Dans **Réessayer si une erreur se produit**, cliquez sur **Oui**.
4. Dans **Nombre de tentatives**, configurez le nombre maximal de nouvelles tentatives en cas d'erreur.

   L'opération de validation est alors réexécutée jusqu'à ce qu'elle aboutisse sans erreur ou que le nombre maximal de nouvelles tentatives soit atteint.
5. Dans **Intervalle entre les tentatives**, configurez le délai entre deux nouvelles tentatives consécutives.
6. Cliquez sur **Terminé**.

Statut de validation

Un statut de validation est affecté aux sauvegardes pour lesquelles une validation a été effectuée.

Lorsqu'une validation est réussie, la sauvegarde est marquée d'un point vert et le libellé indique **Validé**.

Si la validation échoue, la sauvegarde est marquée d'un point rouge.

Le statut de la validation est mis à jour après chaque opération de validation. Le statut de chaque méthode de validation est mis à jour séparément. La validation échoue si l'une des méthodes de validation configurées échoue. Dans certains cas, une validation en échec peut être causée par une mauvaise configuration du plan de validation. Par exemple, si vous utilisez la méthode **Pouls de la MV** pour des machines virtuelles sur un hôte incorrect.

Remarque
Si l'une des méthodes de validation configurées échoue, le statut de la validation de la sauvegarde s'affiche comme échoué. Ce statut persiste, même si vous reconfigurez le plan de validation en désactivant la méthode en échec et que la validation via d'autres méthodes se termine avec succès. Pour le statut **Validé**, la méthode de validation en échec doit se terminer avec succès pour la même sauvegarde.

Vérification du statut de validation

Vous pouvez vérifier le statut de validation d'une sauvegarde dans les onglets **Terminaux** ou **Stockage de sauvegarde**.

© Acronis International GmbH, 2003-2026

Vous pouvez voir le statut de chaque méthode de validation et télécharger la capture d'écran lorsque la méthode de validation de capture d'écran est utilisée.

Pour vérifier le statut de validation

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez une ressource, puis cliquez sur **Restauration**.
3. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde.
4. Sélectionnez la sauvegarde pour laquelle vous souhaitez vérifier le statut de validation.

Stockage de sauvegarde

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de sauvegarde.
3. Sélectionnez l'archive de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
4. Sélectionnez la sauvegarde pour laquelle vous souhaitez vérifier le statut de validation.

Statut de l'activité de validation

Un plan de validation peut inclure plusieurs sauvegardes. Toutes les sauvegardes sont traitées séquentiellement, une par une, dans une seule activité de validation.

Un agent de protection ne peut exécuter qu'une activité de validation à la fois. Cela signifie que deux activités de validation simultanées nécessitent deux agents et trois activités simultanées nécessitent trois agents.

Le tableau suivant récapitule les statuts possibles de l'activité de validation.

Résultat de l'activité	Plan avec une sauvegarde	Plan avec plusieurs sauvegardes
Réussi	Toutes les méthodes de validation ont réussi	Toutes les méthodes de validation ont réussi dans toutes les sauvegardes
Succès avec avertissements	Sans Objet	Une méthode de validation au moins a échoué dans au moins une sauvegarde
Faire échouer	Une méthode de validation au moins a échoué	Une méthode de validation au moins a échoué dans toutes les sauvegardes

Création d'un plan de validation

Pour valider une archive de sauvegarde en tant qu'opération de traitement des données hors hôte, vous devez créer un plan de validation.

© Acronis International GmbH, 2003-2026

Un plan de validation peut inclure de nombreuses sauvegardes et une sauvegarde peut être validée par de nombreux plans de validation.

Pour créer un plan de validation

1. Dans la console Cyber Protect, accédez à **Gestion** > **Validation**.
2. Cliquez sur **Création d'un plan**.
3. [Facultatif] Pour modifier le nom du plan, cliquez sur le nom par défaut, puis spécifiez un nouveau nom.
4. Dans **Agent**, sélectionnez l'agent qui exécutera la validation, puis cliquez sur **OK**.
   - Si vous souhaitez effectuer une validation en exécutant une machine virtuelle depuis une sauvegarde, sélectionnez un ordinateur avec l'agent pour VMware ou l'agent pour Hyper-V.
   - Si vous ne souhaitez pas effectuer de validation en exécutant une machine virtuelle à partir d'une sauvegarde, sélectionnez n'importe quelle ordinateur ayant accès à l'emplacement de sauvegarde.
5. Dans **Éléments à valider**, sélectionnez les archives de sauvegarde que vous souhaitez valider.
   a. Sélectionnez le champ d'application de la validation (archives de sauvegarde ou emplacements de sauvegarde) en cliquant sur **Sauvegardes** ou **Emplacements** dans le coin supérieur droit.
      Si les archives sélectionnées sont chiffrées, elles doivent toutes utiliser le même mot de passe de chiffrement. Pour les archives qui utilisent des mots de passe de chiffrement différents, créez des plans séparés.
   b. Cliquez sur **Ajouter**.
   c. En fonction du champ d'application de la validation, sélectionnez un ou plusieurs emplacements, ou un emplacement et une ou plusieurs archives de sauvegarde, puis cliquez sur **Terminé**.
   d. Cliquez sur **Terminé**.
6. Dans **Que valider**, sélectionnez les sauvegardes (connues également sous le nom de points de restauration) dans les archives sélectionnées à valider. Les options suivantes sont disponibles :
   - **Toutes les sauvegardes**
   - **Dernière sauvegarde uniquement**
7. Dans **Comment valider**, sélectionnez la méthode de validation.
   Vous pouvez sélectionner une des options suivantes, ou les deux :
   - **Vérification de la somme de contrôle**
   - **Exécuter en tant que machine virtuelle**
     L'option **Exécuter en tant que machine virtuelle** fournit les méthodes **Pouls de la MV** et **Validation de capture d'écran**. Pour plus d'informations, voir "Méthodes de validation" (p. 259).
8. [Si vous avez sélectionné **Vérification de la somme de contrôle**] Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

9. [Si vous avez sélectionné **Exécuter en tant que machine virtuelle**]. Configurez les paramètres de cette option.
   a. Dans **Machine cible**, sélectionnez le type de machine virtuelle (ESXi ou Hyper-V), l'hôte et le modèle de nom de l'ordinateur, puis cliquez sur **OK**.
      Par défaut, le nom est **[Nom de la Machine]_validate**.
   b. Dans **Magasin de données** (pour ESXi) ou **Chemin d'accès** (pour Hyper-V), sélectionnez le magasin de données pour la machine virtuelle.
   c. Sélectionnez une méthode de validation, ou les deux :
      - **Pouls de la MV**
      - **Validation de l'instantané**
   d. [Facultatif] Cliquez sur **Paramètres de MV** pour modifier la taille de la mémoire et les connexions réseau de la machine virtuelle.
      Par défaut, la machine virtuelle n'est pas connectée à un réseau et la taille de la mémoire de la machine virtuelle est équivalente à celle de la machine d'origine.
   e. Cliquez sur **Terminé**.
10. [Facultatif] Dans le plan de validation, cliquez sur **Planification**, puis configurez la planification.
11. [Si les archives sélectionnées dans **Éléments à valider** sont chiffrées] Activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement.
12. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
13. Cliquez sur **Créer**.

En conséquence, le plan de validation est créé et s'exécutera selon la planification que vous avez configurée. Pour exécuter le plan immédiatement, sélectionnez-le dans **Gestion** > **Validation**, puis cliquez sur **Exécuter maintenant**. Après le démarrage de la validation, vous pouvez vérifier l'activité en cours et accéder à ses détails dans la console Cyber Protect, sous **Surveillance** > **Activités**.

Nettoyage

Le nettoyage est une opération qui supprime les sauvegardes obsolètes conformément aux règles de conservation. Cette opération ne s'applique qu'aux agents et aux ressources, et non aux sauvegardes cloud à cloud (qui ne peuvent être supprimées que manuellement).

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

Emplacements pris en charge

Les plans de nettoyage prennent en charge tous les emplacements de sauvegarde, sauf les dossiers NFS et Secure Zone.

Pour créer un plan de nettoyage

© Acronis International GmbH, 2003-2026

1. Dans la Cyber Protect console, cliquez sur **Gestion** > **Nettoyage**.
2. Cliquez sur **Création d'un plan**.
3. Dans **Agent**, sélectionnez l'agent qui effectuera le nettoyage.
   Vous pouvez sélectionner n'importe quel agent ayant accès à l'emplacement de sauvegarde.
4. Dans **Éléments à nettoyer**, sélectionnez les archives ou les emplacements de sauvegarde à nettoyer.
   Pour naviguer entre les archives et les emplacements, utilisez le commutateur **Emplacements** / **Sauvegardes** dans le coin supérieur droit.
   Si vous sélectionnez plusieurs archives chiffrées, leur mot de passe de cryptage doit être identique. Pour les archives qui utilisent des mots de passe de cryptage différents, créez des plans distincts.
5. Dans **Planification**, configurez la planification de nettoyage.
6. Dans **Règles de rétention**, indiquez les règles de rétention.
   Les options suivantes sont disponibles :
   - **Par nombre de sauvegardes**
   - **Par âge des sauvegardes** (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires)
   - **Par volume total de sauvegardes**
7. [Si vous avez sélectionné des archives cryptées dans les **Éléments à répliquer**] Activez le commutateur **Mot de passe de sauvegarde**, puis fournissez le mot de passe de chiffrement.
8. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône engrenage, puis configurez les options selon vos besoins.
9. Cliquez sur **Créer**.

Conversion en une machine virtuelle

La conversion en une machine virtuelle n'est disponible que pour les sauvegardes de lecteur. Si une sauvegarde inclut un volume système et contient toutes les informations nécessaires au démarrage du système d'exploitation, la machine virtuelle résultante peut démarrer par elle-même. Sinon, vous pouvez ajouter ses disques virtuels sur une autre machine virtuelle.

Remarque
Les machines virtuelles répliquées via la fonctionnalité native de réplication de machines virtuelles de Scale Computing ne peuvent pas être sauvegardées.

Vous pouvez créer un plan séparé pour la conversion vers une machine virtuelle et exécuter ce plan manuellement ou selon un calendrier.

Pour en savoir plus sur les prérequis et les limitations, reportez-vous à "Ce que vous devez savoir à propos de la conversion" (p. 269).

© Acronis International GmbH, 2003-2026

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

Pour créer un plan de conversion en une machine virtuelle

1. Cliquez sur **Gestion** > **Conversion en MV**.
2. Cliquez sur **Création d'un plan**.
   Le logiciel affiche un nouveau modèle de plan.
3. [Facultatif] Pour modifier le nom du plan, cliquez sur le nom par défaut.
4. Dans **Convertir en**, sélectionnez le type de machine virtuelle cible. **Vous pouvez sélectionner l'une des options suivantes** :
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **Fichiers VHDX**

   Remarque
   Pour économiser de l'espace, chaque conversion en fichiers VHDX ou VMware Workstation écrase les fichiers VHDX/VMDK situés dans l'emplacement cible et qui ont été créés lors de la conversion précédente.
5. Effectuez l'une des actions suivantes :
   - [Pour VMware ESXi, Hyper-V et Scale Computing HC3] Cliquez sur **Hôte**, sélectionnez l'hôte cible et spécifiez le nouveau modèle de nom de machine.
   - [Pour d'autres types de machines virtuelles] Dans **Chemin d'accès**, spécifiez où enregistrer les fichiers de la machine virtuelle et le modèle de nom de machine.

   Par défaut, le nom est **[Nom de la Machine]_converted**.
6. Cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera la conversion.
7. Cliquez sur **Éléments à convertir**, puis sélectionnez les sauvegardes que ce plan devra convertir en machines virtuelles.
   Vous pouvez passer de la sélection de sauvegardes à la sélection d'emplacements entiers, et vice-versa, à l'aide de l'option **Emplacements**/**Sauvegardes** dans l'angle supérieur droit.
   Si les sauvegardes sélectionnées sont chiffrées, elles doivent toutes utiliser le même mot de passe de chiffrement. Pour les sauvegardes qui utilisent différents mots de passe de chiffrement, créez des plans séparés.
8. [Uniquement pour VMware ESXi et Hyper-V] Cliquez sur **Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V, puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.

© Acronis International GmbH, 2003-2026

9. [Uniquement pour VMware ESXi et Hyper-V] Sélectionnez le mode de provisionnement du disque. Le paramètre par défaut est **Dynamique** pour VMware ESXi et **En expansion dynamique** pour Hyper-V.
10. [Facultatif] [Pour VMware ESXi, Hyper-V et Scale Computing HC3] Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs ou les connexions réseau de la machine virtuelle.
11. [Facultatif] Cliquez sur **Planification**, puis modifiez la planification.
12. Si les sauvegardes sélectionnées dans **Éléments à convertir** sont chiffrées, activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement. Sinon, ignorez cette étape.
13. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
14. Cliquez sur **Créer**.

Ce que vous devez savoir à propos de la conversion

Types de machine virtuelle pris en charge

Il est possible d'effectuer la conversion d'une sauvegarde sur une machine virtuelle via le même agent que celui qui a créé la sauvegarde, ou via un autre agent.

Pour effectuer une conversion vers VMware ESXi, Hyper-V ou Scale Computing HC3, vous avez besoin respectivement d'un hôte ESXi, Hyper-V ou HC3 de Scale Computing et d'un agent de protection (agent pour VMware, agent pour Hyper-V ou agent pour Scale Computing HC3) qui gère cet hôte.

La conversion vers des fichiers VHDX présuppose que les fichiers seront connectés en tant que disques virtuels à une machine virtuelle Hyper-V.

Le tableau suivant résume les types de machines virtuelles que vous pouvez créer avec l'opération **Convertir en MV**. Les lignes dans le tableau montrent le type des machines virtuelles converties. Les colonnes montrent les agents qui effectuent la conversion.

Type de MV	Agent pour VMware	Agent pour Hyper-V	Agent pour Windows	Agent pour Linux	Agent pour Mac	Agent pour Scale Computing HC3	Agent pour oVirt (KVM)	Agent pour Virtuozzo Hybrid Infrastructure	Agent pour Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-	–	+	–	–	–	–	–	–	–

© Acronis International GmbH, 2003-2026

V									
VMware Workstation	+	+	+	+	–	–	–	–	–
Fichiers VHDX	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

Limites

- Les sauvegardes stockées sur NFS ne peuvent pas être converties.
- Les sauvegardes stockées dans Secure Zone ne peuvent être converties que par l'agent exécuté sur le même ordinateur.
- Les sauvegardes qui contiennent des volumes logiques Linux (LVM) ne peuvent être converties que si elles ont été créées par l'agent pour VMware, l'agent pour Hyper-V ou l'agent pour Scale Computing HC3, et sont dirigées vers le même hyperviseur. La conversion entre superviseurs n'est pas prise en charge.
- Quand les sauvegardes d'une machine Windows sont converties vers des fichiers VMware Workstation ou VHDX, la machine virtuelle résultante hérite du type de processeur de la machine qui exécute la conversion. En conséquence, les pilotes de processeur correspondants sont installés sur le système d'exploitation invité. S'il est démarré sur un hôte ayant un type de processeur différent, le système invité affiche une erreur de pilote. Mettez à jour ce lecteur manuellement.

Conversion régulière en machine virtuelle ou exécution d'une machine virtuelle depuis une sauvegarde

Les deux opérations vous permettent d'avoir une machine virtuelle qui peut démarrer en quelques secondes si la machine d'origine échoue.

Une conversion régulière en machine virtuelle consomme des ressources de CPU et de mémoire. Les fichiers de la machine virtuelle occupent constamment de l'espace sur le magasin de données (stockage). Cela n'est pas pratique si un hôte de production est utilisé pour la conversion. Cependant, les performances de la machine virtuelle sont limitées uniquement par les ressources de l'hôte.

L'exécution d'une machine virtuelle depuis une sauvegarde consomme des ressources uniquement quand la machine virtuelle est en cours d'exécution. Seule la conservation des modifications des disques virtuels nécessite de l'espace dans le magasin de données (stockage). Cependant, la machine virtuelle peut être plus lente, car l'hôte n'accède pas directement aux disques virtuels, mais

© Acronis International GmbH, 2003-2026

communique avec l'agent qui lit les données de la sauvegarde. De plus, la machine virtuelle est temporaire.

Fonctionnement de la conversion régulière vers une machine virtuelle

La façon dont la conversion régulière fonctionne dépend de l'endroit que vous choisissez pour créer la machine virtuelle.

- **Si vous choisissez d'enregistrer la machine virtuelle comme un ensemble de fichiers :** chaque conversion recrée la machine virtuelle à partir de zéro.
- **Si vous choisissez de créer la machine virtuelle sur un serveur de virtualisation** : lors de la conversion d'une sauvegarde incrémentielle ou différentielle, le logiciel met à jour la machine virtuelle existante de manière incrémentielle au lieu de la recréer. Cette conversion est normalement plus rapide. Elle réduit le trafic réseau et l'utilisation des ressources du CPU de l'hôte qui exécute la conversion. Si la mise à jour de la machine virtuelle n'est pas possible, le logiciel la crée de nouveau à partir de rien.

Voici une description détaillée de ces deux cas.

Si vous choisissez d'enregistrer la machine virtuelle comme un ensemble de fichiers

Suite à la première conversion, une nouvelle machine virtuelle sera créée. Toutes les conversions suivantes vont créer cette machine à nouveau. Premièrement, l'ancienne machine est temporairement renommée. Puis, une nouvelle machine virtuelle est créée avec le nom précédent de l'ancienne machine. Si cette opération réussi, l'ancienne machine est supprimée. Si cette opération échoue, la nouvelle machine est supprimée et l'ancienne machine reprend son nom précédent. De cette façon, la conversion finit toujours avec une seule machine. Toutefois, de l'espace de stockage supplémentaire est requis pendant la conversion pour stocker l'ancienne machine.

Si vous choisissez de créer la machine virtuelle sur un serveur de virtualisation

La première conversion crée une nouvelle machine virtuelle. Toute conversion ultérieure fonctionne comme suit :

- Si une *sauvegarde complète* a été réalisée depuis la dernière conversion, la machine virtuelle est créée de nouveau à partir de zéro, comme décrit plus haut dans cette section.
- Sinon, la machine virtuelle existante est mise à jour pour refléter les changements depuis la dernière conversion. Si mise à jour n'est pas possible (par exemple, si vous avez supprimé les instantanés intermédiaires, voir ci-dessous), la machine virtuelle est créée de zéro à partir de rien.

Instantanés intermédiaires

Pour être en mesure de mettre à jour la machine virtuelle convertie de façon sécurisée, le logiciel stocke un instantané intermédiaire d'hyperviseur de celle-ci. Cet instantané est appelé **Réplica...** et doit être conservé.

© Acronis International GmbH, 2003-2026

L'instantané **Réplica...** correspond au résultat de la dernière conversion. Vous pouvez utiliser cet instantané si vous voulez ramener la machine à cet état ; par exemple, si vous avez travaillé avec la machine et que vous voulez supprimer les modifications apportées.

Pour les machines virtuelles Scale Computing HC3 converties, un **Instantané utilitaire** est créé. Seul le service Cyber Protection l'utilise.

Plan d'analyse des sauvegardes

Pour analyser des sauvegardes à la recherche de malwares (y compris les ransomware), créez un plan d'analyse de sauvegarde.

Important
Les plans d'analyse des sauvegardes ne sont pas pris en charge pour tous les stockages des sauvegardes et les ressources. Pour plus d'informations, voir "Limites" (p. 1218).

Créer un plan d'analyse de sauvegarde

1. Dans la console Cyber Protect, accédez à **Gestion** > **Analyse de la sauvegarde**.
2. Dans le volet **Actions**, cliquez sur **Créer un plan**.
3. [Facultatif] Modifiez le nom du plan par défaut.
4. Dans **Sauvegardes à analyser**, cliquez sur **Spécifier**.
   a. Pour ajouter un nouvel emplacement au plan, cliquez sur **Ajouter**, sélectionnez un emplacement, puis cliquez sur **Terminé**.
   b. Cliquez sur **Emplacements** ou **Sauvegardes** pour sélectionner l'étendue du plan.
   c. Sélectionnez l'emplacement entier ou des archives dans un emplacement.
      Vous pouvez sélectionner un ou plusieurs volumes.
   d. Cliquez sur **Terminé**.
5. [Si les archives sélectionnées sont chiffrées] Dans **Chiffrement**, activez le bouton bascule, puis spécifiez le mot de passe de chiffrement.
   Le mot de passe que vous avez spécifié sera utilisé pour l'analyse de toutes les sauvegardes du plan, de sorte que toutes les archives sélectionnées doivent utiliser le même mot de passe de chiffrement. Pour les archives qui utilisent des mots de passe de chiffrement différents, créez des plans distincts.
6. Cliquez sur **Créer**.

Un plan de recherche de sauvegarde est créé. L'agent cloud analyse automatiquement les archives sélectionnées une fois par heure. Vous ne pouvez pas modifier la planification du plan ni la période entre deux analyses consécutives.

© Acronis International GmbH, 2003-2026

Plans de sauvegarde pour les applications dans le Cloud

L'onglet **Gestion** > **Sauvegarde d'applications dans le Cloud** affiche les plans de sauvegarde cloud à cloud. Ces plans sauvegardent les applications qui s'exécutent au moyen d'agents qui s'exécutent eux-mêmes dans le Cloud, et utilisent l'espace de stockage dans le Cloud en tant qu'emplacement de sauvegarde.

Dans cette section, vous pouvez exécuter les opérations suivantes :

- Créer, afficher, exécuter, stopper, modifier et supprimer un plan de sauvegarde
- Afficher les activités associées à chaque plan de sauvegarde
- Afficher les alertes associées à chaque plan de sauvegarde

Pour en savoir plus sur la sauvegarde d'applications Cloud, consultez les sections suivantes :

- Protection des données Microsoft 365
- Protection des données Google Workspace

Exécution manuelle de sauvegardes de cloud à cloud

Pour éviter l'interruption du service Cyber Protection, le nombre d'exécutions de sauvegardes Cloud à Cloud est limité à 10 par heure et par organisation Microsoft 365 ou Google Workspace. Après avoir atteint ce nombre, le nombre d'exécutions autorisé est réinitialisé à un par heure, puis une exécution supplémentaire est alors disponible chaque heure par la suite (par exemple heure 1, 10 exécutions ; heure 2, 1 exécution ; heure 3, 2 exécutions) jusqu'à ce qu'un total de 10 exécutions par heure soit atteint.

Les plans de sauvegarde appliqués aux groupes de terminaux (boîtes aux lettres, Drive, sites) ou contenant plus de 10 terminaux ne peuvent pas être exécutés manuellement.

Protection des applications de collaboration et de communication

Zoom, Cisco Webex Meetings, Citrix Workspace et Microsoft Teams sont désormais largement utilisés pour les communications et conférences Web et vidéo. Le service Cyber Protection vous permet de protéger vos outils de collaboration.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La configuration de la protection pour Zoom, Cisco Webex Meetings, Citrix Workspace et Microsoft Teams est similaire. Dans l'exemple ci-dessous, nous évoquerons la configuration de Zoom.

Pour configurer la protection pour Zoom

© Acronis International GmbH, 2003-2026

1. Installez l'agent de protection sur la machine sur laquelle l'application de collaboration est installée.
2. Connectez-vous à la console Cyber Protect et appliquez un plan de protection dans lequel l'un des modules suivants est activé :
   - **Protection contre les virus et les malwares** (avec les paramètres **Autoprotection** et **Active Protection** activés) – si vous possédez l'une des éditions Cyber Protect.
   - **Active Protection** (avec le paramètre **Autoprotection** activé) – si vous possédez l'une des éditions Cyber Backup.
3. [Facultatif] Pour l'installation automatique des mises à jour, configurez le module de **Gestion des correctifs** du plan de protection.

Par conséquent, votre application Zoom bénéficiera d'une protection qui inclut les activités suivantes :

- Installation automatique des mises à jour client de Zoom
- Protection des processus de Zoom contre les injections de code
- Protection contre des opérations suspectes par des processus de Zoom
- Protection des fichiers « hôtes » contre l'ajout de domaines liés à Zoom

Plans de transfert SIEM

Important
Cette option est uniquement disponible pour les administrateurs partenaires ayant accès à la Cyberprotection.

Les plates-formes SIEM (Security Information and Event Management) sont des solutions de cybersécurité qui fournissent une gestion centralisée des journaux, offrent une détection des menaces en temps réel, facilitent les enquêtes sur les incidents et aident les organisations à répondre aux exigences de conformité. Elles fonctionnent en consolidant et en analysant les données de sécurité, telles que les journaux des pare-feu, des systèmes de détection d'intrusion, des serveurs et des applications. Cela se fait en temps réel, pour générer des alertes prioritaires pour toute activité suspecte et menace potentielle. Les équipes de sécurité utilisent ensuite les données consolidées et les alertes pour enquêter sur les incidents de cybersécurité signalés, comprendre leur champ d'application et prendre des mesures en temps opportun pour contenir et atténuer les menaces.

Les plates-formes SIEM fournissent une vue d'ensemble de la posture de sécurité d'une organisation, permettant une détection précoce des menaces avancées et des anomalies. Elles aident les organisations à respecter les normes de conformité en matière de sécurité réglementaire et spécifique à l'industrie, en fournissant des données centralisées et du reporting. Elles offrent une console centralisée pour la gestion des événements de sécurité, offrant une meilleure visibilité dans le centre des opérations de sécurité (SOC).

© Acronis International GmbH, 2003-2026

Avec les plans de transfert SIEM Acronis, vous désignez un terminal protégé pour chaque client participant. L'agent Acronis sur ce terminal agit comme terminal d'écriture SIEM. Il écrit les informations d'alerte, d'événement, de tâche, d'activité et de journal d'audit dans un dossier sur le terminal. Ces données peuvent ensuite être transférées vers la plate-forme SIEM pour traitement.

Important
Les exigences de conformité réglementaire imposent que le client dispose de lacs de données SIEM individuels. En utilisant l'agent Acronis pour écrire les données SIEM sur un terminal protégé du client, la conformité est atteinte. Cela signifie que chaque client SIEM doit avoir un plan de transfert SIEM individuel.
Vous pouvez créer des plans de transfert SIEM individuels pour un client spécifique, et vous pouvez également créer un plan SIEM générique pour plusieurs clients, et choisir un terminal protégé Acronis pour chaque client afin d'agir comme terminal d'écriture et de stockage des données.

Installation de la fonctionnalité SIEM

Pour qu'un terminal soit utilisé comme terminal d'écriture SIEM, il doit avoir la fonctionnalité SIEM installée sur l'agent Acronis.

Cela peut être fait soit manuellement, via l'interface graphique standard d'installation de l'agent Acronis, soit sans surveillance, lorsqu'un plan de transfert SIEM est appliqué au terminal.

Installation de la fonctionnalité SIEM à l'aide de l'interface graphique

Vous pouvez installer la fonctionnalité SIEM sur votre terminal d'écriture SIEM à l'aide de l'interface graphique d'installation de l'agent Acronis.

Important
Vous devez explicitement demander la fonctionnalité SIEM Log Forwarder pendant l'installation.

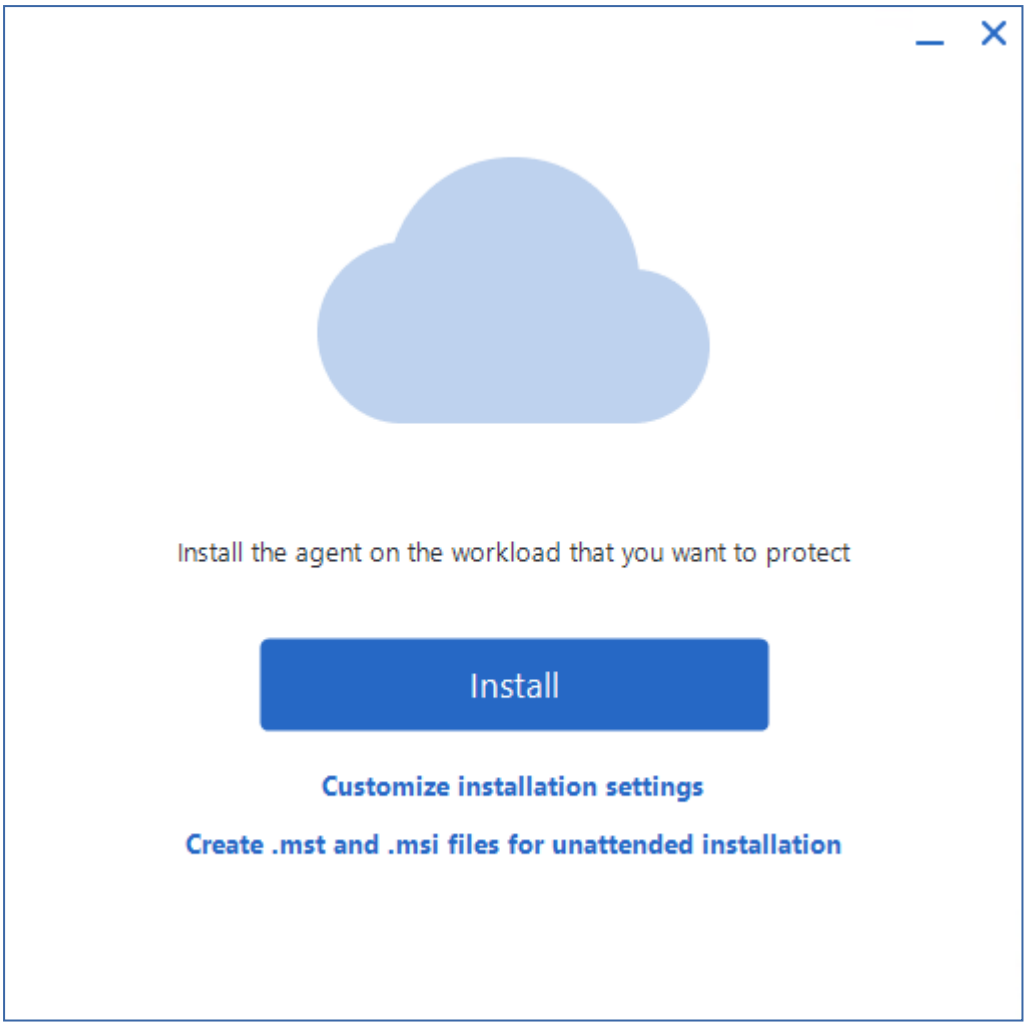
Prérequis

Lisez les instructions trouvées dans "Installation des agents de protection à l'aide de l'interface utilisateur graphique" (p. 64).

Pour installer la fonctionnalité SIEM à l'aide de l'interface graphique

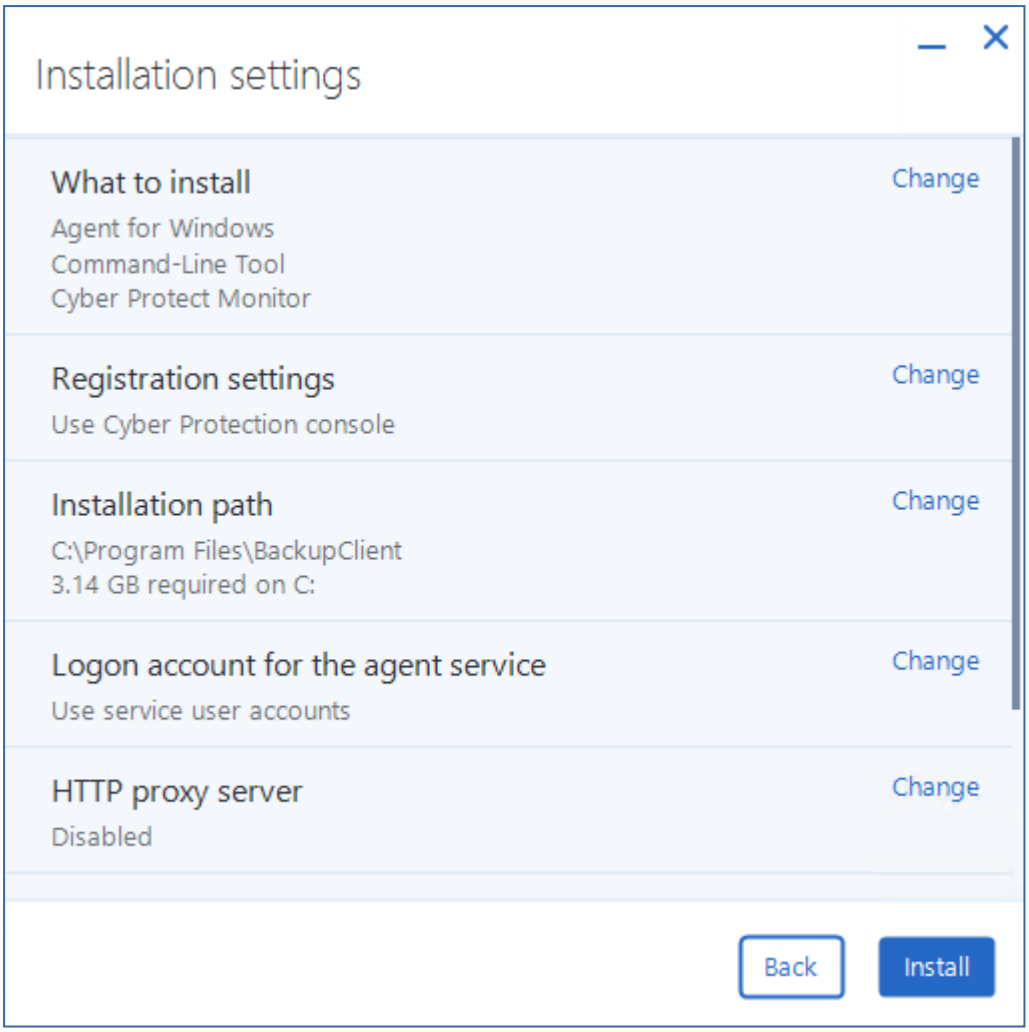
1. Exécutez le fichier d'installation.
   L'écran initial d'installation apparaît.

© Acronis International GmbH, 2003-2026



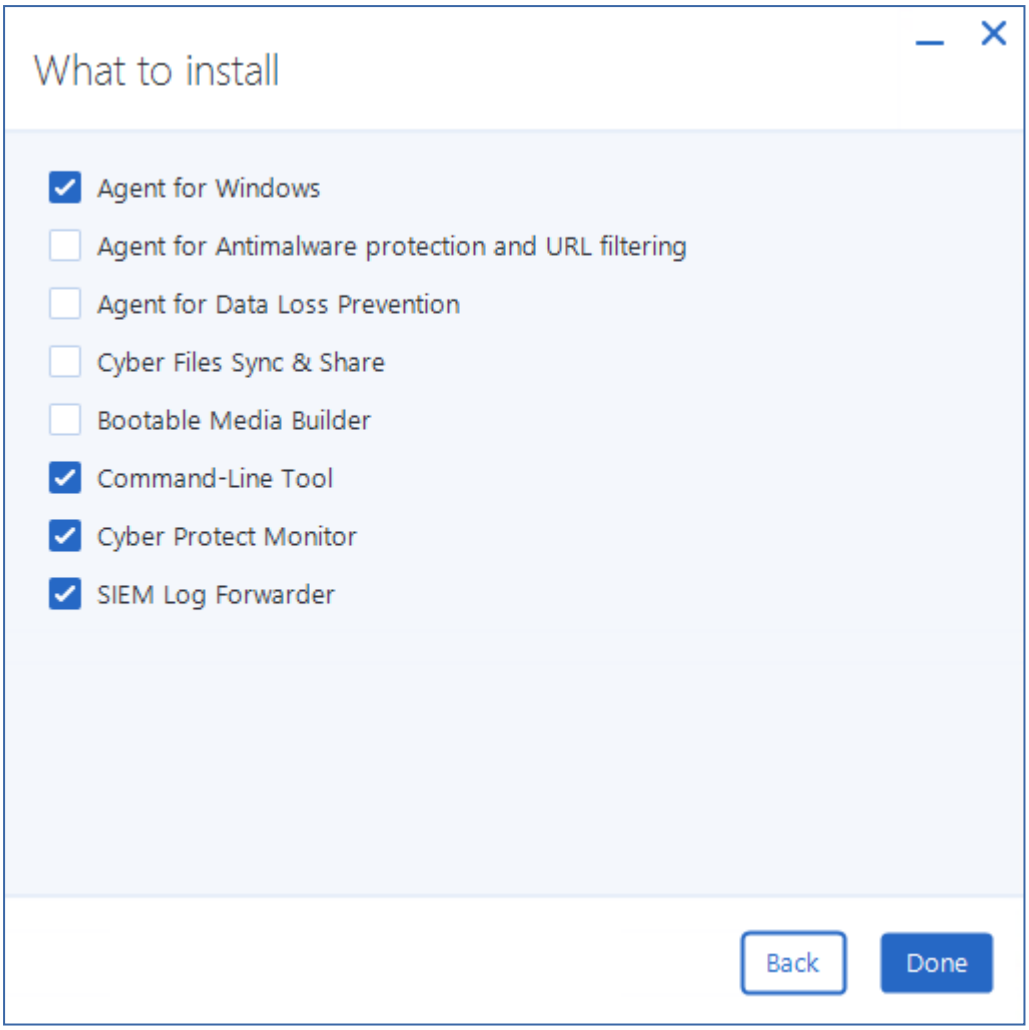
2. Cliquez sur **Personnaliser les paramètres d'installation**.
   L'écran **Paramètres d'installation** apparaît.

© Acronis International GmbH, 2003-2026



3. Cliquez sur **Changer** pour spécifier **Ce qu'il faut installer**.
   L'écran **Ce qu'il faut installer** apparaît.
4. Assurez-vous de sélectionner la case à cocher **SIEM Log Forwarder**.

© Acronis International GmbH, 2003-2026

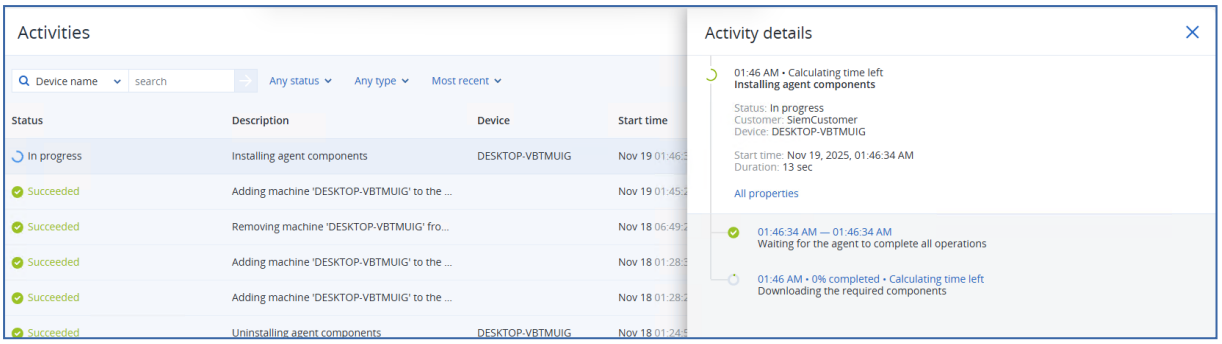


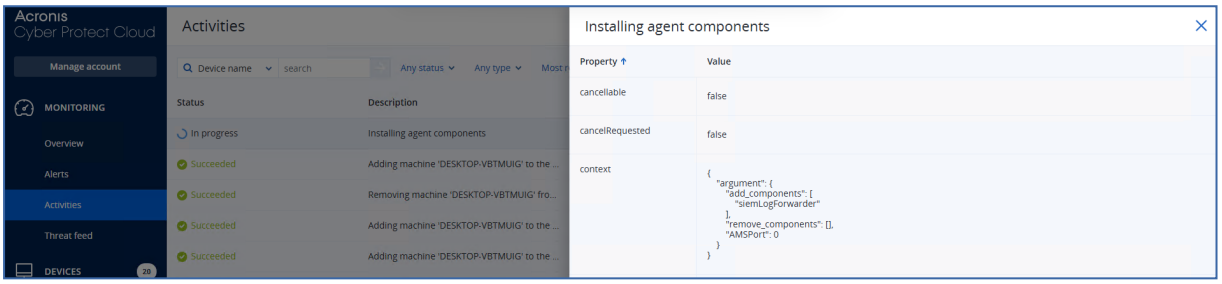
5. Cliquez sur **Terminé**.
6. [Facultatif] Apportez d'autres modifications nécessaires aux paramètres d'installation.
   Pour plus d'informations, voir "Installation des agents de protection à l'aide de l'interface utilisateur graphique" (p. 64).
7. Cliquez sur **Installer** pour installer l' agent Acronis avec la fonctionnalité de transfert de journal SIEM activée.

Installation de la fonctionnalité SIEM sans surveillance

Avec l'installation de la fonctionnalité SIEM sans surveillance, l'installation de la fonctionnalité est déclenchée lorsqu'un plan de transfert SIEM est appliqué au terminal.

© Acronis International GmbH, 2003-2026





Listes de plans de transfert SIEM

Il existe des listes de plans de transfert SIEM à votre niveau de partenaire et à vos niveaux de client.

Au niveau du partenaire, la liste des plans de transfert SIEM fournit un résumé de tous les plans de transfert SIEM que vous avez implémentés pour les clients. La liste des plans de transfert SIEM au niveau du partenaire affiche les détails suivants :

- **Nom**
  Le nom du plan de transfert SIEM.
- **Méthode**
  Indique si le plan de transfert SIEM utilise les fichiers ou la méthode du serveur syslog. Pour plus d'informations, voir "Méthodes de transfert SIEM" (p. 286).
- **Clients**
  Le client ou les clients utilisant le plan.
- **Données**
  Les données Acronis transmises dans le cadre du plan de transfert SIEM.

Chaque client ne peut avoir qu'un seul plan de transfert SIEM. Par conséquent, au niveau du client, la liste des plans de transfert SIEM est soit vide (parce que vous n'avez pas créé de plan pour eux) soit contient une seule entrée, affichant les détails suivants :

- **Nom**
  Le nom du plan de transfert SIEM.
- **Méthode**
  Indique si le plan de transfert SIEM utilise les fichiers ou la méthode du serveur syslog. Pour plus d'informations, voir "Méthodes de transfert SIEM" (p. 286).
- **Terminal d'écriture**

© Acronis International GmbH, 2003-2026

Le terminal utilisé pour écrire et stocker les données SIEM Acronis.

- **Données**

  Les données Acronis transmises dans le cadre du plan de transfert SIEM.

Pour ouvrir une liste de plans de transfert SIEM

1. Ouvrez la console Protection soit au niveau du partenaire, soit au niveau d'un client.
2. Sélectionnez **Gestion** dans le menu principal.
3. Sélectionnez **plans de transfert SIEM** dans le sous-menu.

Créer un plan de transfert SIEM pour plusieurs clients

Pour gagner du temps, vous pouvez créer un seul plan de transfert SIEM générique et l'appliquer à plusieurs clients. Lorsque vous faites cela, vous devez choisir un terminal protégé Acronis pour chaque client participant pour agir en tant que terminal d'écriture et stocker les données.

Pour créer un plan de transfert SIEM générique pour plusieurs clients

1. Ouvrez votre liste de plans de transfert SIEM partenaire.
2. Cliquez sur **Créer**.
3. [Facultatif] Changez le nom par défaut du plan.
   a. Cliquez sur l'icône en forme de crayon.
   b. Modifier le nom.
   c. Cliquez sur la coche pour accepter les modifications.
4. Sélectionnez **Méthode** pour le plan de transfert SIEM :
   - **Fichiers**

     Cette méthode peut utiliser un terminal Windows ou un terminal Linux comme terminal d'écriture.
   - **Serveur Syslog**

     Cette méthode ne peut utiliser qu'un terminal Linux comme terminal d'écriture.

   Pour plus d'informations, voir méthodes de plan de transfert SIEM.
5. ***Méthode des fichiers***
   a. Cliquez sur le champ **Client**.

      Une liste de tous vos clients apparaît. Chaque client a une liste déroulante correspondante de tous leurs terminaux protégés Windows et Linux.

      Pour apparaître dans la liste déroulante, un terminal doit avoir l'agent Acronis installé et doit être en ligne.
   b. Dans les listes déroulantes, sélectionnez un terminal d'écriture pour chaque client pour lequel vous souhaitez utiliser le nouveau plan de transfert SIEM.

© Acronis International GmbH, 2003-2026

Important
Le terminal d'écriture doit rester en ligne en permanence pour que le plan de transfert SIEM fonctionne correctement.

Les clients pour lesquels vous ne spécifiez pas de terminal d'écriture n'utiliseront pas le nouveau plan de transfert SIEM.

c. Cliquez sur **Terminé**.

d. [Facultatif] Cliquez sur **Spécifier** pour changer les valeurs par défaut du **Chemin d'accès au fichier** pour stocker des données SIEM sur les terminaux d'écriture, puis cliquez sur **Terminé**.

Important
Si le répertoire spécifié est supprimé d'un des terminaux de transfert SIEM, le transfert SIEM s'arrête jusqu'à ce que vous restauriez le répertoire supprimé ou modifiiez le **Chemin d'accès au fichier** vers un répertoire valide.

Méthode du serveur Syslog

a. Cliquez sur le champ **Client**.

Une liste de tous vos clients apparaît. Chaque client a une liste déroulante correspondante de tous leurs terminaux protégés Linux.

Pour apparaître dans la liste déroulante, un terminal doit avoir l'agent Acronis installé et doit être en ligne.

b. Dans les listes déroulantes, sélectionnez un terminal d'écriture pour chaque client pour lequel vous souhaitez utiliser le nouveau plan de transfert SIEM.

Important
Le terminal d'écriture doit rester en ligne en permanence pour que le plan de transfert SIEM fonctionne correctement.

Les clients pour lesquels vous ne spécifiez pas de terminal d'écriture n'utiliseront pas le nouveau plan de transfert SIEM.

c. Cliquez sur **Terminé**.

6. [Facultatif] Changez le **Format du fichier**.
   - **CEF** (par défaut)

     Format standardisé, neutre vis-à-vis des fournisseurs, conçu pour les événements de sécurité et l'analyse détaillée des événements.
   - **JSON**

     Format hautement flexible, qui permet des données personnalisées et complexes. Idéal pour les plate-formes modernes de gestion des journaux.

   Pour plus d'informations, voir "Format et exemples de données SIEM" (p. 286).
7. [Facultatif] Sélectionnez les types de données Acronis à inclure dans le plan de transfert SIEM.

© Acronis International GmbH, 2003-2026

Par défaut, tous les types de données Acronis disponibles sont inclus.

a. Cliquez sur le champ **Données**.

b. Décochez les cases correspondant aux types de données Acronis que vous ne souhaitez pas inclure dans le plan de transfert SIEM. Les types de données Acronis sont :

- **Alertes**

  Mises à jour des messages critiques ou d'erreur nécessitant une réponse rapide.
- **Événements**

  Données de journal d'événements avec des informations sur les performances du système et les interactions de l'utilisateur.
- **Activités**

  Tous les messages de succès, d'information, d'avertissement, critiques et d'erreur (par exemple, DLP, filtrage d'URL, sauvegardes).
- **Journal d'audit**

  Événements internes pertinents pour la sécurité qui peuvent affecter la fiabilité et l'intégrité de l'organisation.

  Remarque
  Les données du journal d'audit peuvent être stockées pour des raisons de conformité HIPAA si vous utilisez la méthode **Fichiers**.

c. Cliquez sur **Terminé**.

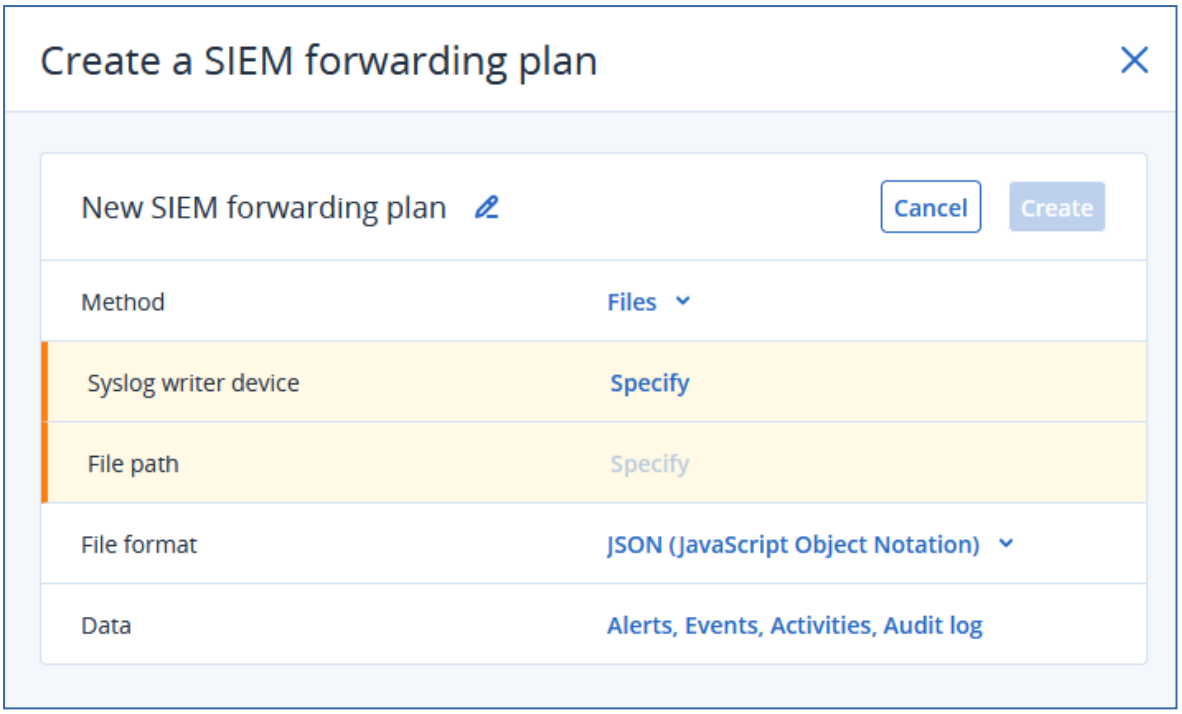
8. Une fois terminé, cliquez sur **Créer**.

Création d'un plan SIEM pour un client individuel

Pour créer un plan pour un client individuel

1. Ouvrez la console Acronis Protection pour le client.
2. Sélectionnez **Gestion** dans le menu principal.
3. Sélectionnez les **plans de transfert SIEM**.
4. Cliquez sur **Créer**.

© Acronis International GmbH, 2003-2026



5. [Facultatif] Changez le nom par défaut du plan.
   a. Cliquez sur l'icône en forme de crayon.
   b. Modifier le nom.
   c. Cliquez sur la coche pour accepter les modifications.
6. Sélectionnez **Méthode** pour le plan de transfert SIEM :
   - **Fichiers**

     Cette méthode peut utiliser un terminal Windows ou un terminal Linux comme terminal d'écriture.
   - **Serveur Syslog**

     Cette méthode ne peut utiliser qu'un terminal Linux comme terminal d'écriture.

   Pour plus d'informations, voir méthodes de plan de transfert SIEM.
7. ***Méthode des fichiers***
   a. Cliquez sur **Spécifier** pour sélectionner le **Terminal d'écriture** dans la liste des terminaux Windows et Linux protégés disponibles, puis cliquez sur **Terminé**.

   Important
   Le terminal de transfert SIEM doit rester en ligne en permanence pour que le plan de transfert SIEM fonctionne correctement.

   b. [Facultatif] Cliquez sur **Spécifier** pour changer le **Chemin d'accès au fichier** par défaut pour stocker des données SIEM sur le terminal de l'écrivain, puis cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Important
Si le répertoire spécifié est supprimé, le transfert SIEM s'arrête jusqu'à ce que vous restauriez le répertoire supprimé ou modifiiez le **Chemin d'accès au fichier** vers un répertoire valide.

Méthode du serveur Syslog

a. Cliquez sur **Spécifier** pour sélectionner le **Terminal d'écriture** dans la liste des terminaux Linux disponibles et protégés, puis cliquez sur **Terminé**.

Important
Le terminal d'écriture doit rester en ligne en permanence pour que le plan de transfert SIEM fonctionne correctement.

b. Cliquez sur **Terminé**.

8. [Facultatif] Changez le **Format du fichier**.
   - **CEF** (par défaut)
     Format standardisé, neutre vis-à-vis des fournisseurs, conçu pour les événements de sécurité et l'analyse détaillée des événements.
   - **JSON**
     Format hautement flexible qui permet des données personnalisées et complexes. Idéal pour les plates-formes modernes de gestion des journaux.

   Pour plus d'informations, voir "Format et exemples de données SIEM" (p. 286).
9. [Facultatif] Sélectionnez les types de données Acronis à inclure dans le plan de transfert SIEM.
   Par défaut, tous les types de données Acronis disponibles sont inclus.
   a. Cliquez sur le champ **Données**.
   b. Décochez les cases des types de données Acronis que vous ne souhaitez pas inclure dans le plan de transfert SIEM.
      Les types de données Acronissont :
      - **Alertes**
        Mises à jour des messages critiques ou d'erreur nécessitant une réponse rapide.
      - **Événements**
        Données de journal d'événements avec des informations sur les performances du système et les interactions de l'utilisateur.
      - **Activités**
        Tous les messages de succès, d'information, d'avertissement, critiques et d'erreur (par exemple, DLP, filtrage d'URL, sauvegardes).
      - **Journal d'audit**
        Événements internes pertinents pour la sécurité qui peuvent affecter la fiabilité et l'intégrité de l'organisation.

© Acronis International GmbH, 2003-2026

Remarque
Les données de journal d'audit peuvent être stockées à des fins de conformité HIPAA.

c. Cliquez sur **Terminé**.

10. Cliquez sur **Créer**.

Renommer un plan de transfert SIEM

Renommer un plan de transfert vers un SIEM

1. Ouvrez votre liste de plans de transfert SIEM partenaire ou la liste spécifique au client.
2. Cliquez sur le plan que vous souhaitez renommer.
   L'encadré des détails et des actions s'ouvre.
3. Cliquez sur **Renommer**.
4. Modifier le nom du plan.
5. Cliquez sur **Renommer**.

Modification d'un plan de transfert SIEM

Remarque
Vous ne pouvez pas changer la **Méthode**. Pour la changer, vous devez supprimer le plan de transfert SIEM et en créer un nouveau.

Pour modifier un plan de transfert SIEM

1. Ouvrez votre liste de plans de transfert SIEM partenaire ou la liste spécifique au client.
2. Cliquez sur le plan que vous souhaitez modifier.
   L'encadré des détails et des actions s'ouvre.
3. Cliquez sur **Modifier**.
4. Apportez vos modifications et cliquez sur **Confirmer**.

Suppression du plan SIEM

Remarque
Lorsque vous supprimez un plan de transfert SIEM, le transfert de données cesse, mais les données qui ont déjà été transférées ne sont pas supprimées.

Supprimer un plan de transfert SIEM

1. Ouvrez votre liste de plans de transfert SIEM partenaire ou la liste spécifique au client.
2. Cliquez sur le plan que vous souhaitez supprimer.
   L'encadré des détails et des actions s'ouvre.

© Acronis International GmbH, 2003-2026

3. Cliquez sur **Supprimer**.
4. Sélectionnez la case de confirmation pour activer le bouton **Confirmer**.
5. Cliquez sur **Confirmer**.

Méthodes de transfert SIEM

Avec le transfert SIEM Acronis, l'agent Acronis écrit les données SIEM terminal d'écriture géré par Acronis. Il peut fonctionner avec l'une des deux méthodes de transfert :

- **Fichiers**
  Applicable avec un terminal d'écriture Windows ou Linux.
- **Syslog**
  Applicable uniquement avec un terminal d'écriture Linux.

Méthode de transfert des fichiers

Cette méthode peut être implémentée avec un terminal Windows ou Linux.

Les données SIEM sont écrites sous forme de fichiers dans un répertoire. Vous pouvez spécifier un répertoire ou accepter le répertoire par défaut.

Répertoires par défaut

- Terminal d'écriture Windows : `C:\`.
- Terminal d'écriture Linux : `/var/log/siem`.

Important
Seuls les administrateurs ont accès à ces fichiers.

Méthode de transfert via serveur syslog

Un serveur syslog est un système centralisé qui reçoit et stocke les messages de journal en utilisant le protocole Syslog.

Important
Seuls les terminaux Linux peuvent être utilisés pour cette méthode.

Pour examiner les données SIEM transférées

1. Exécutez : `cat /var/log/syslog`
2. Exécutez : `cat /var/log/messages`

Format et exemples de données SIEM

Les plans de transfert Acronis SIEM peuvent envoyer des données pour alertes Acronis, événements, activités, tâches et entrées de journal d'audit, avec l'un des deux formats de fichier :

© Acronis International GmbH, 2003-2026

JSON et CEF.

Les fichiers SIEM incluent différentes données avec des structures distinctes, selon le type de données et le format de fichier du plan de transfert. Dans cette section, nous fournissons des exemples de données pour les quatre types de données dans les deux formats.

Format de fichier CEF

- Exemples d'alerte
- Exemples d'événement
- Exemples d'activité
- Exemples de journal d'audit

Format de fichier JSON

- Exemples d'alerte
- Exemples d'événement
- Exemples d'activité
- Exemples de journal d'audit

Exemples d'alerte CEF


```
Oct 15 14:45:01 WIN-R1OR1V5M79O siem_log_forwarder[8608]:
CEF:0|Acronis|DemoCustomer|1.0|BackupStatusUnknown|BackupStatusUnknown|5|cs1=
{"agentId":"c8d66ac4-0d5b-4ecb-b1b0-c3649df91231","backupLocations":
[{"type":"cloud"}],"backupSourcesType":"files","errorMessage":{"kbLink":
{"serCode":"BackupStatusUnknown"}},"planId":"a92799fc-f657-4a10-b6ed-
16975c4d0ef0","planName":"Protect Win","resourceId":"3b9187d6-0853-45ff-aab0-
0c68cd643068","resourceName":"WIN-R1OR1V5M79O"} cs1Label=alertdetails
deviceExternalId=3b9187d6-0853-45ff-aab0-0c68cd643068 dvchost=WIN-R1OR1V5M79O Oct 15
14:42:46 WIN-R1OR1V5M79O siem_log_forwarder[8608]:
CEF:0|Acronis|DemoCustomer|1.0|BackupFailed|BackupFailed|10|cs1={"activité":
{"id":"FE0B2835-3C9D-4D5A-9D02-FD0CBE5042B8","type":"8F01AC13-F59E-4851-9204-
DE1FD77E36B4"},"activityId":"FE0B2835-3C9D-4D5A-9D02-
FD0CBE5042B8","backupLocations":
[{"nom":"","type":"cloud"}],"backupSourcesType":"machines","erreur":
{"code":20250646,"fields":{"$module":"service_process_vsa64_41100","AgentName":"WIN-
R1OR1V5M79O","CommandID":"8F01AC13-F59E-4851-9204-DE1FD77E36B4"},"src":
{"fichier":"c:\\\\b\\\\1223\\\\enterprise\\\\common\\\\tol\\\\command\\\\command.cpp
","func":"Tol::`anonymous-
namespace'::MakeFailResultWithName","line":503,"tag":"0x8d165e86fb8195c5"},"suberro
r":{"code":20250646,"fields":{"$module":"gtob_backup_command_addon_vsa64_
41100","AgentName":"WIN-R1OR1V5M79O","CommandID":"8F01AC13-F59E-4851-9204-
```


© Acronis International GmbH, 2003-2026

```
DE1FD77E36B4"},"src":
{"fichier":"c:\\\\b\\\\1223\\\\enterprise\\\\common\\\\tol\\\\command\\\\command.cpp
","func":"Tol::`anonymous-
namespace'::MakeFailResultWithName","line":503,"tag":"0x8d165e86fb8195c5"},"suberro
r":{"code":10551508,"fields":{"$module":"disk_bundle_vsa64_
41100","IsReturnCode":1},"src":
{"fichier":"c:\\\\b\\\\1223\\\\enterprise\\\\mms\\\\managers\\\\archive\\\\impl\\\\p
rivate_
manager.cpp","func":"ArchiveManagement::PrivateArchiveManager::FindArchive","line":9
58,"tag":"0xb320396adfe3e63"},"suberror":{"code":19333376,"fields":{"$module":"disk_
bundle_vsa64_41100","Domain":"STORAGE_MANAGER","Reason":"CANotFoundErr"},"src":
{"fichier":"c:\\\\b\\\\1223\\\\enterprise\\\\backup\\\\online\\\\storage_manager_
client\\\\impl\\\\storage_manager_client.cpp","func":"`anonymous-
namespace'::StorageManagerImpl::GetErrorDetails","line":130,"tag":"0xb9f2653089b4a64
1"},"suberror":{"code":38207501,"fields":{"$module":"disk_bundle_vsa64_
41100","status":404,"uri":"https://eu-cloud.acronis.com:80/api/infra_
manager/v2/backup_storage"},"src":
{"fichier":"c:\\\\b\\\\1223\\\\enterprise\\\\backup\\\\online\\\\storage_manager_
client\\\\impl\\\\storage_manager_client.cpp","func":"`anonymous-
namespace'::StorageManagerImpl::ParseTransportResult","line":139,"tag":"0xb9f2653089
b4a64a"},"suberror":{},"text":"Échec de la requête HTTP pour l'URL \\"https://eu-
cloud.acronis.com:80/api/infra_manager/v2/backup_storage\\".\\n Code de réponse du
serveur : \\"404 - Not Found: La ressource demandée est introuvable\\".\\n Message
de réponse du serveur : {\\"domain\\":\\"STORAGE_
MANAGER\\",\\"code\\":\\"404\\",\\"reason\\":\\"CANotFoundErr\\",\\"debug\\":
{\\"msg\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not found in CA
table\\"},\\"message\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not
found in CA table\\"}","types":
{"$module":"A","status":"N","uri":"A"}},"text":"Erreur du client de gestion du
stockage","types":{"$module":"A","Domain":"A","Reason":"A"}},"text":"Échec de la
recherche de l'archive 'WIN-R1OR1V5M79O-1A57176B-90DE-494B-BB59-9325C447E513-
3B9187D6-0853-45FF-AAB0-0C68CD643068A'.","types":
{"$module":"A","IsReturnCode":"N"}},"text":"TOL : Échec de l'exécution de la
commande. Sauvegarde en cours","types":
{"$module":"A","AgentName":"W","CommandID":"A"}},"text":"TOL : Échec de l'exécution
de la commande. Sauvegarde en cours","types":
{"$module":"A","AgentName":"W","CommandID":"A"}},"errorMessage":
{"code":"MemoFailedToDiscoverFesUri","context":{"Domain":"STORAGE_MANAGER","cause_
str":"Échec de la requête HTTP pour l'URL \\"https://eu-
cloud.acronis.com:80/api/infra_manager/v2/backup_storage\\".\\n Code de réponse du
serveur : \\"404 - Not Found: La ressource demandée est introuvable\\".\\n Message
de réponse du serveur : {\\"domain\\":\\"STORAGE_
MANAGER\\",\\"code\\":\\"404\\",\\"reason\\":\\"CANotFoundErr\\",\\"debug\\":
{\\"msg\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not found in CA
table\\"},\\"message\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not
found in CA table\\"}","effect_str":"TOL : Échec de l'exécution de la commande.
Sauvegarde en cours"},"domain":"cloud_platform","kbLink":
{"version":20706,"lineTag":"0xB9F2653089B4A64A","os":"Windows","solution":"cloud","s
erCode":"BackupFailed+0x01350016+0x01350016+0x00A100D4+0x01270100+0x0247000D","versi
on":"15.0"},"reason":"MemoFailedToDiscoverFesUri","serCode":"0x01350016+0x01350016+0
x00A100D4+0x01270100+0x0247000D"},"finishTime":1760520707,"planId":"1A57176B-90DE-
494B-BB59-9325C447E513","planName":"Protect Win","resourceId":"3B9187D6-0853-45FF-
AAB0-0C68CD643068","resourceName":"WIN-R1OR1V5M79O","startTime":1760520707}
```


© Acronis International GmbH, 2003-2026

```
me":"DESKTOP-VBTMUIG","verdict":"Malicious threat"} cs1Label=alertdetails
deviceExternalId=292ab054-61b9-41ec-9416-1f1b679a67a5 dvchost=DESKTOP-VBTMUIG
```

Exemples d'événement CEF

```
Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|cti.a.p.em.event.v1.0~a.p.agent.re_
registered.v1.0|cti.a.p.em.event.v1.0~a.p.agent.re_registered.v1.0|1|cs1=
{"id":"380b8b6f-e4cb-4d36-84a2-
2894a7e298b3","type":"cti.a.p.em.event.v1.0~a.p.agent.re_
registered.v1.0","time":"2025-10-10T17:01:32.232185894Z","ingest_time":"2025-10-
10T17:01:32.266874496Z","source":"agent-manager","subject":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","tenant_id":"ba959847-ca47-4a48-90a5-cb42789d5b34"}
cs1Label=eventdetails Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|cti.a.p.em.event.v1.0~a.active_
protection.agent.disabling_uninstall_protection_
requested.v1.0|cti.a.p.em.event.v1.0~a.active_protection.agent.disabling_uninstall_
protection_requested.v1.0|1|cs1={"id":"4b6b4e57-a679-0d94-2175-
2a015cdfa9f6","type":"cti.a.p.em.event.v1.0~a.active_protection.agent.disabling_
uninstall_protection_requested.v1.0","time":"2025-10-10T17:00:51Z","ingest_
time":"2025-10-10T17:00:51.247926345Z","source":"active-protection-service","tenant_
id":"ba959847-ca47-4a48-90a5-cb42789d5b34","client_id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231"} cs1Label=eventdetails Oct 24 09:00:03 DESKTOP-VBTMUIG siem_log_
forwarder[776]:
CEF:0|Acronis|DemoCustomer|1.0|cti.a.p.em.event.v1.0~a.edr.incident.created.v1.0|cti
.a.p.em.event.v1.0~a.edr.incident.created.v1.0|1|cs1={"id":"dd71a7b9-3319-4007-a9b3-
0760bed289c6","type":"cti.a.p.em.event.v1.0~a.edr.incident.created.v1.0","time":"202
5-10-24T15:50:54.353938775Z","ingest_time":"2025-10-
24T15:50:54.361561996Z","source":"edr-etlsvc/2509.1.0-394","subject":"a999c62b-9b1e-
4d3a-85d9-d54743107b22","tenant_id":"38c8ff04-99fb-446a-967d-461a5e299814"}
cs1Label=eventdetails
```

Exemples d'activité CEF

```
Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|agent.add|agent.add|1|cs1=
{"IsProcessRoot":true,"Persistent":{"ID":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","Name":"WIN-
R1OR1V5M79O","OwnerID":"67"},"Specific":"Business","UserName":"WIN-
R1OR1V5M79O\\\\AMS User","isLegacy":true,"title":"Adding agent 'WIN-R1OR1V5M79O' to
```


© Acronis International GmbH, 2003-2026

```
the management server"} cs1Label=taskcontext cs2={"code":"ok"} cs2Label=taskresult
cs3={"uuid":"ee54f502-4a06-498c-8b00-22824ba40231","type":"A59E8BF2-39C3-42C4-B667-
CB672381A214","queue":"legacySync","priority":"normal","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"cancellable":true,"startedByUser":"WIN-
R1OR1V5M79O\\\\AMS
User","id":1634697080134496256,"idString":"1634697080134496256","state":"completed",
"issuer":{"id":"","clusterId":""},"enqueuedAt":"2025-10-
10T17:01:32.022739593Z","startedAt":"2025-10-
10T17:01:32.022739593Z","updatedAt":"2025-10-
10T17:01:32.031865547Z","completedAt":"2025-10-
10T17:01:32.022739593Z","cancelRequested":false} cs3Label=taskdetails dvchost=
suser=WIN-R1OR1V5M79O\\AMS User deviceExternalId= Oct 10 20:14:15 WIN-R1OR1V5M79O
siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|AddFeatures|AddFeatures|1|cs1={"_runtime":
{},"argument":{"add_components":["agentForAmp"],"remove_components":[],"AMSPort":0}}
cs1Label=activitycontext cs2={"code":"ok"} cs2Label=activityresult cs3=
{"uuid":"515980ce-3e51-4cc9-846d-
dd8d8fbd1918","type":"AddFeatures","taskId":1634696473042546688,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","id":1634696841088528384,"idString":"1634696841088
528384","taskIdString":"1634696473042546688","createdAt":"2025-10-
10T17:00:32.272567181Z","startedAt":"2025-10-
10T17:00:32.272567181Z","updatedAt":"2025-10-
10T17:01:36.542446095Z","completedAt":"2025-10-10T17:01:36.542446095Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""}} cs3Label=activitydetails dvchost=WIN-R1OR1V5M79O
suser= deviceExternalId=3B9187D6-0853-45FF-AAB0-0C68CD643068 Oct 10 20:14:15 WIN-
R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|policy.revoke|policy.revoke|1|cs1=
{"IsProcessRoot":true,"Persistent":{"PlanID":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","PlanName":"XDR plan"},"PlanName":"XDR
plan","Specific":"Business","isLegacy":true,"title":"Revoking plan 'XDR plan' with
ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' from the resource with ID '3b9187d6-0853-
45ff-aab0-0c68cd643068'"} cs1Label=activitycontext cs2={"code":"ok"}
cs2Label=activityresult cs3={"uuid":"7092f0e8-7945-4774-8453-
a28b66534d73","type":"44328016-20D7-4799-A357-
CF152C904ED0","taskId":1634699005819154432,"resource":{"id":"3b9187d6-0853-45ff-
aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","id":1634699005819154432,"idString":"1634699005819
154432","taskIdString":"1634699005819154432","policy":{"id":"8cc61f3c-46b0-40a6-
9d60-7d72f68555db","type":"policy.protection.total","name":"XDR
plan"},"startedByUser":"DemoCustomer2","createdAt":"2025-10-
10T17:09:33.40794126Z","startedAt":"2025-10-
10T17:09:33.40794126Z","updatedAt":"2025-10-
10T17:09:33.453071958Z","completedAt":"2025-10-10T17:09:33.40794126Z","tenant":
{"id":"66","uuid":"07f6adf7-4665-4340-865d-
c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"executor":
{"id":"","clusterId":""}} cs3Label=activitydetails dvchost=WIN-R1OR1V5M79O
suser=DemoCustomer2 deviceExternalId=3b9187d6-0853-45ff-aab0-0c68cd643068 Oct 10
```


© Acronis International GmbH, 2003-2026

```
55db' from the resource with ID '3b9187d6-0853-45ff-aab0-0c68cd643068'"}
cs1Label=taskcontext cs2={"code":"ok"} cs2Label=taskresult cs3={"uuid":"7092f0e8-
7945-4774-8453-a28b66534d73","type":"44328016-20D7-4799-A357-
CF152C904ED0","queue":"legacySync","priority":"normal","tenant":
{"id":"66","uuid":"07f6adf7-4665-4340-865d-
c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"cancellable":true,"started
ByUser":"DemoCustomer2","policy":{"id":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","type":"policy.protection.total","name":"XDR plan"},"resource":
{"id":"3b9187d6-0853-45ff-aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"id":1634699005819154432,"idString":"1634699005819154432","state":"com
pleted","issuer":{"id":"","clusterId":""},"enqueuedAt":"2025-10-
10T17:09:33.40794126Z","startedAt":"2025-10-
10T17:09:33.40794126Z","updatedAt":"2025-10-
10T17:09:33.453071958Z","completedAt":"2025-10-
10T17:09:33.40794126Z","cancelRequested":false} cs3Label=taskdetails dvchost=WIN-
R1OR1V5M79O suser=DemoCustomer2 deviceExternalId=3b9187d6-0853-45ff-aab0-
0c68cd643068 Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|AutoUpdateStandby|AutoUpdateStandby|1|cs1=
{"argument":{"add_components":[],"remove_components":["agentForAmp"],"AMSPort":0}}
cs1Label=activitycontext cs2={"code":"ok"} cs2Label=activityresult cs3=
{"uuid":"5622f2e5-880e-4fae-98c4-
4260373ffbd3","type":"AutoUpdateStandby","taskId":1634699287147900928,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","id":1634699287684771840,"idString":"1634699287684
771840","taskIdString":"1634699287147900928","createdAt":"2025-10-
10T17:10:43.921111256Z","startedAt":"2025-10-
10T17:10:43.921111256Z","updatedAt":"2025-10-
10T17:10:44.319913633Z","completedAt":"2025-10-10T17:10:44.319913633Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""}} cs3Label=activitydetails dvchost=WIN-R1OR1V5M79O
suser= deviceExternalId=3B9187D6-0853-45FF-AAB0-0C68CD643068
```


Exemples de journal d'audit CEF


```
Oct 15 14:42:46 WIN-R1OR1V5M79O siem_log_forwarder[8608]: CEF:0|Acronis
audit|DemoCustomer|1.0|user.login|user.login|2|cs1={"created_at":"2025-10-
15T11:36:34.623186Z","id":"9281f317-2d71-4741-ac85-d085c94e95b6","date":"2025-10-
15T11:36:28Z","event_type":"user.login","request_type":"ui","initiator_
ip":"10.136.42.69","initiator_tenant_name":"DemoCustomer","initiator_tenant_
uuid":"882d7a61-7124-433d-88fd-215399399838","initiator_user_
name":"DemoCustomer","initiator_user_uuid":"f0c90ee2-b350-47be-a6d8-
ce2e178bb937","object_name":"Demo Customer (DemoCustomer)","object_tenant_
name":"DemoCustomer","object_tenant_uuid":"882d7a61-7124-433d-88fd-
215399399838","object_user_name":"DemoCustomer","object_user_uuid":"f0c90ee2-b350-
47be-a6d8-ce2e178bb937","original_event_uuid":"1e179947-6608-49cb-b733-
```


© Acronis International GmbH, 2003-2026

d744c4bbc90e","severity_int":6,"severity_name":"info","tag":"all","topic":"audit_
event_retention"} cs1Label=eventdetails Oct 15 14:42:46 WIN-R1OR1V5M79O siem_log_
forwarder[8608]: CEF:0|Acronis audit|DemoCustomer|1.0|settings_
service.audit.setting.value.update|settings_
service.audit.setting.value.update|2|cs1={"created_at":"2025-10-
15T11:42:14.614182Z","id":"101f7fb1-dd59-424a-b016-8986691f139f","date":"2025-10-
15T11:42:11Z","event_type":"settings_service.audit.setting.value.update","request_
type":"api","initiator_ip":"10.233.95.53","initiator_tenant_name":"/","initiator_
tenant_uuid":"0e467be0-d567-4427-9dce-e7a2a16f9ada","object_name":"uninstall_
protection","object_tenant_name":"Demo Customer (DemoCustomer)","object_tenant_
uuid":"3c580230-60bb-42f6-a2da-ccabf0942065","original_event_uuid":"a23b3692-12c8-
48b6-a828-ceceabbb2ffa","severity_int":6,"severity_
name":"info","tag":"all","topic":"audit_event_retention"} cs1Label=eventdetails Oct
24 08:15:00 DESKTOP-VBTMUIG siem_log_forwarder[7292]: CEF:0|Acronis
audit|DemoCustomerA|1.0|offering_item.turn_on|offering_item.turn_on|2|cs1={"created_
at":"2025-10-24T15:06:10.192939Z","id":"1d53c87f-5a6f-4596-9368-
6929671b788d","date":"2025-10-24T15:06:03Z","event_type":"offering_item.turn_
on","request_type":"ui","initiator_ip":"10.35.7.44","initiator_tenant_
name":"/","initiator_tenant_uuid":"0e467be0-d567-4427-9dce-e7a2a16f9ada","initiator_
user_name":"root","initiator_user_uuid":"3e43c07f-a0e4-407c-a30a-
280462bc8538","object_name":"bndl_archiving_storage","object_tenant_
name":"DemoCustomerA","object_tenant_uuid":"d4155dae-f7cc-4063-8df5-
a0610149f074","original_event_uuid":"dbb34536-e8f2-481f-8f3d-
03094f9b385d","severity_int":6,"severity_name":"info","tag":"all","topic":"audit_
event_retention"} cs1Label=eventdetails Oct 24 08:15:00 DESKTOP-VBTMUIG siem_log_
forwarder[7292]: CEF:0|Acronis audit|DemoCustomerA|1.0|offering_item.turn_
off|offering_item.turn_off|5|cs1={"created_at":"2025-10-
24T15:06:10.186668Z","id":"e588f538-96bc-48f3-a799-9de073b0795f","date":"2025-10-
24T15:06:03Z","event_type":"offering_item.turn_off","request_type":"ui","initiator_
ip":"10.35.7.44","initiator_tenant_name":"/","initiator_tenant_uuid":"0e467be0-d567-
4427-9dce-e7a2a16f9ada","initiator_user_name":"root","initiator_user_
uuid":"3e43c07f-a0e4-407c-a30a-280462bc8538","object_name":"bndl_archiving_
storage","object_tenant_name":"DemoCustomer A (DemoCustomerA)","object_tenant_
uuid":"38c8ff04-99fb-446a-967d-461a5e299814","original_event_uuid":"bfbe9c06-f5ac-
4804-bde8-4770659e8d9a","severity_int":4,"severity_
name":"warning","tag":"all","topic":"audit_event_retention"} cs1Label=eventdetails
Oct 24 08:15:00 DESKTOP-VBTMUIG siem_log_forwarder[7292]: CEF:0|Acronis
audit|DemoCustomerA|1.0|offering_item.turn_off|offering_item.turn_off|5|cs1=
{"created_at":"2025-10-24T15:06:10.193067Z","id":"dbc0aa56-3aa3-44fc-bf91-
83ac06aae807","date":"2025-10-24T15:06:03Z","event_type":"offering_item.turn_
off","request_type":"ui","initiator_ip":"10.35.7.44","initiator_tenant_
name":"/","initiator_tenant_uuid":"0e467be0-d567-4427-9dce-e7a2a16f9ada","initiator_
user_name":"root","initiator_user_uuid":"3e43c07f-a0e4-407c-a30a-
280462bc8538","object_name":"bndl_dr_compute_points","object_tenant_
name":"DemoCustomerA","object_tenant_uuid":"d4155dae-f7cc-4063-8df5-
a0610149f074","original_event_uuid":"b529f7b7-7f49-4c83-b465-
530b826ea664","severity_int":4,"severity_name":"warning","tag":"all","topic":"audit_
event_retention"} cs1Label=eventdetails

© Acronis International GmbH, 2003-2026

Exemples d'alerte JSON


```
{"id":"A5BD4F48-6D24-4FF0-BD43-
FD7CE7367B0E","type":"EDRIncidentDetected","createdAt":"2025-10-
24T15:24:25.873371Z","severity":"warning","receivedAt":"2025-10-
24T15:24:26.63156432Z","updatedAt":"2025-10-24T15:24:26.63156432Z","tenant":
{"id":"102","uuid":"38c8ff04-99fb-446a-967d-
461a5e299814","locator":"/1/100/101/102/"},"category":"EDR","details":
{"changeId":"1","customerIncidentId":"1","customerName":"DemoCustomer","detectionTim
e":"2025-10-24T15:24:25.873371Z","edrAlertId":"637e4e23-bf95-4147-8fb8-
4b3664a7f51f","incidentCategories":"URL_BLOCKED","incidentId":"5894ce04-f94b-4cd3-
8685-f91efb3fd6a0","incidentTrigger":"no-ssl.acronis-detection-
test.com","isMalicious":"true","isMitigated":"true","mitigationState":"AUTO_
MITIGATED","osType":"WINDOWS","redirectLink":"https://eu-
cloud.acronis.com/ui/#/endpoint-detection/customer/101/incidents/5894ce04-f94b-4cd3-
8685-f91efb3fd6a0/investigation","resourceId":"292ab054-61b9-41ec-9416-
1f1b679a67a5","resourceName":"DESKTOP-VBTMUIG","verdict":"Malicious threat"}}
{"id":"33A7E16F-9FE4-08BB-0EA1-
EF91855ACAFC","type":"BackupCanceled","createdAt":"2025-10-
24T15:19:15Z","severity":"warning","receivedAt":"2025-10-
24T15:04:08.316243862Z","updatedAt":"2025-10-24T15:19:15.216375706Z","tenant":
{"id":"104","uuid":"04cc830f-cc2d-4d85-bc0c-
154d3246ed55","locator":"/1/100/103/104/"},"category":"Backup","details":
{"activity":{"id":"EA9B4383-5B06-4F5C-8008-61D329714981"},"activityId":"EA9B4383-
5B06-4F5C-8008-61D329714981","backupLocations":
[{"name":"","type":"cloud"}],"backupSourcesType":"machines","finishTime":1761319155,
"planId":"A0210313-39A8-469F-AC1D-
D68B88923322","planName":"Linux","resourceId":"9386E27C-A64C-4E24-A2BC-
391A0DC8F9DE","resourceName":"syslog","startTime":1761319142}}
```


Exemples d'événements JSON


```
{"id":"dc405251-539d-11cc-612f-86ebefff04bf","type":"cti.a.p.em.event.v1.0~a.active_
protection.agent.disabling_uninstall_protection_requested.v1.0","time":"2025-10-
10T17:24:19Z","ingest_time":"2025-10-10T17:24:19.619132791Z","source":"active-
protection-service","tenant_id":"ba959847-ca47-4a48-90a5-cb42789d5b34","client_
id":"c8d66ac4-0d5b-4ecb-b1b0-c3649df91231"} {"id":"29126f6f-218c-49d4-82a6-
3bbc5ef1e405","type":"cti.a.p.em.event.v1.0~a.p.agent.re_
registered.v1.0","time":"2025-10-10T17:25:08.517475067Z","ingest_time":"2025-10-
10T17:25:08.989631899Z","source":"agent-manager","subject":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","tenant_id":"ba959847-ca47-4a48-90a5-cb42789d5b34"} {"id":"1d21027d-
5282-4e82-90a7-
de907a6b8808","type":"cti.a.p.em.event.v1.0~a.edr.incident.created.v1.0","time":"202
5-10-24T15:25:54.348310092Z","ingest_time":"2025-10-
24T15:25:54.354555228Z","source":"edr-etlsvc/2509.1.0-394","subject":"5894ce04-f94b-
4cd3-8685-f91efb3fd6a0","tenant_id":"38c8ff04-99fb-446a-967d-461a5e299814"}
```


© Acronis International GmbH, 2003-2026

exemples d'activité JSON


```
{"uuid":"0b013dcd-a606-4baf-80d9-
e209d74eb0f6","type":"policy.apply","queue":"legacySync","priority":"normal","tenan
t":{"id":"66","uuid":"07f6adf7-4665-4340-865d-
c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"cancellable":true,"started
ByUser":"DemoCustomer2","policy":{"id":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","type":"policy.protection.total","name":"XDR plan"},"resource":
{"id":"3b9187d6-0853-45ff-aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"context":{"IsProcessRoot":true,"Persistent":{"PlanID":"8cc61f3c-46b0-
40a6-9d60-7d72f68555db","PlanName":"XDR plan"},"PlanName":"XDR
plan","Specific":"Business","isLegacy":true,"title":"Applying plan 'XDR plan' with
ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' to resource 'WIN-R1OR1V5M79O' with ID
'3b9187d6-0853-45ff-aab0-
0c68cd643068'"},"id":1634702033410387968,"idString":"1634702033410387968","state":"c
ompleted","issuer":{"id":"","clusterId":""},"enqueuedAt":"2025-10-
10T17:22:10.323642031Z","startedAt":"2025-10-
10T17:22:10.323642031Z","updatedAt":"2025-10-
10T17:22:10.350557478Z","completedAt":"2025-10-
10T17:22:10.323642031Z","cancelRequested":false,"result":{"code":"ok"}}
{"uuid":"0b013dcd-a606-4baf-80d9-
e209d74eb0f6","type":"policy.apply","taskId":1634702033410387968,"resource":
{"id":"3b9187d6-0853-45ff-aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","context":{"IsProcessRoot":true,"Persistent":
{"PlanID":"8cc61f3c-46b0-40a6-9d60-7d72f68555db","PlanName":"XDR
plan"},"PlanName":"XDR plan","Specific":"Business","isLegacy":true,"title":"Applying
plan 'XDR plan' with ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' to resource 'WIN-
R1OR1V5M79O' with ID '3b9187d6-0853-45ff-aab0-
0c68cd643068'"},"id":1634702033410387968,"idString":"1634702033410387968","taskIdStr
ing":"1634702033410387968","policy":{"id":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","type":"policy.protection.total","name":"XDR
plan"},"startedByUser":"DemoCustomer2","createdAt":"2025-10-
10T17:22:10.323642031Z","startedAt":"2025-10-
10T17:22:10.323642031Z","updatedAt":"2025-10-
10T17:22:10.350557478Z","completedAt":"2025-10-10T17:22:10.323642031Z","tenant":
{"id":"66","uuid":"07f6adf7-4665-4340-865d-
c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"executor":
{"id":"","clusterId":""},"result":{"code":"ok"}} {"uuid":"fe72e679-541b-42fe-a622-
31bd5711ca1f","type":"Download","taskId":1634709492787113984,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","context":{"_runtime":{},"argument":{"add_
components":[],"remove_components":
["agentForAmp"],"AMSPort":0}},"id":1634709499225370624,"idString":"16347094992253706
24","taskIdString":"1634709492787113984","createdAt":"2025-10-
10T17:53:16.811530215Z","startedAt":"2025-10-
10T17:53:16.811530215Z","updatedAt":"2025-10-
10T17:54:33.700680609Z","completedAt":"2025-10-10T17:54:33.700680609Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""},"result":{"code":"ok"}} {"uuid":"fc557426-9e62-4550-
```


© Acronis International GmbH, 2003-2026

```
9e8c-
b276bffa8911","type":"AutoUpdateStandby","taskId":1634702108316463104,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","context":{"argument":{"add_components":
["agentForAmp"],"remove_components":
[],"AMSPort":0}},"id":1634702109243404288,"idString":"1634702109243404288","taskIdSt
ring":"1634702108316463104","createdAt":"2025-10-
10T17:22:29.312989889Z","startedAt":"2025-10-
10T17:22:29.312989889Z","updatedAt":"2025-10-
10T17:22:29.386614232Z","completedAt":"2025-10-10T17:22:29.386614232Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""},"result":{"code":"ok"}} {"uuid":"ae0905c8-a94c-4d18-
bcd1-
d22b88dc37f6","type":"agent.add","taskId":1634710042987524096,"state":"completed","c
ontext":{"IsProcessRoot":true,"Persistent":{"ID":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","Name":"WIN-
R1OR1V5M79O","OwnerID":"67"},"Specific":"Business","UserName":"WIN-R1OR1V5M79O\\AMS
User","isLegacy":true,"title":"Adding agent 'WIN-R1OR1V5M79O' to the management
server"},"id":1634710042987524096,"idString":"1634710042987524096","taskIdString":"1
634710042987524096","startedByUser":"WIN-R1OR1V5M79O\\AMS User","createdAt":"2025-
10-10T17:55:32.736020984Z","startedAt":"2025-10-
10T17:55:32.736020984Z","updatedAt":"2025-10-
10T17:55:32.745019179Z","completedAt":"2025-10-10T17:55:32.736020984Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":
{"id":"","clusterId":""},"result":{"code":"ok"}} {"uuid":"6868ba4c-1859-4079-a6d2-
9fcd03d5db0e","type":"F5CD89C9-3CD1-4DBC-97F3-
82BF93687B46","taskId":1639510477987147776,"state":"completed","context":
{"IsProcessRoot":true,"Persistent":{"PlanID":"9371c058-e474-4e66-b4c7-
89c1f5473276","PlanName":"EDR - XDR Protection"},"PlanName":"EDR - XDR
Protection","Specific":"Business","isLegacy":true,"title":"Editing plan 'EDR - XDR
Protection' with ID '9371c058-e474-4e66-b4c7-
89c1f5473276'"},"id":1639510477987147776,"idString":"1639510477987147776","taskIdStr
ing":"1639510477987147776","policy":{"id":"9371c058-e474-4e66-b4c7-
89c1f5473276","type":"policy.protection.total","name":"EDR - XDR
Protection"},"startedByUser":"Demo3","createdAt":"2025-10-
24T15:17:21.489728531Z","startedAt":"2025-10-
24T15:17:21.489728531Z","updatedAt":"2025-10-
24T15:17:21.494705812Z","completedAt":"2025-10-24T15:17:21.489728531Z","tenant":
{"id":"101","uuid":"d4155dae-f7cc-4063-8df5-
a0610149f074","name":"CustomerA","locator":"/1/101/"},"executor":
{"id":"","clusterId":""},"result":{"code":"ok"}}
```


Exemple d'audit JSON


```
{"created_at":"2025-10-10T17:24:27.614209Z","id":"40731c13-d69d-4557-a20a-
9009addfd65b","date":"2025-10-10T17:24:23Z","event_type":"settings_
service.audit.setting.value.update","request_type":"api","initiator_
```


© Acronis International GmbH, 2003-2026

```
ip":"10.233.95.90","initiator_tenant_name":"/","initiator_tenant_uuid":"ea80595e-
d07e-402a-b5bf-cb854cf6a437","object_name":"uninstall_protection","object_tenant_
name":"Demo Customer2 (DemoCustomer2)","object_tenant_uuid":"ba959847-ca47-4a48-
90a5-cb42789d5b34","original_event_uuid":"bf70ee8e-3c55-49ed-98ca-
b089490a4758","severity_int":6,"severity_name":"info","tag":"all","topic":"audit_
event_retention"}
```


Exemple de contenu Red Hat

Ce qui suit est un exemple de contenu SIEM basé sur Red Hat (Rocky Linux).

Ce contenu se trouve dans le fichier `/etc/rsyslog.conf`.

```
# rsyslog configuration file # For more information see /usr/share/doc/rsyslog-
*/rsyslog_conf.html # or latest version online at
http://www.rsyslog.com/doc/rsyslog_conf.html # If you experience problems, see
http://www.rsyslog.com/doc/troubleshoot.html #### GLOBAL DIRECTIVES #### # Where to
place auxiliary files global(workDirectory="/var/lib/rsyslog") # Use default
timestamp format module(load="builtin:omfile" Template="RSYSLOG_
TraditionalFileFormat") #### MODULES #### module(load="imuxsock" # provides support
for local system logging (e.g. via logger command) SysSock.Use="off") # Turn off
message reception via local log socket; # local messages are retrieved through
imjournal now. module(load="imjournal" # provides access to the systemd journal
UsePid="system" # PID nummber is retrieved as the ID of the process the journal
entry originates from FileCreateMode="0644" # Set the access permissions for the
state file StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability # Include all config
files in /etc/rsyslog.d/ include(file="/etc/rsyslog.d/*.conf" mode="optional") #
Provides UDP syslog reception # for parameters see
http://www.rsyslog.com/doc/imudp.html #module(load="imudp") # needs to be done just
once #input(type="imudp" port="514") # Provides TCP syslog reception # for
parameters see http://www.rsyslog.com/doc/imtcp.html #module(load="imtcp") # needs
to be done just once #input(type="imtcp" port="514") #### RULES #### # Log all
kernel messages to the console. # Logging much else clutters up the screen. #kern.*
/dev/console # Log anything (except mail) of level info or higher. # Don't log
private authentication messages! *.info;mail.none;authpriv.none;cron.none
/var/log/messages # The authpriv file has restricted access. authpriv.*
/var/log/secure # Log all the mail messages in one place. mail.* -/var/log/maillog #
Log cron stuff cron.* /var/log/cron # Everybody gets emergency messages *.emerg
:omusrmsg:* # Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler # Save boot messages also to boot.log local7.*
/var/log/boot.log # ### sample forwarding rule ### #action(type="omfwd" # # An on-
disk queue is created for this action. If the remote host is # # down, messages are
spooled to disk and sent when it is up again. #queue.filename="fwdRule1" # unique
name prefix for spool files #queue.maxdiskspace="1g" # 1gb space limit (use as much
as possible) #queue.saveonshutdown="on" # save messages to disk on shutdown
#queue.type="LinkedList" # run asynchronously #action.resumeRetryCount="-1" #
infinite retries if host is down # # Remote Logging (we use TCP for reliable
delivery) # # remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
```


© Acronis International GmbH, 2003-2026

Exemple de contenu Debian

Ce qui suit est un exemple de contenu SIEM basé sur Debian (Ubuntu Linux).

Ce contenu se trouve dans le fichier `/etc/rsyslog.conf`.

```
# /etc/rsyslog.conf configuration file for rsyslog # # For more information install
rsyslog-doc and see # /usr/share/doc/rsyslog-doc/html/configuration/index.html # #
Default logging rules can be found in /etc/rsyslog.d/50-default.conf
################## #### MODULES #### ################## module(load="imuxsock") #
provides support for local system logging #module(load="immark") # provides --MARK--
message capability # provides UDP syslog reception #module(load="imudp") #input
(type="imudp" port="514") # provides TCP syslog reception #module(load="imtcp")
#input(type="imtcp" port="514") # provides kernel logging support and enable non-
kernel klog messages module(load="imklog" permitnonkernelfacility="on")
############################ #### GLOBAL DIRECTIVES #### ############################
# # Use traditional timestamp format. # To enable high precision timestamps, comment
out the following line. # $ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat #
Filter duplicated messages $RepeatedMsgReduction on # # Set the default permissions
for all log files. # $FileOwner syslog $FileGroup adm $FileCreateMode 0640
$DirCreateMode 0755 $Umask 0022 $PrivDropToUser syslog $PrivDropToGroup syslog # #
Where to place spool and state files # $WorkDirectory /var/spool/rsyslog # # Include
all config files in /etc/rsyslog.d/ # $IncludeConfig /etc/rsyslog.d/*.conf
```


© Acronis International GmbH, 2003-2026

Présentation de votre niveau de protection actuel

Surveillance

L'onglet **Surveillance** fournit des informations importantes concernant votre niveau de protection actuelle, et comprend les tableaux de bord suivants :

- **Vue d'ensemble**
- **Activités**
- **Alertes**
- **Flux de menaces** (pour plus d'informations, voir "Flux de menaces" (p. 364))

Tableau de bord Vue d'ensemble

Le tableau de bord **Vue d'ensemble** fournit un certain nombre de widgets personnalisables qui apporteront une vue d'ensemble des opérations liées au service Cyber Protection. Des widgets pour d'autres services seront disponibles dans les versions à venir.

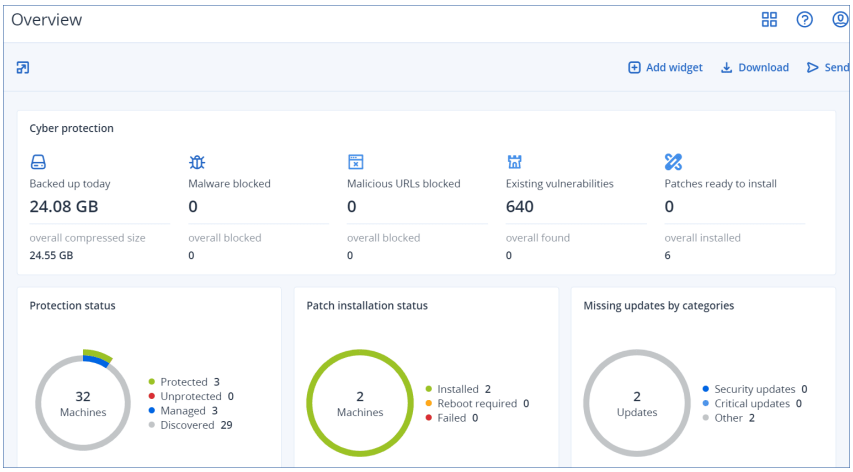
Les widgets sont mis à jour toutes les cinq minutes. Les widgets disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Vous pouvez télécharger l'état actuel du tableau de bord ou bien l'envoyer par e-mail au format .pdf et/ou .xlsx.

Vous pouvez faire un choix parmi de nombreux widgets se présentant sous la forme de tableaux, de diagrammes circulaires, de graphiques à barres, de listes et de cartes proportionnelles. Vous pouvez ajouter plusieurs widgets du même type en choisissant différents filtres.

Dans **Surveillance** > **Vue d'ensemble**, les boutons **Télécharger** et **Envoyer** ne sont pas disponibles dans les éditions Standard du service Cyber Protection.

Important
Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

© Acronis International GmbH, 2003-2026



Pour réorganiser les widgets sur le tableau de bord

Glissez-déplacez les widgets en cliquant sur leur nom.

Pour modifier un widget

Cliquez sur l'icône en forme de crayon à côté du nom du widget. Modifier un widget vous permet de le renommer, de modifier l'intervalle de temps, de définir des filtres et de grouper des lignes.

Pour ajouter un widget

Cliquez sur **Ajouter widget**, puis effectuez l'une des actions suivantes :

- Cliquez sur le widget que vous désirez ajouter. Le widget sera ajouté avec les paramètres par défaut.
- Pour modifier le widget avant de l'ajouter, cliquez sur Personnaliser lorsque le widget est sélectionné. Lorsque vous avez terminé de modifier le widget, cliquez sur **Terminé**.

Pour supprimer un widget

Cliquez sur le signe X à côté du nom du widget.

Le tableau de bord Activités

Le tableau de bord **Activités** fournit un aperçu des activités actuelles et passées sur les ressources protégées. La période de rétention est de 90 jours. Cette période peut être plus courte si le nombre d'activités est trop important ou en raison de la maintenance du centre de données. Pour les dernières informations sur la maintenance du centre de données, voir cet article de la base de connaissances.

Les dates et heures sont affichées selon les paramètres de fuseau horaire de l'ordinateur que vous utilisez pour accéder à la Cyber Protect console.

Pour personnaliser la vue du tableau de bord **Activités**, cliquez sur l'icône en forme d'engrenage, puis sélectionnez les colonnes que vous souhaitez afficher.

© Acronis International GmbH, 2003-2026

Pour consulter la progression des activités en temps réel, sélectionnez la case **Actualiser automatiquement**. Notez toutefois que l'actualisation fréquente de nombreuses activités a pour effet de dégrader les performances du serveur de gestion.

Vous pouvez effectuer une recherche parmi les activités répertoriées selon les critères suivants :

- **Nom du terminal**
  Il s'agit de l'ordinateur sur lequel l'activité est exécutée.
- **Démarrée par**
  Il s'agit du compte qui a démarré l'activité.

Vous pouvez également filtrer les activités selon les propriétés suivantes :

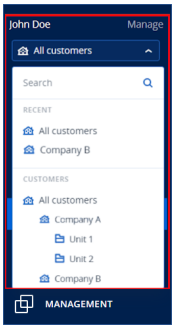
- **Statut**
  Par exemple, « a réussi », « a échoué », « en cours », « annulée ».
- **Type**
  Par exemple, application de plan, suppression de sauvegardes, installation de mises à jour logicielles.
- **Heure**
  Par exemple, les activités les plus récentes, les activités des dernières 24 heures ou les activités pendant une période spécifique au sein de la période de rétention par défaut.

Pour en savoir plus à propos d'une activité, sélectionnez l'activité dans la liste, puis, dans le volet **Détails de l'activité**, cliquez sur **Toutes les propriétés**. Pour plus d'informations sur les propriétés disponibles, reportez-vous aux références d'API Activité et Tâche sur le portail Developer Network.

Le tableau de bord des alertes

Le tableau de bord **Surveillance** > **Alertes** affiche les alertes actuelles des tenants que vous gérez. Les alertes sont affichées pour tous les tenants clients ou pour un tenant client spécifique, selon le niveau sélectionné dans la liste déroulante du menu de navigation.

La liste déroulante n'est pas disponible si vous gérez un seul tenant.



Chaque alerte contient des informations générales sur sa cause ou des conseils de dépannage. Pour obtenir une assistance supplémentaire dans la résolution du problème sous-jacent, cliquez sur **Obtenir de l'assistance** sous chaque alerte. En fonction de votre rôle et des services activés dans

© Acronis International GmbH, 2003-2026

votre tenant, vous pouvez rechercher une solution dans la base de connaissances ou soumettre un ticket d'assistance.

Personnalisation du tableau de bord Alertes

Le tableau de bord **Alertes** prend en charge la vue simple et la vue tableau. La vue simple affiche une liste déroulante des alertes actuelles, tandis que la vue tableau affiche un plus grand nombre d'alertes dans un écran, ainsi que des informations supplémentaires concernant ces alertes.

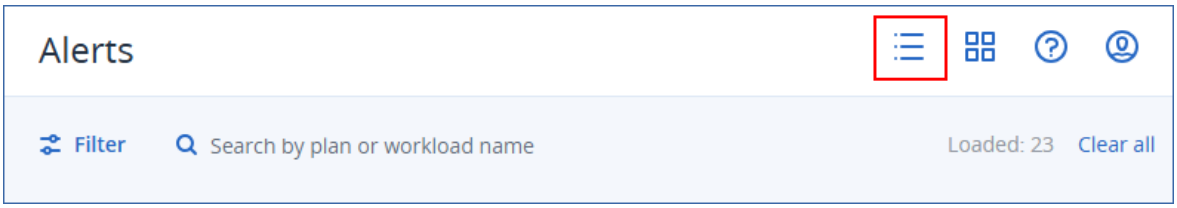
Lorsque vous utilisez la vue tableau, vous pouvez personnaliser le tableau de bord **Alertes** en ajoutant ou en supprimant des colonnes.

Avec les vues simple et tableau, vous pouvez masquer la section de filtre rapide.

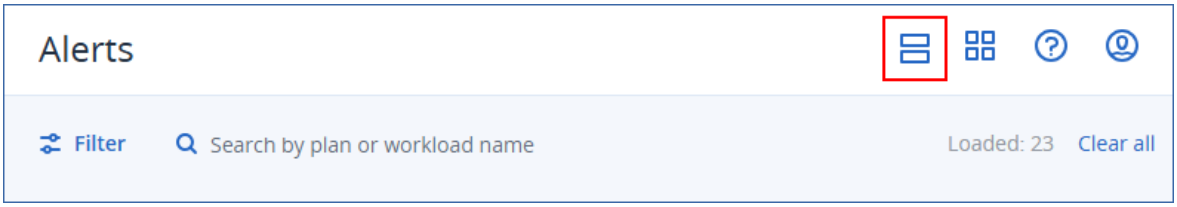
Basculer d'une vue à l'autre

Pour basculer de la vue simple à la vue tableau, et inversement

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Pour basculer en vue en tableau, cliquez sur l'icône de la vue tableau.



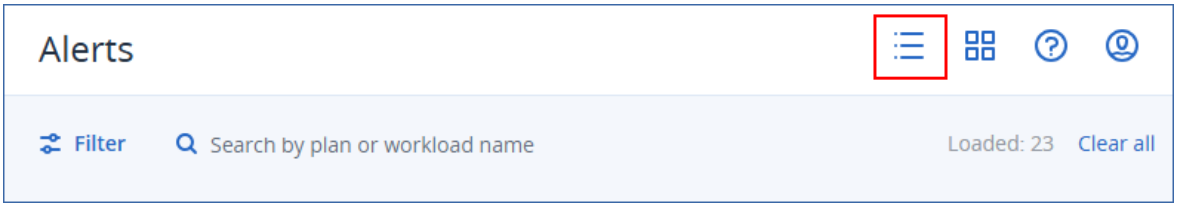
3. Pour basculer en vue simple, cliquez sur l'icône de la vue simple.



Ajouter ou supprimer des colonnes

Pour ajouter ou supprimer des colonnes

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. [Si vous utilisez la vue simple] Cliquez sur l'icône de la vue tableau.



3. Cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit, puis sélectionnez les colonnes qui doivent être visibles.
   Les colonnes suivantes sont disponibles.

© Acronis International GmbH, 2003-2026

Colonne	Description
La gravité (toujours disponible)	Niveau d'importance de l'alerte. La gravité a les différentes valeurs suivantes : • Critique • Erreur • Avertissement • Informations
Type d'alerte	Résumé des alertes. Pour plus d'informations, voir "Types et catégories d'alertes" (p. 305).
Message (toujours disponible)	Détails de l'alerte
Type de surveillance	Type de surveillance : basée sur des seuils ou sur des anomalies. Pour plus d'informations, voir "Surveillance de l'intégrité et des performances de la ressource" (p. 1523).
Ressource	Ressource pour laquelle l'alerte est générée
Date et heure	Horodatage de l'alerte
Plan	Plan lié à l'alerte (le cas échéant)
Catégorie d'alerte	Groupe d'alertes par zone fonctionnelle. Pour plus d'informations, voir "Types et catégories d'alertes" (p. 305).
Source	Origine de l'alerte : système ou application d'intégration

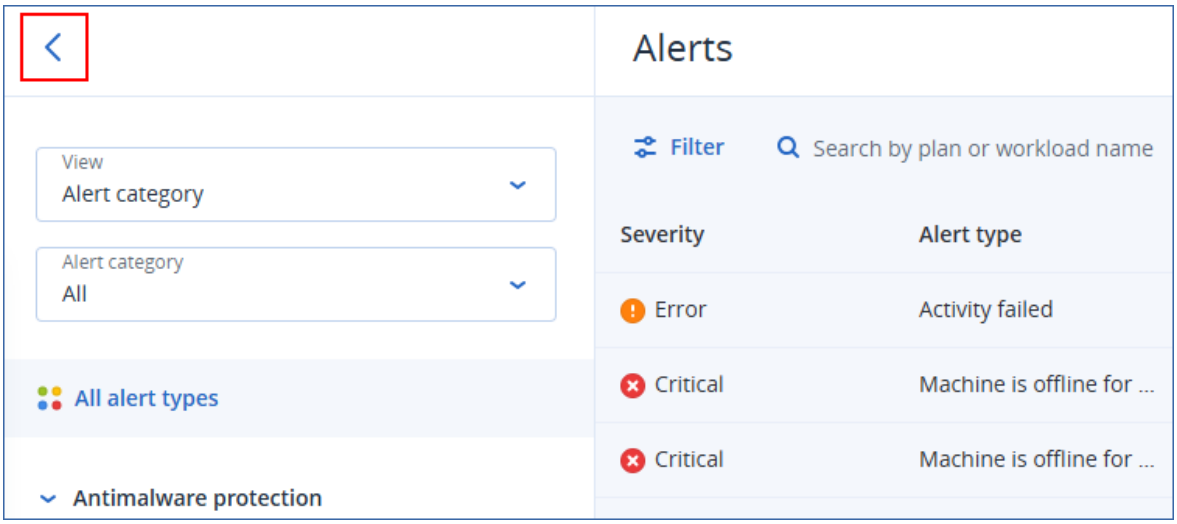
Remarque
Si plusieurs colonnes sont sélectionnées, vous devrez peut-être faire défiler l'écran horizontalement pour afficher toutes les informations disponibles.

Masquer le filtre rapide

Pour masquer la section de filtre rapide

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Cliquez sur l'icône en haut de la section de filtre rapide.

© Acronis International GmbH, 2003-2026



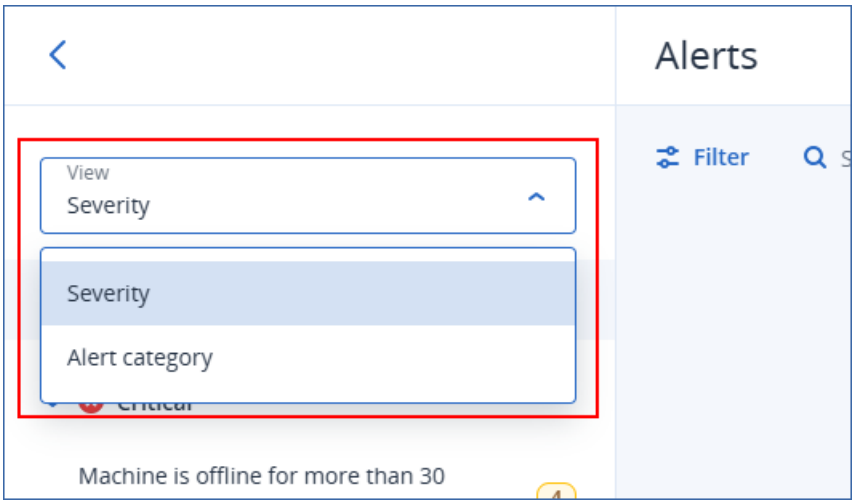
Alertes de filtrage

Vous pouvez utiliser le filtre rapide ou le filtre principal.

Filtre rapide

Pour filtrer les alertes

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Dans la liste déroulante **Vue**, sélectionnez les critères de filtrage.



3. [Facultatif] [Si vous avez sélectionné **Catégorie d'alerte**] Sélectionnez une catégorie d'alerte spécifique.
4. [Facultatif] Sélectionnez un type d'alerte spécifique.

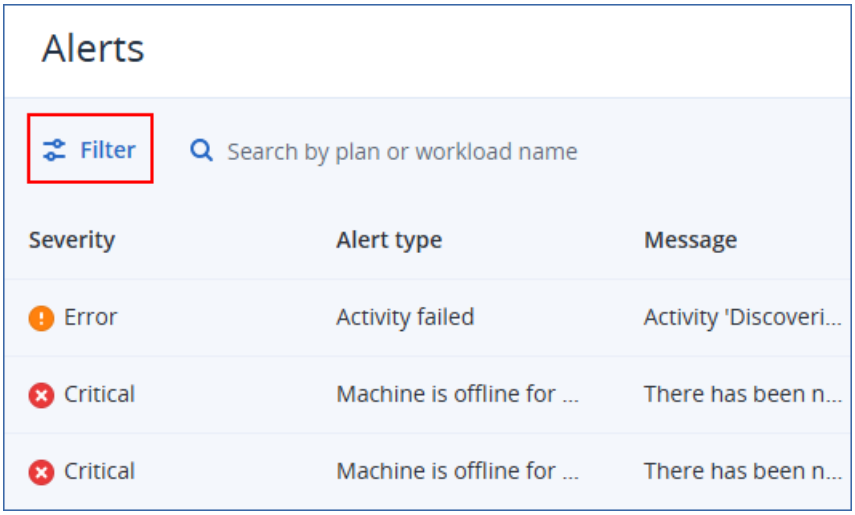
Les alertes correspondant aux critères de filtre sont répertoriés.

Filtre principal

Pour filtrer les alertes

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Cliquez sur **Filtre**.



3. Configurez les critères de filtre, puis cliquez sur **Appliquer**.

Remarque
Les critères de filtre disponibles dépendent des paramètres de filtre rapide que vous avez peut-être déjà configurés.

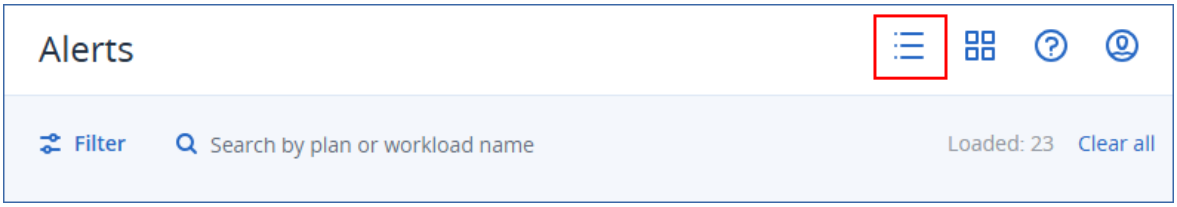
Les alertes correspondant aux critères de filtre sont répertoriés.

Tri des alertes

Lorsque vous utilisez la vue en tableau, vous pouvez trier les alertes par ordre croissant ou décroissant.

Pour trier les alertes

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. [Si vous utilisez la vue simple] Cliquez sur l'icône de la vue tableau.



3. Cliquez sur le nom du système avec lequel vous souhaitez trier les alertes.

Remarque
Vous ne pouvez pas trier les alertes en cliquant sur la colonne **Message**.

Les alertes sont triées et une flèche est affichée à côté du nom de la colonne sélectionnée.

© Acronis International GmbH, 2003-2026

Création d'un ticket de service d'assistance à partir d'une alerte

Si le service PSA est activé pour votre compte, vous pouvez créer un ticket auprès du service d'assistance directement à partir de l'alerte.

Pour créer un ticket auprès du service d'assistance

1. Dans l'alerte concernée, cliquez sur **Créer un nouveau ticket**.
   Lorsque vous travaillez en mode d'affichage tableau, vous pouvez également sélectionner une alerte puis sélectionner **Créer un nouveau ticket** dans le volet de droite.
2. Définissez ce qui suit :
   - Dans la section d'en-tête, sélectionnez la case **Facturable** si vous souhaitez que le temps passé sur le ticket soit facturé au client. Cochez également la case **Envoyer un e-mail au client** si vous souhaitez envoyer des mises à jour concernant le ticket au client.
   - Dans la section **Informations générales**, donnez un titre au ticket. Ce champ est prérempli avec un résumé de l'alerte, vous pourrez cependant le modifier.
   - Dans la section **Informations sur le client**, les champs sont préremplis avec les informations concernant l'alerte.
   - Dans la section **Élément ou service de configuration**, les champs sont préremplis avec le terminal associé à l'alerte. Vous pouvez réaffecter un terminal, selon vos besoins.
   - Dans la section **Agent de support**, les champs sont préremplis avec l'agent de support, la catégorie et le groupe de support par défaut. Vous pouvez réaffecter un autre agent, selon vos besoins.
   - Dans la section **Mise à jour du ticket**, les champs sont préremplis avec la description et les détails de l'alerte. Le champ **Statut** est défini sur **Nouveau** par défaut, et peut être modifié.
   - Dans les sections **Pièces jointes**, **Éléments facturables** et **Remarques internes**, ajoutez les éléments pertinents selon vos besoins.
3. Cliquez sur **Terminé**.
   Une fois le ticket créé, un lien vers ce ticket est ajouté à l'alerte.
   Si une alerte est fermée, le ticket associé est également automatiquement fermé.

Remarque
Vous ne pouvez créer qu'un seul ticket par alerte.

Types et catégories d'alertes

Les types d'alertes sont regroupés dans les catégories suivantes :

- Alertes de sauvegarde
- Alertes de reprise d'activité après sinistre
- Alertes de protection antimalware
- Alertes de filtrage d'URL
- Alertes de licence

© Acronis International GmbH, 2003-2026

- Alertes EDR
- Alertes de contrôle des terminaux
- Alertes système
- Alertes de connexion aux clouds publics
- Alertes de déploiement logiciel
- Gestion
- Rechercher
- Surveillance

Alertes de sauvegarde

Type d'alerte	Description	Comment résoudre l'alerte
Échec sauvegarde	L'alerte est générée en cas d'échec (avec erreur pouvant être résolue) d'exécution de la sauvegarde ou d'interruption en raison d'un arrêt du système.	Consultez le journal de l'opération de sauvegarde. Cliquez sur la ressource pour la sélectionner, puis sur **Activités** pour trouver l'avertissement dans le journal. Le message devrait vous indiquer la cause du problème.
Sauvegarde réussie avec avertissements	L'alerte est générée lorsqu'une sauvegarde a réussi avec des avertissements.	Consultez le journal de l'opération de sauvegarde. Cliquez sur la ressource pour la sélectionner, puis sur **Activités** pour trouver l'avertissement dans le journal. Le message devrait vous indiquer la cause du problème.
La sauvegarde est annulée	L'alerte est générée à chaque annulation manuelle d'une sauvegarde par l'utilisateur.	Vous pouvez démarrer la sauvegarde manuellement en cliquant sur **Exécuter maintenant** ou patienter jusqu'à l'heure de sa prochaine planification.
Sauvegarde annulée en raison d'un créneau de sauvegarde fermé	L'alerte est générée lorsque l'activité de sauvegarde a été manquée, car elle était plus longue que le créneau indiqué dans les options de sauvegarde.	Reconfigurez la planification ou modifiez les options du plan de sauvegarde dans **Performance et créneau de sauvegarde**. Développez la section concernant votre produit pour accéder aux instructions.
Sauvegarde en attente	L'alerte est générée en cas de conflit de planification et lorsque deux tâches de sauvegarde sont démarrées en même temps. Dans ce cas, la seconde tâche est mise en file d'attente jusqu'à la fin ou	Veillez à ce que vos sauvegardes s'exécutent dans les créneaux attendus et conformément à leur planification, et évitez les conflits de planification.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	l'arrêt de la première.	
La sauvegarde ne répond pas	L'alerte est générée lorsque la sauvegarde n'indique aucune progression depuis un certain temps, ce qui peut signifier qu'elle est figée.	Le problème peut être dû à un blocage. Pour plus d'informations, consultez cet article de la base de connaissances.
La sauvegarde n'a pas démarré	L'alerte est générée lorsque la sauvegarde planifiée n'a pas démarré pour une raison inconnue.	Vérifiez que vous utilisez la dernière version de votre produit Acronis Backup. • Si l'ordinateur avec agent était disponible à l'heure de démarrage de la sauvegarde : 1. Modifiez l'heure de démarrage de la sauvegarde. 2. Si l'alerte réapparaît, recréez la tâche de sauvegarde. 3. Si la tâche de sauvegarde que vous venez de créer déclenche également une alerte, contactez le support pour obtenir de l'aide. • Si l'agent était hors ligne : 1. Ne mettez pas l'ordinateur hors tension pendant la sauvegarde. 2. Si l'ordinateur n'a pas été éteint, assurez-vous qu'Acronis Managed Machine Service est en cours d'exécution : Démarrer -> Rechercher -> services.msc -> localiser Acronis Managed Machine Service. Si vous avez besoin d'aide, contactez l'équipe d'assistance.
L'état de la sauvegarde est inconnu	L'alerte est générée si l'agent de sauvegarde était hors ligne au moment d'une sauvegarde planifiée. L'état des sauvegardes de ressources sera inconnu jusqu'à ce que l'agent de sauvegarde soit en ligne.	1. Vérifiez si l'agent est censé être hors ligne (s'il s'agit, par exemple, d'un notebook qui se trouve à l'extérieur du réseau du serveur de gestion). 2. Si l'agent ne devrait pas être hors ligne, vérifiez qu'Acronis Managed Machine Service est en cours d'exécution : Démarrer -> Rechercher -> services.msc -> localisez Acronis Managed Machine Service et vérifiez son statut. Si le service est arrêté,

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		démarrez-le.
La sauvegarde est manquante	Cette alerte est générée lorsqu'aucune sauvegarde réussie n'a été effectuée depuis plus de [Nombre de jours depuis la dernière sauvegarde] jours, comme défini dans l'option de sauvegarde des alertes.	Assurez-vous que le plan avec l'option de sauvegarde **Alertes** activée est planifié et s'exécute au moins une fois pendant la période définie configurée pour cette option
La sauvegarde est corrompue	L'alerte est générée lorsque l'activité de validation s'est déroulée avec succès et indique que la sauvegarde est corrompue.	Suivez les étapes de l'article Résolution des problèmes liés aux sauvegardes corrompues. Si vous avez besoin d'aide pour identifier la cause première de la corruption des archives, contactez l'équipe d'assistance.
Échec de la protection continue des données	L'alerte est générée si la protection continue de la sauvegarde a échoué.	Vérifiez les limitations suivantes : 1. La protection continue des données n'est prise en charge que pour le système de fichiers NTFS et pour les systèmes d'exploitation suivants : • Ordinateur de bureau : Windows 7 et versions ultérieures • Serveur : Windows Server 2008 R2 et versions ultérieures 2. La protection continue des données ne prend pas en charge **Acronis Secure Zone** en tant que destination. 3. Les dossiers NFS montés sous Windows ne sont pas pris en charge. 4. La réplication en continue n'est pas prise en charge : si le plan de protection comprend deux emplacements, les tranches de protection continue des données ne sont créées que dans la première destination. Les modifications sont ensuite répliquées sur la seconde destination lors de la sauvegarde suivante. 5. Si des modifications d'un dossier local

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		protégé sont appliquées depuis une source réseau (par exemple, lorsque les utilisateurs ont accès au dossier depuis le réseau), la protection continue des données ne les détecte pas. 6. Si un fichier est utilisé (par exemple, si un fichier Excel est modifié), la protection continue des données ne détecte pas les modifications. Pour que les modifications soient détectées par la protection continue des données, enregistrez-les et fermez le fichier.
Échec de la validation	L'alerte est générée lorsque la validation de la sauvegarde ne peut pas aboutir.	Consultez le journal de l'opération ayant échoué. Cliquez sur la ressource pour la sélectionner, puis sur **Activités** pour trouver l'avertissement dans le journal. Le message devrait vous indiquer la cause du problème.
Le mot de passe de chiffrement est manquant	L'alerte est générée lorsque la clé de chiffrement de base de données est incorrecte, corrompue ou manquante.	Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe. Vous devez définir le mot de passe de chiffrement localement, sur le terminal protégé. Il n'est pas possible de définir le mot de passe de chiffrement dans le plan de protection. Pour plus d'informations, voir Définition du mot de passe de chiffrement.
Le transfert est en attente	L'alerte est générée si la vérification programmée constate que les données physiques envoyées aux archives en nuage pour ce plan de sauvegarde ne sont pas téléchargées dans le stockage.	
La restauration de la sauvegarde a échoué	L'alerte est générée si l'opération de restauration échoue lorsque vous essayez de restaurer des fichiers ou des sauvegardes système.	Déterminez la date exacte de l'échec de la sauvegarde et essayez d'effectuer une restauration avec la dernière sauvegarde aboutie.

© Acronis International GmbH, 2003-2026

Alertes de reprise d'activité après sinistre

Type d'alerte	Description	Comment résoudre l'alerte
Quota conditionnel des serveurs Cloud atteint	L'alerte est générée lorsque le quota conditionnel du stockage de reprise après sinistre est dépassé.	Augmentez le quota ou supprimez des sauvegardes du stockage dans le cloud.
Le quota conditionnel est atteint	L'alerte est générée lorsque le quota conditionnel des éléments suivants est dépassé : • Serveur Cloud. • Points de calcul. • Adresses IP publiques.	
Le quota de stockage est dépassé	L'alerte est générée lorsque le quota inconditionnel du stockage de reprise après sinistre est dépassé. Ce stockage est utilisé par les serveurs primaires et de restauration. Si la surconsommation de ce quota est atteinte, il n'est pas possible de créer des serveurs primaires et de restauration, ni d'ajouter ou d'étendre les disques des serveurs primaires existants. Si ce quota est dépassé, il n'est pas possible d'effectuer un basculement ou de démarrer un serveur arrêté. Les serveurs en cours d'exécution continuent de fonctionner.	Contactez votre partenaire pour augmenter le quota affecté.
Le quota inconditionnel est dépassé	L'alerte est générée lorsque le quota inconditionnel des éléments suivants est dépassé : • Serveurs cloud. • Points de calcul. • Adresses IP publiques.	Envisagez de faire l'acquisition de quotas supplémentaires ou désactivez les tâches de sauvegarde des terminaux que vous n'avez plus besoin de protéger.
Erreur de basculement	L'alerte est générée lorsqu'un problème système survient	1. Sélectionnez le serveur de restauration, puis cliquez sur

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	après le démarrage du basculement.	**Modifier**. 2. Réduisez le processeur/la mémoire RAM du serveur de restauration. 3. Réessayez d'effectuer un basculement.
Erreur de basculement test	L'alerte est générée lorsqu'un problème système survient après le démarrage d'un basculement test.	1. Sélectionnez le serveur de restauration, puis cliquez sur **Modifier**. 2. Réduisez le processeur/la mémoire RAM du serveur de restauration. 3. Réessayez d'effectuer un basculement test. **Remarque** Vérifiez que l'adresse IP du réseau de production est la même que celle configurée sur le serveur DHCP.
Erreur de restauration automatique	L'alerte est générée lorsqu'un problème système survient après le démarrage de la restauration automatique.	Vous voyez l'emplacement erroné dans la liste des stockages des sauvegardes : un numéro est indiqué à la place du nom (en général, le nom de l'emplacement correspond à celui de l'un des utilisateurs finaux existants) et vous n'êtes pas à l'origine de la création de cet emplacement. Supprimez l'emplacement erroné : 1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde**. 2. Recherchez l'emplacement et cliquez sur l'icône représentant une croix (x) pour la supprimer. 3. Confirmez votre choix en cliquant sur **Supprimer**. 4. Retentez le basculement.
Erreur de restauration automatique : échec de la sauvegarde	Cette alerte est générée lorsque la sauvegarde du serveur de restauration pendant le processus de restauration automatique a échoué.	

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Erreur de restauration automatique : le basculement a échoué.	Cette alerte est générée lorsque le processus de restauration automatique est revenu à la phase de transfert de données, et que la machine virtuelle dans le cloud a été démarrée.	Essayez d'effectuer à nouveau le basculement. Si cela échoue, contactez l'équipe de support.
La restauration automatique est annulée	L'alerte est générée lorsqu'un utilisateur a annulé une restauration automatique.	Fermez manuellement l'alerte dans la console.
Erreur de connexion VPN	L'alerte est générée lorsqu'une connexion VPN échoue pour des raisons qui ne sont pas liées aux actions de l'utilisateur. Le rapport d'état de l'appliance VPN est obsolète.	Si vous avez rencontré un problème lors du déploiement ou de la connexion de l'appliance VPN Acronis, contactez l'équipe de support. Veuillez inclure les informations suivantes dans votre e-mail : • Captures d'écran des messages d'erreur (le cas échéant) • Capture d'écran de l'interface de ligne de commande de l'appliance VPN Acronis • Votre centre de données Acronis Backup Cloud et votre nom de groupe.
(VPN inaccessible) La passerelle de connectivité est inaccessible	L'alerte est générée lorsque le service de Disaster Recovery ne peut pas atteindre la passerelle de connectivité. Le rapport d'état de la passerelle de connectivité est obsolète.	Si vous rencontrez un problème lors du déploiement ou de la connexion de l'appliance VPN Acronis, contactez l'équipe de support. Veuillez inclure les informations suivantes dans votre e-mail : • Captures d'écran des messages d'erreur (le cas échéant) • Capture d'écran de l'interface de ligne de commande de l'appliance VPN Acronis • Votre centre de données Acronis Backup Cloud et votre nom de groupe
Erreur de connexion VPN Ipsec	Cette alerte est générée lorsqu'il y a une erreur lors de	Vérifiez les paramètres IPsec IKE (Internet Key Exchange) sur le site

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	la négociation de la Phase 1 de l'IKE (Internet Key Exchange).	Cloud et le site local.
Réaffectation nécessaire de l'adresse IP RAS	L'alerte est générée lorsque l'appliance VPN détecte des changements dans le réseau.	Réaffectez l'adresse IP. Pour plus d'informations, voir "Réaffectation d'adresses IP" (p. 1061).
Échec de la passerelle de connectivité	L'alerte est générée lorsque le déploiement du serveur VPN dans le cloud a échoué.	Utilisez l'outil Connection Verification Tool et recherchez d'éventuelles erreurs dans son résultat. Autorisez le logiciel Acronis à traverser le contrôle des applications de votre pare-feu et de votre logiciel antimalware.
Échec de création du serveur primaire	L'alerte est générée lorsque le serveur primaire n'a pas été créé en raison d'une erreur.	
Échec de création du serveur de restauration	L'alerte est générée lorsque le serveur de restauration n'a pas été créé en raison d'une erreur.	Vérifiez que le serveur de restauration correspond à la configuration logicielle requise. Pour plus d'informations, voir "Exigences logicielles pour Disaster Recovery vers Cyber Protect Cloud" (p. 1017).
Supprimer le serveur primaire	L'alerte est générée lors de la suppression d'un serveur primaire.	
Échec de restauration du serveur	L'alerte est générée lorsque le serveur primaire ou de restauration ne parvient pas à effectuer la reprise.	Recherchez les informations détaillées. Si le message d'erreur est générique ou peu clair (par exemple, « Erreur interne »), accédez à **Disaster Recovery → Serveurs**, puis cliquez sur l'ordinateur concerné et sur **Activités**. Maintenez la touche Ctrl enfoncée et cliquez sur une activité à l'aide du bouton gauche. Cliquez sur les points de suspension (...) de l'activité, puis sur **Informations sur l'activité de cette tâche**.
Échec sauvegarde	L'alerte est générée lorsque la sauvegarde du serveur cloud (primaire ou serveur dans l'état	1. Vérifiez la connexion à l'emplacement de sauvegarde. 2. Vérifiez le périphérique de stockage

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	de basculement de production) a échoué.	des sauvegardes (sauvegardes locales).
La limite réseau est dépassée	L'alerte est générée lorsque le nombre maximal (5) de réseaux dans le cloud est atteint.	Supprimez ou modifiez les réseaux cloud pour vous assurer qu'ils correspondent aux paramètres réseau du réseau local.
Échec de runbook	L'alerte est générée en cas d'échec d'exécution du runbook.	Cela n'a pas d'incidence sur la fonctionnalité du produit et peut sans risque être ignoré. Pour plus d'informations, voir "Création d'un runbook" (p. 1105).
Avertissement de runbook	L'alerte est générée si l'exécution du runbook se termine avec des avertissements.	Cela n'a pas d'incidence sur la fonctionnalité du produit et peut sans risque être ignoré. Pour plus d'informations, voir "Création d'un runbook" (p. 1105).
Intervention de l'utilisateur du runbook requise	L'alerte est générée lorsque le runbook attend l'intervention de l'utilisateur.	Cela n'affecte pas la fonctionnalité de la solution, et cela peut être ignoré en toute sécurité. Alternativement, vous pouvez effectuer l'action décrite dans la section **Action de l'utilisateur**. Pour plus d'informations, voir "Création d'un runbook" (p. 1105).
Trafic Internet bloqué	L'alerte est générée lorsque, en raison de risques de sécurité, un administrateur bloque le trafic Internet pour une ou plusieurs des IP publiques de votre compte.	Contactez l'équipe d'assistance.
Trafic Internet débloqué	L'alerte est générée lorsque le trafic Internet de votre compte a été débloqué par un administrateur.	
Chevauchement de réseaux locaux	L'alerte est générée lors de la détection de réseaux locaux identiques ou se chevauchant.	Vérifiez la configuration de l'appliance VPN.
Quota de serveur insuffisant dans le paramètre de licence	L'alerte est générée lorsque le quota des serveurs cloud n'est pas suffisant.	• Si l'alerte est générée pour un serveur physique, assurez-vous que le tenant et l'utilisateur disposent d'un quota suffisant pour les

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		serveurs d'hébergement Web ou les éléments **Serveurs**. • Si l'alerte est générée pour un serveur virtuel, assurez-vous que le tenant et l'utilisateur disposent d'un quota suffisant pour les éléments **Serveurs d'hébergement Web** ou **Machines virtuelles**. Un serveur virtuel ne peut pas utiliser le quota de l'élément **Serveurs**.
Offre insuffisante dans le paramètre de licence	L'alerte est générée lorsque l'élément **Stockage de reprise d'activité après sinistre** est désactivé.	
Erreur de paramètre de licence	L'alerte est générée lorsque la mise à niveau de reprise d'activité après sinistre a rencontré une erreur.	Dans ce cas, contactez l'équipe d'assistance.
Points de calcul insuffisants dans le paramètre de licence	L'alerte est générée si aucun point de calcul n'est disponible.	Augmentez le quota inconditionnel pour l'élément **Points de calcul**.
Offres de serveurs insuffisantes dans le paramètre de licence	L'alerte est générée lorsque l'élément **Serveurs cloud** est désactivé.	
La stratégie n'est pas parvenue à créer le serveur de restauration	L'alerte est générée lorsqu'une erreur s'est produite pendant la configuration de l'infrastructure de reprise d'activité après sinistre.	Créez un serveur de restauration manuellement, sans la propriété **Accès Internet**. Pour plus d'informations, voir "Création d'un serveur de restauration" (p. 1067).
Basculement test automatisé du processeur de sauvegarde replanifié	L'alerte est générée lorsque l'exécution du basculement test automatisé a été replanifiée.	• Démarrez manuellement un basculement test du serveur de restauration. Pour plus d'informations, voir "Réalisation d'un basculement test" (p. 1083). • Attendez la prochaine date planifiée pour le basculement test automatique.
Basculement test automatisé du processeur de sauvegarde expiré	L'alerte est générée lorsque le basculement test automatisé a expiré.	• Augmentez la valeur du délai d'expiration pour le basculement test automatisé. • Attendez la prochaine date planifiée

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	Remarque Chaque basculement test automatisé consomme des points de calcul.	pour le basculement test automatique. • Démarrez manuellement un basculement test du serveur de restauration. Pour plus d'informations, voir "Réalisation d'un basculement test" (p. 1083).
Échec global du basculement test automatisé du processeur de sauvegarde	L'alerte est générée en cas d'échec du dernier basculement test automatisé et programmé du serveur de restauration.	• Démarrez un basculement test du serveur de restauration manuellement. Pour plus d'informations, voir "Réalisation d'un basculement test" (p. 1083). • Patientez jusqu'à la date de planification du prochain basculement test automatique.
Avertissement de basculement test automatisé	Cette alerte est générée lorsque la sauvegarde est chiffrée.	Entrez le mot de passe de chiffrement dans les paramètres du serveur de restauration.
Erreur de basculement test automatisé	Cette alerte est générée lorsqu'un basculement test automatique a échoué.	Entrez le mot de passe de chiffrement pour la sauvegarde dans les paramètres du serveur de restauration. L'opération redémarrera automatiquement.
Échec du basculement test automatique – quota d'éléments d'offre dépassé	Cette alerte est générée lorsque le basculement test automatisé a échoué. Le serveur de restauration n'est plus sous licence en raison d'un quota inconditionnel dépassé pour l'un des éléments d'offre suivants : • **DR et sauvegarde directe sur Azure** • **DR vers Acronis ou cloud hybride** • **Postes de travail** • **Machines virtuelles** • **Serveurs**	Contactez votre partenaire pour augmenter le quota affecté.
Échec du basculement test automatique – élément d'offre désactivé	Cette alerte est générée lorsque le basculement test automatique a échoué. Le	Contactez votre partenaire pour augmenter le quota affecté.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	serveur de restauration n'est plus sous licence car l'un des éléments d'offre suivants a été désactivé : • **Postes de travail** • **Machines virtuelles** • **Serveurs**	
La protection de Disaster Recovery a été désactivée pour une ressource	Cette alerte est générée lorsque la protection Disaster Recovery a été désactivée pour une ressource parce que le quota inconditionnel a été dépassé pour l'un des éléments d'offre suivants : • **DR et sauvegarde directe sur Azure** • **DR vers Acronis ou cloud hybride**	Contactez votre partenaire pour augmenter le quota affecté.
Le serveur de restauration n'est pas sous licence	Cette alerte est générée lorsque le serveur de restauration n'est plus sous licence parce que le quota inconditionnel a été dépassé pour l'un des éléments d'offre suivants : • **DR et sauvegarde directe sur Azure** • **DR vers Acronis ou cloud hybride**	Contactez votre partenaire pour augmenter le quota affecté.
Le serveur primaire n'est pas sous licence	Cette alerte est générée lorsque le serveur principal n'est plus sous licence parce que : • le quota inconditionnel pour l'élément d'offre **Serveurs Principaux** a été dépassé. • l'élément d'offre **Serveurs Principaux** a été désactivé.	Contactez votre partenaire pour augmenter le quota affecté.
Le serveur de restauration n'est plus sous licence –	Cette alerte est générée lorsque le serveur de	Contactez votre partenaire pour augmenter le quota affecté.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
quota d'éléments d'offre dépassé	restauration n'est plus sous licence en raison d'un quota inconditionnel dépassé pour l'un des éléments d'offre suivants : • **Postes de travail** • **Machines virtuelles** • **Serveurs** Les opérations de reprise d'activité après sinistre pourraient être limitées ou non prises en charge.	
Le serveur de restauration n'est plus sous licence – élément d'offre désactivé	Cette alerte est générée lorsque le serveur de restauration n'est plus sous licence parce que l'un des éléments d'offre a été désactivé : • **Postes de travail** • **Machines virtuelles** • **Serveurs** Les opérations de reprise d'activité après sinistre pourraient être limitées ou non prises en charge.	Contactez votre partenaire pour augmenter le quota affecté.
Erreur de transfert de données lors de la restauration automatique	L'alerte est générée lorsque la phase de transfert de données de la restauration automatique échoue.	Réessayez l'opération. Si elle échoue à nouveau, contactez l'équipe de support.
Échec de restauration automatique	L'alerte est générée en cas d'erreur dans la restauration automatique.	Vous voyez l'emplacement erroné dans la liste des stockages des sauvegardes : un numéro est indiqué à la place du nom (en général, le nom de l'emplacement correspond à celui de l'un des utilisateurs finaux existants) et vous n'êtes pas à l'origine de la création de cet emplacement. Supprimez l'emplacement erroné : 1. Dans Cyber Protection, accédez à **Stockage de sauvegarde**.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		2. Recherchez l'emplacement et cliquez sur l'icône représentant une croix (x) pour le supprimer. 3. Confirmez votre choix en cliquant sur **Supprimer**. 4. Relancez le basculement.
Échec de confirmation de la restauration automatique	L'alerte est générée en cas d'échec de confirmation de la restauration automatique.	Réessayez l'opération. Si elle échoue à nouveau, contactez l'équipe de support.
L'ordinateur de restauration automatique est prêt pour le basculement	Cette alerte est générée lorsque l'ordinateur est prêt pour le basculement. Plus de 90 % des données ont été transférées vers le site local.	
Basculement de la restauration automatique terminé	L'alerte est générée lorsque le basculement est réussi. La machine virtuelle est restaurée sur le site local.	Fermez manuellement l'alerte dans la console.
Agent cible de la restauration automatique hors ligne	L'alerte est générée lorsque l'agent utilisé dans le processus de restauration automatique est hors ligne.	Assurez-vous que l'agent a accès à Internet. Si nécessaire, redémarrez l'agent.
WebCP client_id dupliqué	Cette alerte est générée lorsqu'il y a un client_id dupliqué pour une ressource.	
Déploiement Azure restauré depuis la corbeille	Cette alerte est générée lorsque l'infrastructure de reprise d'activité après sinistre a été restaurée depuis la corbeille. Les serveurs de restauration en basculement de production ont été arrêtés.	
Déploiement restauré depuis la corbeille	Cette alerte est générée lorsque l'infrastructure de reprise d'activité après sinistre a été restaurée depuis la corbeille. Les serveurs principaux et les serveurs de restauration en basculement de production ont été arrêtés.	

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Suppression du groupe de ressources Azure ignorée	Cette alerte est générée lorsqu'un groupe de ressources Azure n'a pas pu être supprimé en raison d'un problème de connexion au cloud.	

Alertes de protection antimalware

Type d'alerte	Description	Comment résoudre l'alerte
Tentative de désinstallation/mise à jour de l'agent empêchée	L'alerte est générée à chaque tentative de mise à jour ou de désinstallation manuelle d'un agent de protection en dehors de la période de maintenance spécifiée, lorsque l'option **Protection contre la désinstallation de l'agent** est activée pour l'agent.	Fermez manuellement l'alerte dans la console. Consultez "Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée" (p. 208).
Une activité suspecte de connexion à distance est détectée	L'alerte est générée lorsqu'un ransomware est détecté sur une connexion à distance.	Fermez manuellement l'alerte dans la console.
Une activité suspecte est détectée	L'alerte est générée lorsqu'un ransomware est détecté dans la ressource.	Fermez manuellement l'alerte dans la console. pour désactiver l'alerte. Selon l'option indiquée dans le plan Active Protection, le processus malveillant est arrêté et les modifications apportées par ce processus sont annulées. Si aucune action n'a encore été exécutée, vous devrez résoudre le problème manuellement. Pour plus d'informations sur le processus à l'origine du chiffrement des fichiers et sur les fichiers concernés, consultez les informations détaillées de l'alerte. Si vous considérez que le processus à l'origine du chiffrement des fichiers est sanctionné par erreur (alerte de type faux positif), ajoutez-le aux processus de confiance :

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		1. Ouvrez le plan Active Protection. 2. Cliquez sur **Modifier** pour modifier les paramètres. 3. Dans **Processus de confiance**, spécifiez les processus de confiance à ne jamais considérer comme des ransomware. Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur. Par exemple : `C:\Windows\Temp\er76s7sdkh.exe`
Une activité de cryptomining est détectée	L'alerte est générée lorsque des cryptomineurs interdits sont détectés dans la ressource.	Fermez manuellement l'alerte dans la console.
Défense MBR : Une activité suspecte est détectée et suspendue	L'alerte est générée lorsqu'un ransomware est détecté dans la ressource (spécifiquement, la partition MBR/GPT est modifiée par le ransomware).	Fermez manuellement l'alerte dans la console.
Un chemin d'accès réseau non valide est spécifié	L'alerte est générée lorsque le chemin de la restauration que fournit l'administrateur n'est pas un chemin d'accès à un dossier local.	Spécifiez le chemin d'accès local pour la protection des dossiers réseau (chemin de restauration). Fermez manuellement l'alerte dans la console.
Le processus critique est ajouté avec le statut « dangereux » au plan Active Protection	L'alerte est générée lorsqu'un processus critique est ajouté en tant que processus bloqué dans la liste des exclusions de la protection.	Contactez l'administrateur pour retirer le processus critique de la liste des exclusions.
Échec de l'application d'une règle Active Protection	L'alerte est générée en cas d'échec d'application de la stratégie Active Protection.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles la stratégie Active Protection ne peut pas être appliquée.
Secure Zone : Une opération non autorisée est détectée et bloquée	L'alerte est générée lorsqu'un ransomware est détecté dans la ressource (la partition ASZ est modifiée par le	Fermez manuellement l'alerte dans la console.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	ransomware).	
Le service Active Protection ne fonctionne pas	L'alerte est générée en cas de plantage/de non-exécution du service Active Protection.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles le service Active Protection ne s'exécute pas.
Le service Active Protection n'est pas disponible	L'alerte est générée lorsque le service Active Protection n'est pas disponible, car un pilote est absent ou incompatible.	Consultez les journaux d'événements Windows et recherchez-y les plantages du service Acronis Active Protection (acronis_protection_service.exe).
Conflit avec une autre solution de sécurité	Une alerte est générée si Active Protection n'est pas disponible pour l'ordinateur {{resourceName}}, car un conflit avec une autre solution de sécurité a été détecté. Pour activer Active Protection, désactivez ou désinstallez l'autre solution de sécurité.	**Solution 1** : si vous souhaitez utiliser la protection en temps réel de Acronis, désinstallez le logiciel antivirus tiers de la ressource. **Solution 2** : si vous souhaitez utiliser un antivirus tiers, désactivez dans le plan de protection appliqué à la ressource la protection en temps réel d'Acronis, le filtrage d'URL et l'antivirus Windows Defender.
Échec de l'action de quarantaine	L'alerte est générée lorsque l'antimalware ne parvient pas à mettre en quarantaine un malware qu'il a détecté.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles la mise en quarantaine a échoué.
Un processus malveillant est détecté	L'alerte est générée lorsque le moteur de comportement détecte un malware (type processus). Le malware détecté est mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un processus malveillant est détecté, mais il n'est pas mis en quarantaine	L'alerte est générée lorsque le moteur de comportement détecte un malware (type processus). Le malware détecté n'est pas mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un malware est détecté et bloqué (ODS)	L'alerte est générée lorsqu'une analyse planifiée détecte un malware. Le malware détecté est mis en quarantaine.	Fermez manuellement l'alerte dans la console.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Un malware est détecté et bloqué (RTP)	L'alerte est générée lorsque la protection en temps réel détecte un malware. Le malware détecté est mis en quarantaine.	Fermez manuellement l'alerte dans la console.
Un malware a été détecté dans une sauvegarde	L'alerte est générée lorsque l'analyse de la sauvegarde détecte un malware.	Fermez manuellement l'alerte dans la console.
Conflit détecté entre la protection antimalware en temps réel et un produit de sécurité	L'alerte est générée lorsque l'antimalware ne parvient pas à s'inscrire auprès du Centre de sécurité Windows.	**Solution 1** : si vous souhaitez utiliser la protection en temps réel de Acronis, désinstallez le logiciel antivirus tiers de la ressource. **Solution 2** : si vous souhaitez utiliser un antivirus tiers, désactivez dans le plan de protection appliqué à la ressource la protection en temps réel d'Acronis, le filtrage d'URL et l'antivirus Windows Defender.
Échec de l'exécution du module Microsoft Security Essentials	L'alerte est générée lorsque le module Microsoft Security Essentials ne s'est pas exécuté.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles l'exécution de Microsoft Security Essentials a échoué.
La protection en temps réel n'est pas disponible car un logiciel antivirus tiers est installé	L'alerte est générée lorsque la protection en temps réel n'a pas été activée, car l'antivirus tiers a activé la protection en temps réel.	Désactivez ou désinstallez le produit de sécurité tiers, ou désactivez la protection antimalware en temps réel dans le plan de protection.
La protection en temps réel n'est pas disponible en raison d'un pilote absent ou incompatible	L'alerte est générée lorsque la protection en temps réel n'est pas disponible, car un pilote est incompatible ou manquant.	Consultez le message d'erreur pour savoir pourquoi l'installation du pilote sur la ressource a échoué.
Le service Cyber Protection (ou Active Protection) ne répond pas	L'alerte est générée lorsque le service de cyberprotection répond à un ping de vérification de l'intégrité à partir de la console.	
Échec de la mise à jour des définitions de sécurité	L'alerte est générée en cas d'échec de mise à jour de la définition de sécurité.	Consultez le message d'erreur pour découvrir les raisons pour lesquelles la mise à jour des définitions de sécurité a échoué.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
La protection de l'intégrité est activée	L'alerte est générée lorsque les paramètres Microsoft Defender ne peuvent pas être modifiés, car la protection de l'intégrité est activée.	Désactivez les paramètres de protection de l'intégrité sur la ressource Windows.
Échec de l'exécution du module Windows Defender	L'alerte est générée en cas d'échec de l'exécution du module Windows Defender.	Consultez le message d'erreur si vous souhaitez connaître les raisons pour lesquelles l'exécution du module Windows Defender a échoué.
Windows Defender est bloqué par un logiciel antivirus tiers	L'alerte est générée si Windows Defender est bloqué en raison de la présence d'un antivirus tiers installé sur l'ordinateur.	Désactivez ou désinstallez le produit de sécurité tiers.
Conflit de stratégie de groupe	L'alerte est générée lorsque les paramètres Microsoft Defender ne peuvent pas être modifiés, car ils sont contrôlés par une stratégie de groupe.	Désactivez les paramètres de stratégie de groupe sur la ressource Windows.
Microsoft Security Essentials a entrepris une action pour protéger cette machine des malware	L'alerte est générée lorsque Microsoft Security Essentials a supprimé/mis en quarantaine un malware.	Fermez manuellement l'alerte dans la console.
Microsoft Security Essentials a détecté un malware	L'alerte est générée lorsque Microsoft Security Essentials a détecté un malware et d'autres logiciels potentiellement indésirables.	Fermez manuellement l'alerte dans la console.
Malware détecté dans la sauvegarde de la boîte aux lettres M365	Cette alerte est générée lorsqu'un malware est détecté lors de l'analyse de sauvegarde.	Fermez manuellement l'alerte dans la console.
Le moteur de comportement n'est pas disponible	Cette alerte est générée lorsque le moteur de comportement n'est pas disponible sur une ressource parce qu'un pilote est incompatible ou manquant.	Assurez-vous que le pilote est correctement installé sur la ressource.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Une application potentiellement indésirable a été détectée	Cette alerte est générée lorsqu'une application potentiellement indésirable est détectée.	Fermez manuellement l'alerte dans la console.
L'analyse de la sauvegarde pour la recherche de malware n'a pas démarré	Cette alerte est générée lorsque l'analyse de sauvegarde ne s'exécute pas selon la planification.	Vérifiez le message d'erreur, pourquoi l'analyse de sauvegarde n'a pas démarré.

Alertes de filtrage d'URL

Type d'alerte	Description	Comment résoudre l'alerte
Une URL malveillante a été bloquée	L'alerte est générée lorsqu'une adresse URL malveillante est bloquée par le filtrage d'URL.	Vérifiez les paramètres du filtrage d'URL. Le filtrage d'URL bloque des pages conformément aux paramètres Filtrage d'URL. Pour plus d'informations, voir "Filtrage d'URL" (p. 1197).
Un avertissement d'URL malveillante a été ignoré	L'alerte est générée lorsque vous avez choisi de poursuivre la navigation sur une adresse URL malveillante bloquée par le filtrage d'URL.	Vérifiez les paramètres du filtrage d'URL.
Conflit détecté entre le filtrage d'URL et un produit de sécurité	L'alerte est générée lorsque le filtrage des adresses URL ne peut pas être activé en raison d'un conflit avec une autre solution de sécurité.	Vérifiez les paramètres du filtrage d'URL.
L'URL du site Web est bloquée	L'alerte est générée lorsqu'une adresse URL remplit tous les critères spécifiés dans la catégorie des adresses bloquées pour le filtrage d'URL.	Vérifiez les paramètres du filtrage d'URL.
Une URL malveillante est détectée dans un e-mail	Cette alerte est générée lorsque le filtrage d'URL a détecté une URL malveillante dans une sauvegarde de boîte aux lettres M365. L'action sur détection pour le filtrage d'URL est réglée sur notification uniquement.	Vérifiez les paramètres du filtrage d'URL.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Une URL malveillante a été détectée	Cette alerte est générée lorsque le filtrage d'URL a détecté une URL malveillante. L'action sur détection pour le filtrage d'URL est réglée sur notification uniquement.	Vérifiez les paramètres du filtrage d'URL.
Impossible de se connecter à l'extension de filtrage d'URL du navigateur web	Cette alerte est générée lorsque la **protection du navigateur** est activée dans le plan de protection, qu'une connexion précédente à l'extension du navigateur a réussi, mais que l'extension est actuellement déconnectée.	Cliquez sur **Obtenez du support** pour voir l'article de la base de connaissances.
La protection du navigateur est presque prête	Cette alerte est générée lorsque la configuration de la **protection du navigateur** est incomplète. Les clés de la base de registre requises sont créées, mais aucune connexion à l'extension du navigateur Web n'a été détectée.	Fermez toutes les fenêtres du navigateur et redémarrez le navigateur web. Assurez-vous qu'aucun processus du navigateur ne s'exécute en arrière-plan.

Alertes de licence

Type d'alerte	Description	Comment résoudre l'alerte
Quota de stockage presque atteint	L'alerte est générée lorsque l'utilisation chute en dessous de 80 % (après un nettoyage ou une mise à niveau de quota).	Achetez un stockage supplémentaire ou libérez de l'espace dans votre stockage dans le cloud.
Quota de stockage dépassé	L'alerte est générée lorsque le quota de stockage est utilisé à 100 %.	Achetez plus d'espace de stockage. Pour plus d'informations, consultez cet article de la base de connaissances.
Quota de la ressource atteint	L'alerte est générée lorsque l'utilisation de l'élément est supérieure à 0, qu'elle est supérieure au quota, mais inférieure ou égale au quota + surconsommation.	
Quota de la ressource dépassé	L'alerte est générée lorsque l'utilisation de l'élément est supérieure au quota +	

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	surconsommation.	
La ressource n'a aucun quota pour appliquer un plan de sauvegarde (aucun quota de service)	L'alerte est générée dans les cas suivants : • Le quota a été supprimé manuellement : **Terminal** > **Détails** > **Quota de service**, puis cliquez sur **Modifier** et sélectionnez l'option **Aucun quota**. • L'élément **Console de gestion** est désactivé. • La valeur quota+surconsommation de l'élément **Console de gestion** est inférieure à l'utilisation en cours.	
Impossible de protéger une ressource avec un quota affecté	L'alerte est générée lorsque l'élément est insuffisant et que vous avez besoin des éléments suivants : • Un groupe dynamique. • Un plan de sauvegarde affecté à ce groupe. • Une ressource appartenant à ce groupe dynamique, mais dont certaines propriétés empêchent l'application de ce même plan de sauvegarde.	
Licence d'abonnement expirée	L'alerte est générée lorsqu'une licence a expiré.	Après l'expiration d'un abonnement, toutes les fonctionnalités du produit, à l'exception de la restauration, sont bloquées jusqu'au renouvellement de l'abonnement. Les données sauvegardées restent accessibles pour la restauration. Faites l'achat d'une nouvelle licence.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		Remarque Si vous avez fait l'achat récemment d'un nouvel abonnement, mais continuez à recevoir un message indiquant que votre abonnement est arrivé à expiration, vous devez importer le nouvel abonnement depuis le compte Acronis : dans la console de gestion, accédez à **Paramètres** -> **Licences**, puis cliquez sur **Sync**, en haut à droite. Les abonnements seront synchronisés.
La licence par abonnement arrivera bientôt à expiration	L'alerte est générée si une licence expire dans moins de 30 jours.	Faites l'achat d'un nouvel abonnement.

Alertes EDR

Type d'alerte	Description	Comment résoudre l'alerte
Incident détecté	L'alerte est générée lorsqu'un incident est créé ou que le statut d'un incident existant est mis à jour.	Cette alerte vous informe d'un nouvel incident ou de la mise à jour d'un ancien incident. Vous pouvez visualiser l'alerte et la fermer. Vous pouvez choisir d'ouvrir l'incident à des fins d'investigation.
Indicateur de compromission détecté	L'alerte est générée lorsque le service EDR de recherche de menaces a détecté un nouvel indicateur de compromission.	Cette alerte vous informe qu'un indicateur de compression a été détecté sur une ou plusieurs ressources. Lorsque cette alerte s'affiche, vous pouvez cliquer sur son lien afin de visualiser les détails concernant l'indicateur de compromission.
Échec de l'isolation de la ressource du réseau	L'alerte est générée lorsque l'utilisateur déclenche l'action permettant d'isoler l'ordinateur du réseau, mais que cette action échoue.	Prenez les mesures nécessaires.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Échec de reconnexion de la ressource au réseau	L'alerte est générée lorsque l'utilisateur déclenche l'action permettant de reconnecter l'ordinateur au réseau, mais que cette action échoue.	Prenez les mesures nécessaires.
Les paramètres du Pare-feu Windows Defender ont été modifiés	L'alerte est générée lorsque les paramètres du pare-feu ont été modifiés sur un ordinateur isolé.	Cette alerte vous informe que les informations détaillées du pare-feu ont été modifiées sur l'ordinateur isolé. Elle n'est fournie qu'à titre d'information et vous pouvez la fermer après en avoir pris connaissance.

Alertes de contrôle des terminaux

Type d'alerte	Description	Comment résoudre l'alerte
Le contrôle des terminaux et la prévention de perte de données s'exécuteront avec des fonctionnalités limitées (processeur incompatible détecté)	L'alerte est générée lorsque l'agent DeviceLock a démarré sur une machine physique avec processeur prenant en charge la technologie CET.	Désactivez l'option sur les ordinateurs concernés afin d'éviter ces alertes.
La fonctionnalité de contrôle de terminaux n'est pas encore prise en charge sur macOS Ventura	L'alerte est générée lorsque l'agent DeviceLock a démarré sur une machine physique macOS Ventura et que le plan de protection avec contrôle des terminaux est appliqué à cet agent. S'applique uniquement aux versions présentant un problème de panique du noyau lié au pilote DeviceLock.	
Transfert autorisé des données sensibles	L'alerte est générée lorsque le transfert de contenu de sensibilité est autorisé.	
Transfert justifié de données sensibles	L'alerte est générée lorsque le transfert de contenu de sensibilité est justifié.	
Transfert de données sensibles refusé	L'alerte est générée lorsque le transfert de contenu de sensibilité est bloqué.	

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Examinez les résultats du mode d'observation de la prévention de perte de données	L'alerte est générée lorsque les résultats de l'observation doivent être examinés : • La licence DLP n'est pas appliquée. • Un mois s'est écoulé depuis l'activation du mode Observation dans un plan de protection appliqué à une ressource au moins. • Un mois s'est écoulé depuis la dernière génération d'une alerte semblable et la détection d'une utilisation de DLP en mode Observation.	
L'identificateur de sécurité a été modifié pour l'utilisateur	L'alerte est générée lorsqu'un SID est mis à jour pour un nom d'utilisateur connu. Cela peut se produire lorsque le système d'exploitation est réinstallé sur une ressource hors domaine.	
L'accès au périphérique est bloqué	L'alerte est générée lorsque certaines actions (lecture/écriture) sont bloquées sur les terminaux pris en charge.	
Impossible de se connecter à une ressource SSL distante.	L'alerte est générée lorsque l'accès à une ressource SSL distante est bloqué en raison d'une prévention d'échange supplémentaire utilisée au niveau de la ressource.	Ajoutez la ressource à la liste d'autorisations pour les hôtes distants.

Alertes système

Type d'alerte	Description	Comment résoudre l'alerte
L'agent est obsolète	L'alerte est générée lorsque la version de l'agent est obsolète.	Accédez à la liste des agents et mettez l'agent à jour.
Échec de la mise à jour automatique	L'alerte est générée en cas d'échec de la mise à jour automatique de l'agent.	Essayez d'effectuer une mise à jour manuelle.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Vous devez redémarrer le terminal après avoir installé un nouvel agent	L'alerte est générée lorsqu'une installation à distance exige un redémarrage.	Redémarrez la ressource.
Vous devez redémarrer le terminal après avoir mis l'agent à jour	Cette alerte est générée lorsqu'un redémarrage est nécessaire après une installation locale réussie.	Redémarrez la ressource.
Échec de l'activité	L'alerte est générée lorsqu'une activité a échoué.	Redémarrez tous les services Acronis sur la ressource.
Activité réussie avec avertissements	L'alerte est générée lorsqu'une activité a abouti, mais que des avertissements ont été générés.	
L'activité ne répond pas	L'alerte est générée lorsqu'une activité en cours ne répond pas.	
Échec du plan de déploiement	L'alerte est générée en cas d'échec de déploiement du plan de protection.	
Échec de la conversion du nom d'utilisateur en SID	L'alerte est générée en cas d'échec de la conversion SID de la planification.	
Machine hors connexion pendant plus de 20 jours	Cette alerte est générée lorsqu'il n'y a pas eu de connexion à une ressource depuis plus de 20 jours. Les sauvegardes de la ressource seront arrêtées si la connexion n'est pas restaurée avant que le statut hors ligne atteigne 30 jours.	
Machine hors connexion pendant plus de 30 jours	Cette alerte est générée lorsqu'il n'y a pas eu de connexion à une ressource depuis plus de 30 jours. Les sauvegardes de la ressource sont arrêtées. Pour reprendre les sauvegardes, restaurer la connexion à la ressource.	
Désinstallation/mise à jour de l'agent empêchée	Cette alerte est générée lorsque le service Active Protection a mis fin à une tentative de désinstallation ou de mise à jour de l'agent de protection.	Cliquez sur **Autoriser pendant 1 heure** pour activer l'opération.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
Un conflit de plan de protection a été détecté	Cette alerte est générée lorsqu'il y a un conflit entre un plan de protection appliqué à une ressource et un plan de protection d'un groupe dynamique.	
Échec de la protection détectée	Cette alerte est générée lorsque certains pilotes sur une ressource ne fonctionnent pas correctement et que le module de protection Antivirus et de protection Antimalware est temporairement indisponible.	
Espace disque insuffisant	Cette alerte est générée lorsque l'installation d'un agent a échoué en raison d'un espace disque insuffisant sur une ressource.	Libérez de l'espace disque et redémarrez l'installation.
Redémarrage requis pour terminer l'installation de l'agent	Cette alerte est générée lorsque l'installation d'un agent s'est terminée avec succès et qu'un redémarrage est requis pour appliquer les changements.	
L'installation de l'agent ne peut pas être démarrée, car un redémarrage du système d'exploitation est en attente	Cette alerte est générée lorsque l'installation d'un agent ne peut pas être démarrée parce que la ressource attend un redémarrage.	
L'installation de l'agent a échoué, car un redémarrage du système d'exploitation est en attente	Cette alerte est générée lorsque l'installation d'un agent a échoué parce que la ressource nécessite un redémarrage.	
Échec de la mise à jour automatique	Cette alerte est générée lorsqu'une mise à jour automatique de l'agent installé sur une ressource a échoué et qu'elle est maintenant suspendue.	Mettre à jour l'agent manuellement.
Mise à jour automatique interrompue	Cette alerte est générée lorsque la mise à jour automatique vers une autre version sur une ressource a échoué. Le système	

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
	réessaiera automatiquement la mise à jour.	
L'agent est hors ligne	Cette alerte est générée lorsqu'un plan de planification n'a pas été exécuté parce que l'agent était hors ligne.	

Alertes de connexion au cloud public

Type d'alerte	Description	Comment résoudre l'alerte
Access to Azure subscription will expire soon	The alert is generated one month before the connection token for Azure subscription expires.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis cliquez sur **Renouveler l'accès**.
Access to Azure subscription expired	L'alerte est générée lorsque le jeton de connexion pour l'abonnement Azure expire.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis cliquez sur **Renouveler l'accès**.
New version of agent for Azure is available	The alert is generated when there is a new version of Agent for Azure.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis cliquez sur **Mettre à jour** pour Agent pour Azure.
The version of Agent for Azure will reach end of life soon	This alert is generated when a version of Agent for Azure will reach end of life after one release (monthly release).	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis cliquez

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		sur **Mettre à jour** pour Agent pour Azure.
The version of Agent for Azure has reached end of life	This alert is generated when a version of Agent for Azure has reached end of life.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis cliquez sur **Mettre à jour** pour Agent pour Azure.
Agent for Azure configuration failed	This alert is generated when the Agent for Azure configuration failed. Go to the **Activities** tab.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis consultez l'onglet **Activités** pour plus de détails.
Agent for Azure is in status Failed	This alert is generated when the Agent for Azure is in status Failed. Check the status of the Azure virtual machine.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis consultez l'onglet **Agent pour Azure** pour plus de détails ainsi que le lien vers le portail Microsoft Azure pour gérer la machine virtuelle.
Agent for Azure update failed	This alert is generated when the Agent for Azure update failed and the Agent for Azure version is reverted back to the previous version.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		consultez l'onglet **Activités** pour plus de détails.
Agent for Azure deletion failed	This alert is generated when the Agent for Azure was not deleted successfully.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure, puis consultez l'onglet **Agent pour Azure** pour les détails, pour le lien vers le portail Microsoft Azure où vous pouvez effectuer l'opération de suppression pour la machine virtuelle, et pour les groupes de ressources correspondants.
Agent for Azure deallocation failed	Cette alerte est générée lorsqu'un agent pour Azure inutilisé n'a pas été supprimé.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez l'abonnement Azure et consultez l'onglet **Agent pour Azure** pour les détails, pour un lien vers le portail Microsoft Azure où vous pouvez effectuer l'opération de suppression pour la machine virtuelle, et pour les groupes de ressources

© Acronis International GmbH, 2003-2026

Type d'alerte	Description	Comment résoudre l'alerte
		correspondants.
Access to S3 public cloud expiring	This alert is generated one month before the connection token for access to Amazon S3 or another S3-compatible public cloud expires.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez la connexion Amazon S3/S3-compatible dans la liste, puis cliquez sur **Renouveler l'accès**.
Access to S3 public cloud expired	This alert is generated when the connection token for access to Amazon S3 or another S3-compatible public cloud expires.	Accédez à **Infrastructure** > **Clouds publics**, sélectionnez la connexion Amazon S3/S3-compatible dans la liste, puis cliquez sur **Renouveler l'accès**.

Alertes de déploiement logiciel

Type d'alerte	Description
Incompatibilité de package logiciel détectée	Il s'agit d'une alerte critique générée lorsqu'un package logiciel ne peut pas être installé, car il n'est pas compatible avec le système d'exploitation de la ressource cible.
Tentative d'installation du logiciel manquant	Il s'agit d'une alerte critique qui est générée lorsqu'un plan de déploiement de logiciel tente d'installer un package logiciel non trouvé dans le référentiel.
Tentative de désinstallation d'un logiciel manquant	Il s'agit d'une alerte critique générée lorsqu'un plan de déploiement de logiciel tente de désinstaller un package logiciel non trouvé dans le référentiel.
Redémarrage nécessaire après l'installation du logiciel	Il s'agit d'un avertissement généré lorsque l'installation du package logiciel nécessite le redémarrage du système d'exploitation de ressource cible.

© Acronis International GmbH, 2003-2026

Type d'alerte	Description
Redémarrage nécessaire après la désinstallation du logiciel	Il s'agit d'un avertissement généré lorsque la désinstallation du package logiciel nécessite le redémarrage du système d'exploitation de la ressource cible.

Gestion

Type d'alerte	Description
Redémarrage en attente	Cette alerte est générée lorsqu'un terminal n'a pas été redémarré pendant 7 jours après un déploiement logiciel réussi.
L'analyse de vulnérabilité a échoué	Ceci est une alerte d'avertissement qui est générée lorsqu'une analyse d'évaluation des vulnérabilités a échoué en raison d'une erreur.
Échec de l'installation des correctifs	Ceci est une alerte d'avertissement qui est générée lorsqu'une installation de gestion des correctifs a échoué en raison d'une erreur.
Redémarrage PM requis	Ceci est une alerte d'avertissement qui est générée lorsqu'un redémarrage du système est requis pour compléter le processus d'installation du correctif.
Connexion Bureau à distance échouée	Cette alerte est générée lorsque la connexion à une ressource distante ne peut pas être établie en raison d'une erreur.
Identifiants manquants	Ceci est une alerte d'avertissement qui est générée lorsqu'un script ne peut pas s'exécuter sur une ressource en raison d'identifiants manquants pour le script.
Échec de l'exécution du script	Ceci est une alerte critique qui est générée lorsque : • un script ne peut pas s'exécuter car il a le statut « Brouillon ». • un script n'est pas dans le référentiel de scripts. • un script ne peut pas s'exécuter car il est impossible de télécharger ses dépendances. • un script met trop de temps à s'exécuter sur une ressource. • un script ne peut pas s'exécuter sur une ressource car l'exécuteur de script est passé hors ligne.
Préférences du pare-feu	Ceci est une alerte d'avertissement qui est générée lorsque : • les paramètres de Microsoft Defender ont été modifiés. • les paramètres de Microsoft Defender sont verrouillés et ne peuvent pas être modifiés en raison d'une erreur interne.
Règles locales du pare-feu désactivées	Ceci est une alerte d'avertissement qui est générée lorsque les

© Acronis International GmbH, 2003-2026

Type d'alerte	Description
	règles locales pour la gestion du pare-feu sont désactivées.
Package incompatible	Il s'agit d'une alerte critique générée lorsqu'un logiciel ne peut pas être installé car il n'est pas compatible avec le système d'exploitation de la ressource cible.
Installation de package manquante	Ceci est une alerte critique qui est générée lorsque le logiciel ne peut pas être installé car il est manquant.
Désinstallation de package manquante	Ceci est une alerte critique qui est générée lorsque le logiciel ne peut pas être désinstallé car il est manquant.
Redémarrage requis pour l'installation du package	Ceci est une alerte d'avertissement qui est générée lorsqu'un redémarrage est requis pour compléter l'installation du logiciel.
Redémarrage requis pour la désinstallation du package	Ceci est une alerte d'avertissement qui est générée lorsqu'un redémarrage est requis pour compléter la désinstallation du logiciel.

Recherche

Type d'alerte	Description	Comment résoudre l'alerte
L'indexation de recherche a échoué	Cette alerte est générée lorsque l'index a échoué à se construire pour l'archive d'e-mails de Microsoft 365.	Essayez de mettre à jour ou de reconstruire l'index.
Échec de la suppression de l'élément de recherche	Cette alerte est générée lorsqu'un élément n'a pas pu être supprimé de l'archive d'e-mails de Microsoft 365 en raison d'une erreur dans les règles de rétention.	

Surveillance

Type d'alerte	Description
Une défaillance du disque dur est possible	Ceci est une alerte d'avertissement qui est générée lorsqu'un disque sur une ressource est susceptible d'échouer à

© Acronis International GmbH, 2003-2026

Type d'alerte	Description
	l'avenir.
La défaillance du disque dur est imminente	Ceci est une alerte critique qui est générée lorsqu'un disque sur une ressource est dans un état critique et échouera bientôt.
Échec de la collecte de données	Cette alerte est générée lorsque la surveillance n'a pas réussi à collecter des données pour une ressource en raison d'une erreur.

Widgets d'alerte

Dans les widgets d'alertes, vous pouvez consulter les détails suivants des alertes relatives à votre ressource :

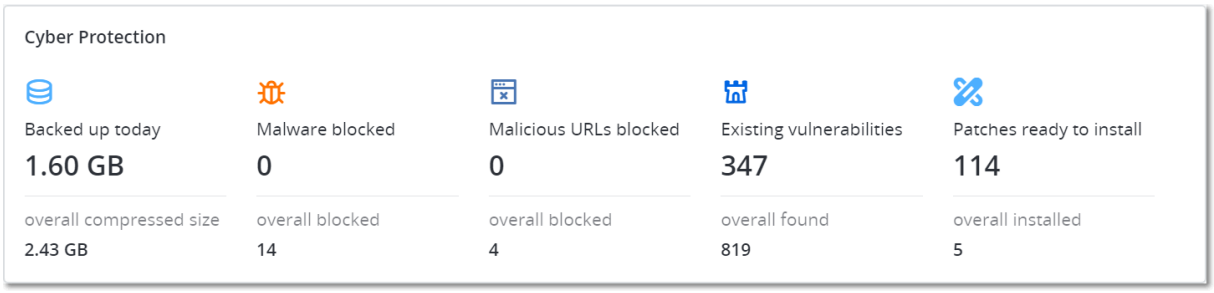
Champs	Description
Widget 5 dernières alertes	Liste des cinq dernières alertes.
Résumé de l'historique des alertes	Widget graphique affichant les alertes par gravité, type et période.
Résumé des alertes actives	Widget graphique affichant les alertes activez par gravité et type, ainsi que la somme des alertes actives.
Historique des alertes	Affichage tableau de l'historique des alertes.
Détails des alertes actives	Affichage tableau des alertes actives.

Cyber Protection

Ce widget affiche les informations globales concernant la taille des sauvegardes, des malware bloqués, des URL bloquées, des vulnérabilités trouvées et des correctifs installés.

© Acronis International GmbH, 2003-2026

Important
Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.



La ligne supérieure affiche les statistiques actuelles :

- **Sauvegardé aujourd'hui :** la somme des tailles de point de restauration pour les dernières 24 heures.
- **Malwares bloqués :** le nombre d'alertes relatives à des malwares bloqués, actives actuellement.
- **URL bloquées** : le nombre d'alertes relatives à des URL bloquées, actives actuellement
- **Vulnérabilités existantes :** le nombre actuel de vulnérabilités existantes.
- **Correctifs prêts à être installés :** le nombre actuel de correctifs disponibles et prêts à être installés.

La ligne inférieure affiche les statistiques globales :

- La taille compressée de toutes les sauvegardes
- Le nombre accumulé de malware bloqués sur l'ensemble des machines
- Le nombre accumulé d'URL bloquées sur l'ensemble des machines
- Le nombre cumulé des vulnérabilités découvertes sur l'ensemble des machines
- Le nombre cumulé de mises à jour/correctifs installés sur l'ensemble des machines

État de protection

Ce widget affiche l'état de protection actuel de toutes les machines.

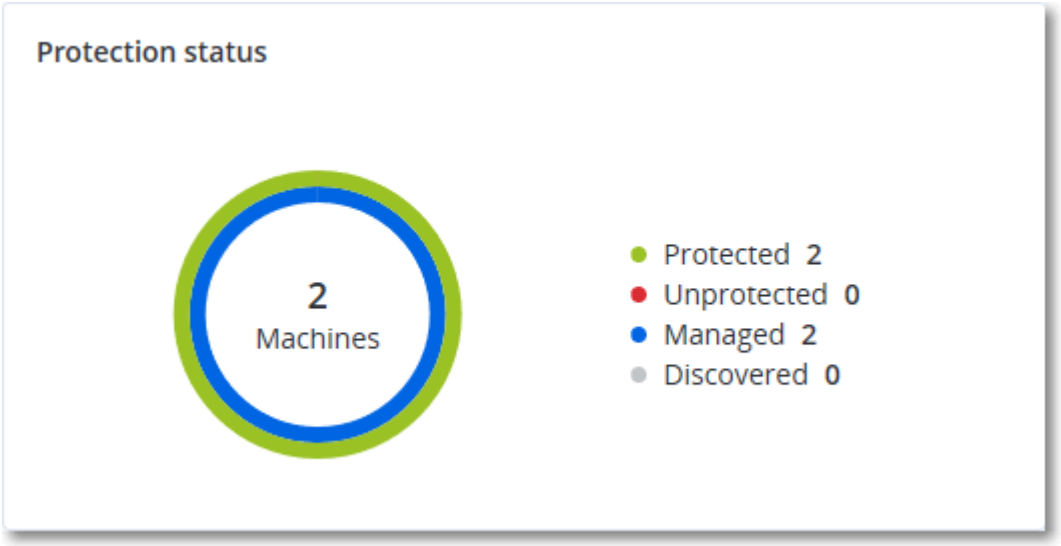
Une machine peut présenter l'un des états suivants :

- **Protégé** : machines sur lesquelles le plan de protection est appliqué.
- **Non protégé** : machines sur lesquelles le plan de protection n'est pas appliqué. Elles comprennent à la fois les machines découvertes et les machines gérées auxquelles aucun plan de protection n'est appliqué.

© Acronis International GmbH, 2003-2026

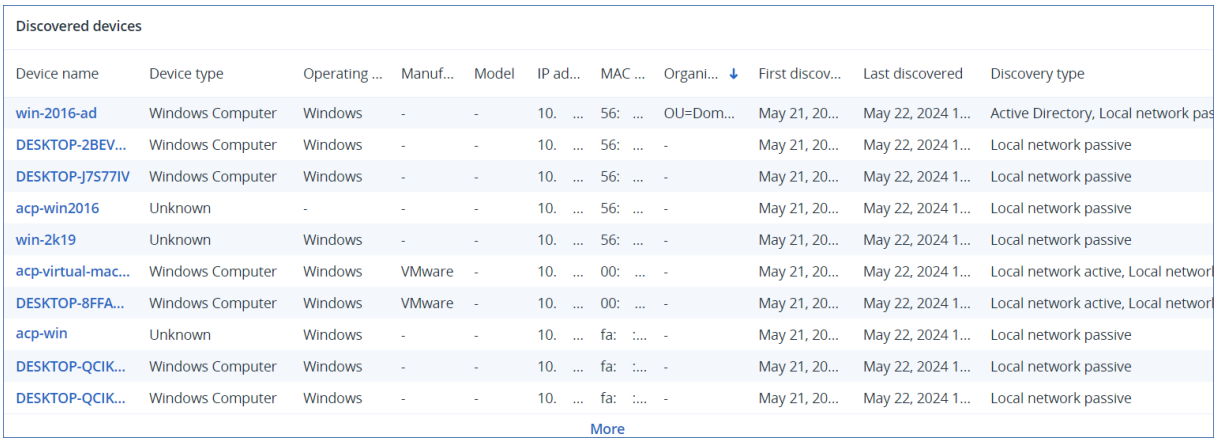
- **Géré** : machines sur lesquelles l'agent de protection est installé.
- **Découvert** : les machines sur lesquelles l'agent de protection n'est pas installé.

Si vous cliquez sur l'état de la machine, vous serez redirigé vers la liste des machines qui présentent le même état pour en savoir plus.



Terminaux découverts

Ce widget affiche des informations détaillées sur les terminaux qui ont été découverts dans les réseaux de l'organisation.



Widgets de Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) comprend sept widgets qui sont tous accessibles depuis le tableau de bord **Vue d'ensemble**. Trois d'entre eux sont également affichés par défaut dans la fonctionnalité EDR (voir "Examen des incidents" (p. 1259)).

Voici les sept widgets disponibles :

© Acronis International GmbH, 2003-2026

- Distribution des principaux incidents par ressource
- Statut de la menace (affiché dans EDR)
- Historique de gravité de l'incident (affiché dans EDR)
- Temps moyen de réparation des incidents de sécurité
- Résolution des incidents de sécurité
- Détection par tactique (affiché dans EDR)
- Statut réseau des ressources

Distribution des principaux incidents par ressource

Ce widget affiche les cinq premières ressources qui comportent le plus d'incidents (cliquez sur **Afficher tout** pour rediriger l'utilisateur vers la liste des incidents ; elle est filtrée en fonction des paramètres du widget).

Survolez une ligne de ressource pour afficher le détail de l'état des enquêtes en cours menées sur les incidents ; les états d'enquête sont les suivants : **Non démarrée**, **Enquête en cours**, **Clôturée** et **Faux positif**. Cliquez ensuite sur la ressource que vous souhaitez analyser plus en détail ; la liste des incidents est actualisée en fonction des paramètres du widget.

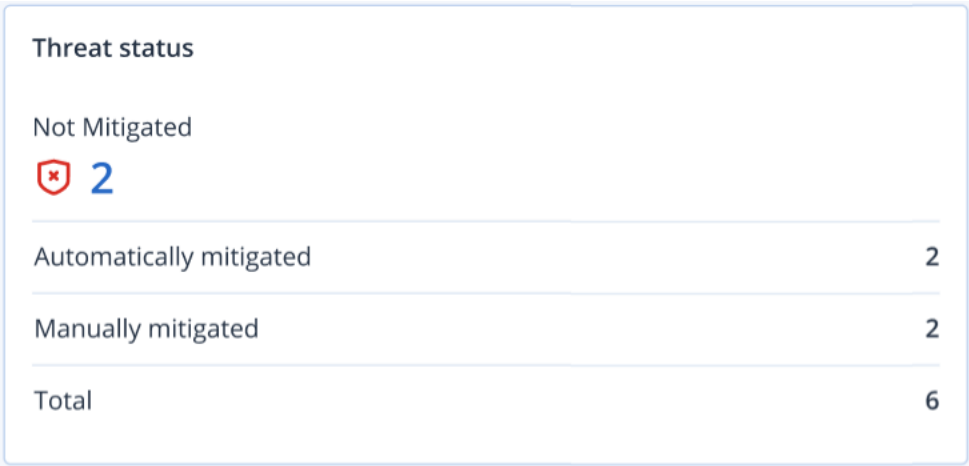


Statut de la menace

Ce widget affiche le statut de menace actuel pour toutes les ressources en mettant en évidence le nombre actuel d'incidents qui ne sont pas résolus et doivent faire l'objet d'enquêtes. Le widget indique également le nombre d'incidents résolus (manuellement et/ou automatiquement par le système).

Cliquez sur le numéro **Non atténué** pour affiche la liste des incidents non résolus uniquement.

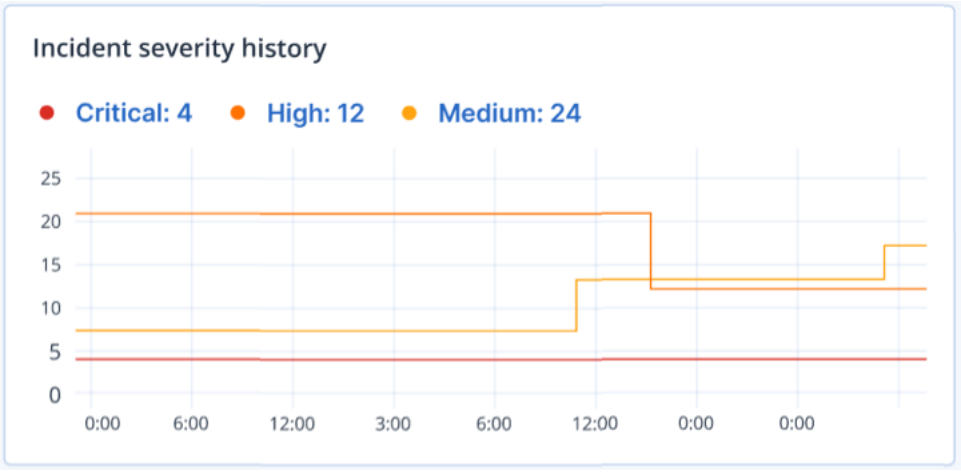
© Acronis International GmbH, 2003-2026



Historique de gravité de l'incident

Ce widget affiche l'évolution des attaques classées par gravité et peut indiquer des campagnes d'attaques. Lorsque des pics sont visibles, cela indique que l'organisation subit une attaque.

Survolez le graphique pour afficher le détail de l'historique d'un incident à un point spécifique au cours des 24 dernières heures (période par défaut). Cliquez sur le niveau de gravité (**Critique**, **Élevé** ou **Moyen**) si vous souhaitez afficher la liste des incidents associés. Vous êtes alors redirigé vers la liste préfiltrée des incidents correspondant au niveau de gravité sélectionné.

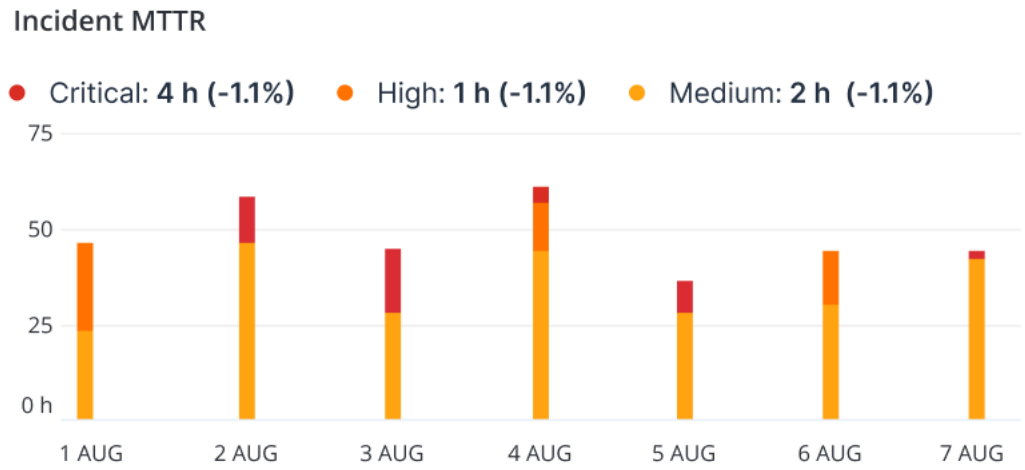


Temps moyen de réparation des incidents de sécurité

Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus.

Cliquez sur une colonne pour afficher le détail des incidents en fonction de la gravité (**Critique**, **Élevé** et **Moyen**), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.

© Acronis International GmbH, 2003-2026

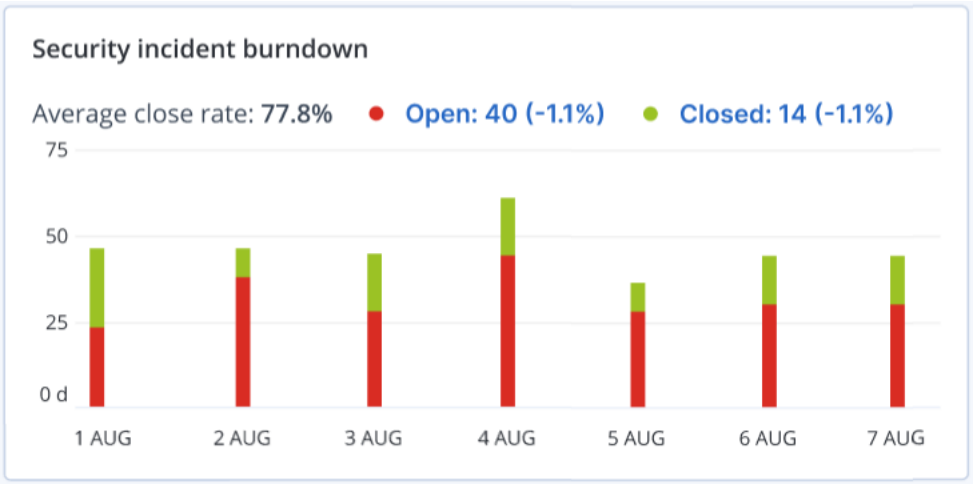


Résolution des incidents de sécurité

Ce widget indique l'efficacité de la clôture des incidents ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie.

Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. Si vous cliquez sur Ouvrir, la liste des incidents apparaît et n'affiche que les incidents ouverts (état **Enquête en cours** ou **Non démarré**). Si vous cliquez sur Clôturé, la liste des incidents qui s'affiche ne répertorie que les incidents qui ne sont plus ouverts (état **Clôturé** ou **Faux positif**).

La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.



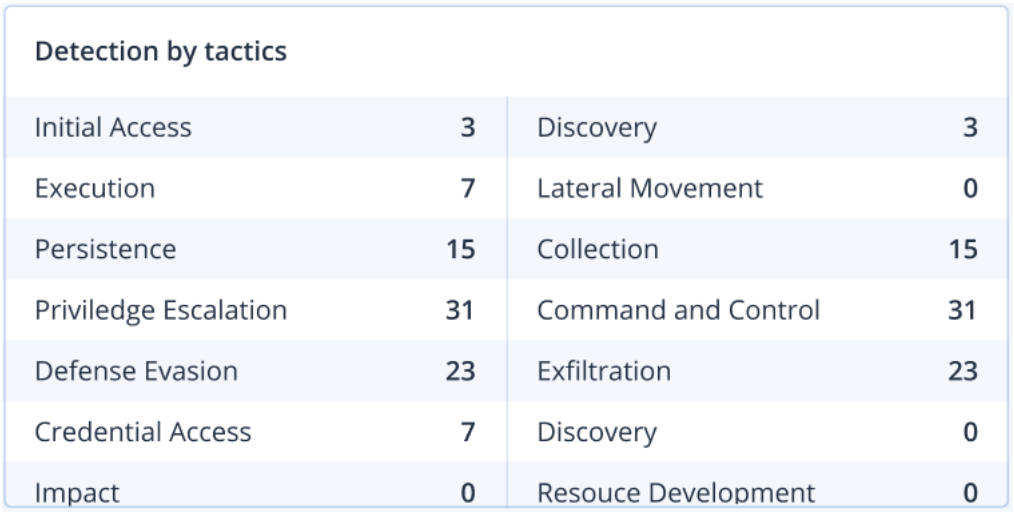
Détection par tactique

Ce widget affiche le nombre de techniques d'attaque spécifiques détectées dans les incidents au cours de la période sélectionnée.

Les valeurs affichées en vert et en rouge indiquent respectivement une augmentation ou une diminution au cours de la période précédente. Dans l'exemple ci-dessous, les attaques d'élévation

© Acronis International GmbH, 2003-2026

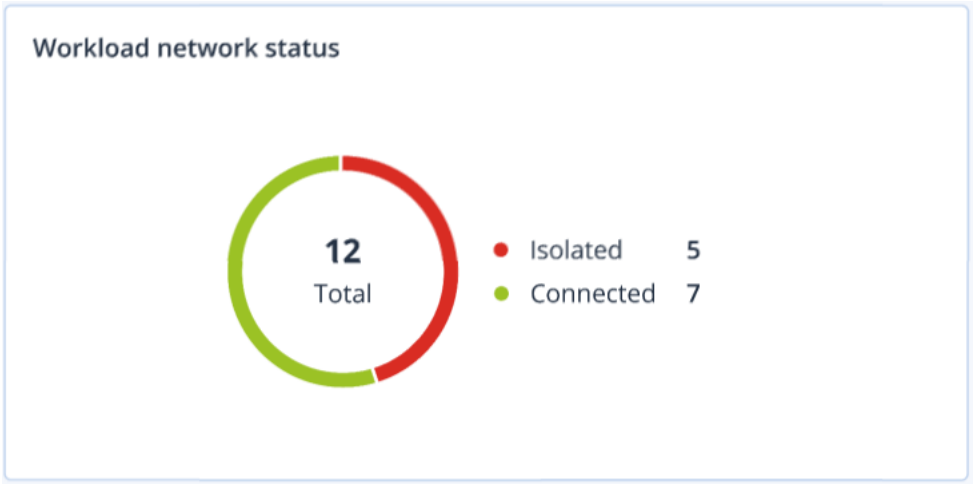
de privilèges et de commande et contrôle ont augmenté au cours de la période précédente. Cela peut indiquer que votre gestion des identifiants doit être analysée et que les mesures de sécurité doivent être améliorées.



Statut réseau des ressources

Ce widget affiche le statut réseau actuel de vos ressources ; il indique le nombre de ressources isolées et le nombre de ressources connectées.

Cliquez sur Isolé (dans le menu **Ressources** sur la console Cyber Protect) pour afficher uniquement la liste des ressources isolées avec agents. Cliquez sur Connecté pour afficher la liste des ressources avec agents connectées.



Score #CyberFit par machine

Ce widget affiche, pour chaque machine, le Score #CyberFit total, une combinaison de ses scores ainsi que les résultats pour chaque indicateur évalué :

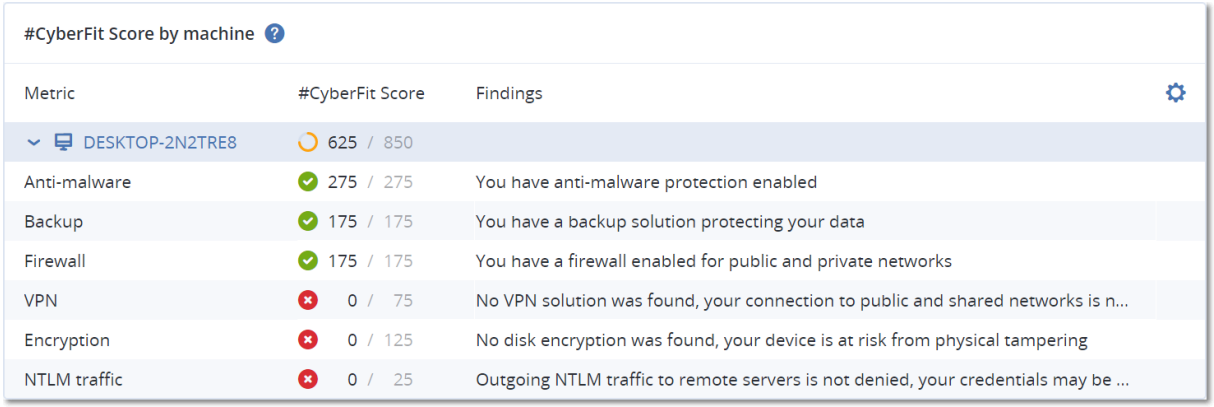
- Antimalware
- Sauvegarde

© Acronis International GmbH, 2003-2026

- Pare-feu
- VPN
- Chiffrement
- Trafic NTLM

Afin d'améliorer le score de chaque indicateur, vous pouvez afficher les recommandations disponibles dans le rapport.

Pour en savoir plus sur le Score #CyberFit, reportez-vous à « Score #CyberFit pour les machines ».



Surveillance de l'intégrité du disque

La surveillance de l'intégrité du disque fournit des informations sur l'intégrité actuelle du disque, ainsi que des prévisions concernant cette dernière. Vous pouvez ainsi prévenir les pertes de données liées à une panne du disque. Les disques durs, tout comme les SSD, sont pris en charge.

Limites

- La prévision de l'intégrité du disque est prise en charge uniquement pour les ordinateurs Windows.
- Seuls les disques des machines physiques sont surveillés. Les disques des machines virtuelles ne peuvent pas être surveillés et ne s'affichent pas dans les widgets d'intégrité du disque.
- Les configurations RAID ne sont pas prises en charge. Les widgets d'intégrité du disque n'incluent aucune information sur les ordinateurs avec implémentation RAID.
- Les disques SSD NVMe ne sont pas supportés.
- Les terminaux de stockage externes ne sont pas pris en charge.

L'intégrité du disque est représentée par l'un des états suivants :

- **OK :**
  l'intégrité du disque est comprise entre 70 et 100 %.
- **Avertissement :**
  l'intégrité du disque est comprise entre 30 et 70 %.
- **Critique :**
  l'intégrité du disque est comprise entre 0 et 30 %.

© Acronis International GmbH, 2003-2026

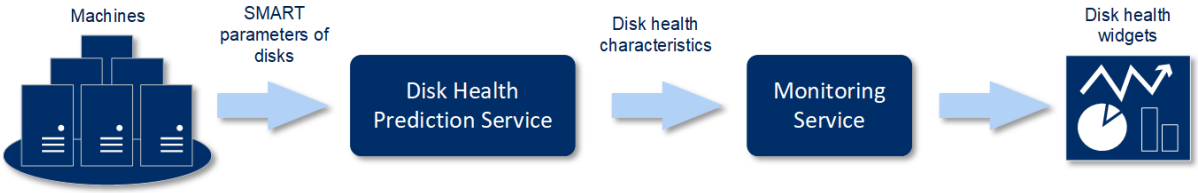
- **Calcul des données du disque :**
  l'intégrité actuelle et la prévision de l'intégrité du disque sont en cours de calcul.

Fonctionnement

Le service Prévision de l'intégrité du disque se sert d'un modèle de prévision basé sur l'intelligence artificielle.

1. L'agent de protection collecte les paramètres SMART des disques et transmet ces données au service Prévision de l'intégrité du disque :
   - SMART 5 : nombre de secteurs réalloués.
   - SMART 9 : nombre d'heures de fonctionnement.
   - SMART 187 : nombre d'erreurs signalées qui n'ont pas été corrigées.
   - SMART 188 : expiration de commandes.
   - SMART 197 : nombre actuel de secteurs en attente.
   - SMART 198 : nombre de secteurs hors ligne impossible à corriger.
   - SMART 200 : taux d'erreurs d'écriture.
2. Le service Prévision de l'intégrité du disque traite les paramètres SMART reçus, effectue des prévisions, puis fournit les caractéristiques d'intégrité du disque suivantes :
   - État de santé actuel du disque : OK, Avertissement, Critique.
   - Prévision de l'état de santé du disque : négatif, stable, positif.
   - Probabilité de prévision de l'état de santé du disque en pourcentage.

   La période de prévision est d'un mois.
3. Le service de surveillance reçoit ces caractéristiques, puis affiche les informations pertinentes dans les widgets d'intégrité du disque dans la console Cyber Protect.



Widgets de l'état de santé du disque

Les résultats de la surveillance de l'intégrité du disque sont présentés dans les widgets suivants, disponibles dans la console Cyber Protect.

- **Vue d'ensemble de l'intégrité du disque** est un widget en forme de carte proportionnelle, qui possède deux niveaux de détails que vous pouvez explorer :
  - Niveau ordinateur
    Affiche des informations résumées concernant l'intégrité du disque en fonction des ordinateurs client que vous avez sélectionnés. Seul l'état de disque le plus critique est affiché.

© Acronis International GmbH, 2003-2026

Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur sur un bloc en particulier. La taille du bloc d'un ordinateur dépend de la taille totale de l'ensemble de ses disques. La couleur du bloc d'une machine dépend de l'état de disque le plus critique identifié.



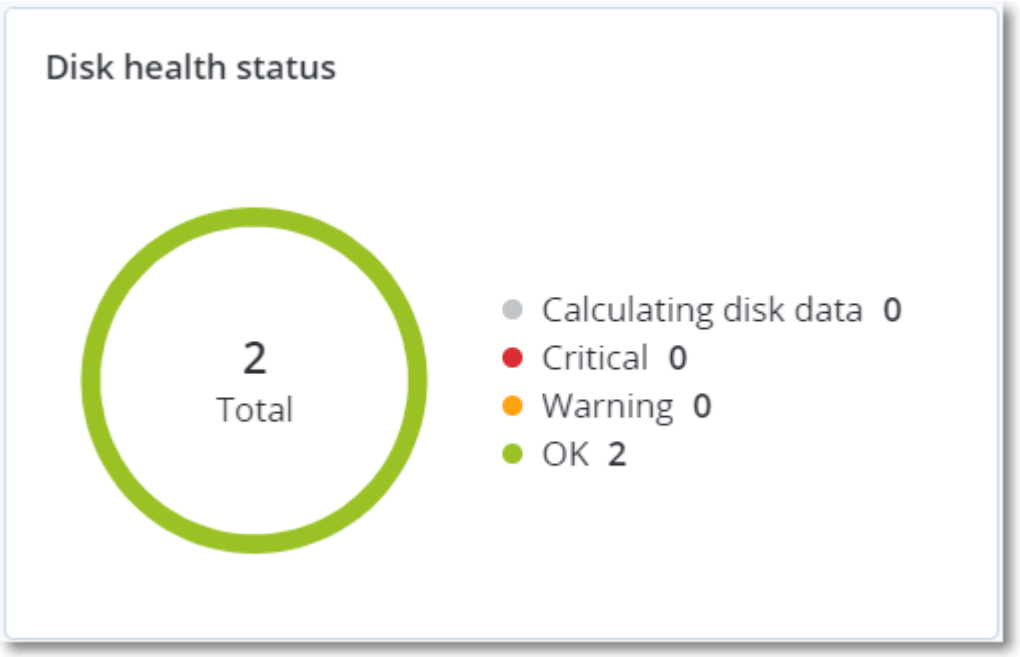
- Niveau disque
  Affiche l'intégrité actuelle de tous les disques pour l'ordinateur sélectionné. Chaque bloc de disque affiche les prévisions d'intégrité du disque suivantes, ainsi que leur probabilité en pourcentage :
  - Sera altéré
  - Restera stable

© Acronis International GmbH, 2003-2026

- Sera amélioré



- **Intégrité du disque** est un widget de graphique circulaire qui affiche le nombre de disques pour chaque état.



© Acronis International GmbH, 2003-2026

Alertes relatives à l'état de santé du disque

La vérification de l'intégrité du disque est exécutée toutes les 30 minutes, alors que l'alerte correspondante n'est générée qu'une fois par jour. Lorsque l'intégrité du disque passe de **Avertissement** à **Critique**, une alerte est toujours générée.

Nom de l'alerte	La gravité	Intégrité du disque	Description
Une défaillance du disque dur est possible	Avertissement	(30 – 70)	Il est possible que le disque <disk name> sur cet ordinateur échoue à l'avenir. Exécutez une sauvegarde d'image complète du disque dès que possible, remplacez ce dernier, puis restaurez l'image sur le nouveau disque.
La défaillance du disque dur est imminente	Critique	(0 – 30)	Le disque <disk name> sur cet ordinateur est dans un état critique et risque fortement d'échouer très bientôt. Nous ne vous recommandons pas d'effectuer une sauvegarde d'image de ce disque à ce stade, car la contrainte supplémentaire risque de causer la défaillance du disque. Sauvegardez les fichiers les plus importants sur le disque dès maintenant et remplacez-le.

Widgets de protection de l’intelligence artificielle générative

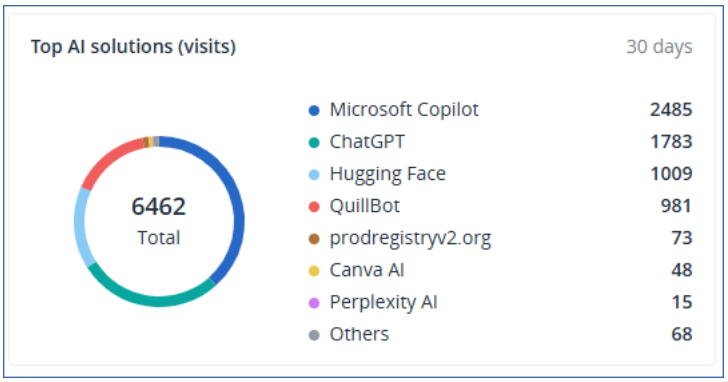
Les widgets de protection de l’intelligence artificielle générative fournissent une visibilité sur la façon dont les terminaux accèdent aux services d’intelligence artificielle générative. Utilisez-les pour identifier les solutions d’intelligence artificielle les plus populaires, les terminaux avec la plus grande activité, et les détails récents d’utilisation.

Les widgets liés à la protection de l’intelligence artificielle générative sont disponibles à la fois dans le Portail de gestion et la console Cyber Protect. Les widgets que vous pouvez ajouter et visualiser dépendent de votre rôle et du niveau actuellement sélectionné - partenaire ou client.

Principales solutions d’intelligence artificielle (visites)

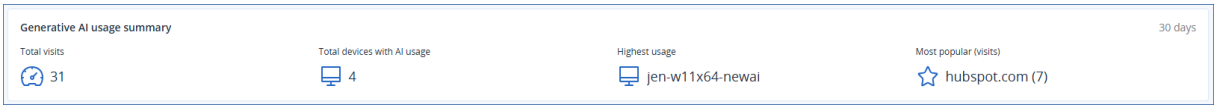
Ce widget montre les statistiques d’utilisation de l’intelligence artificielle générative par solution.

© Acronis International GmbH, 2003-2026



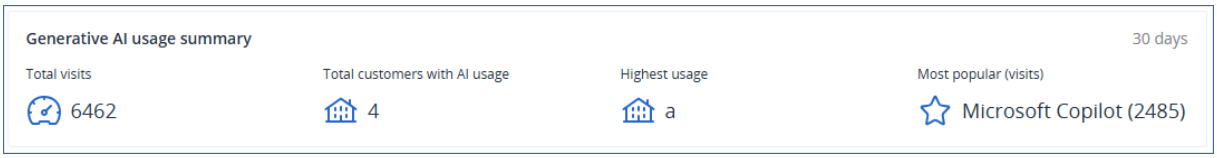
Résumé de l'utilisation de l'intelligence artificielle générative (terminaux)

Ce widget est disponible au niveau client. Il montre le résumé de l'utilisation de l'intelligence artificielle générative pour une période spécifiée.



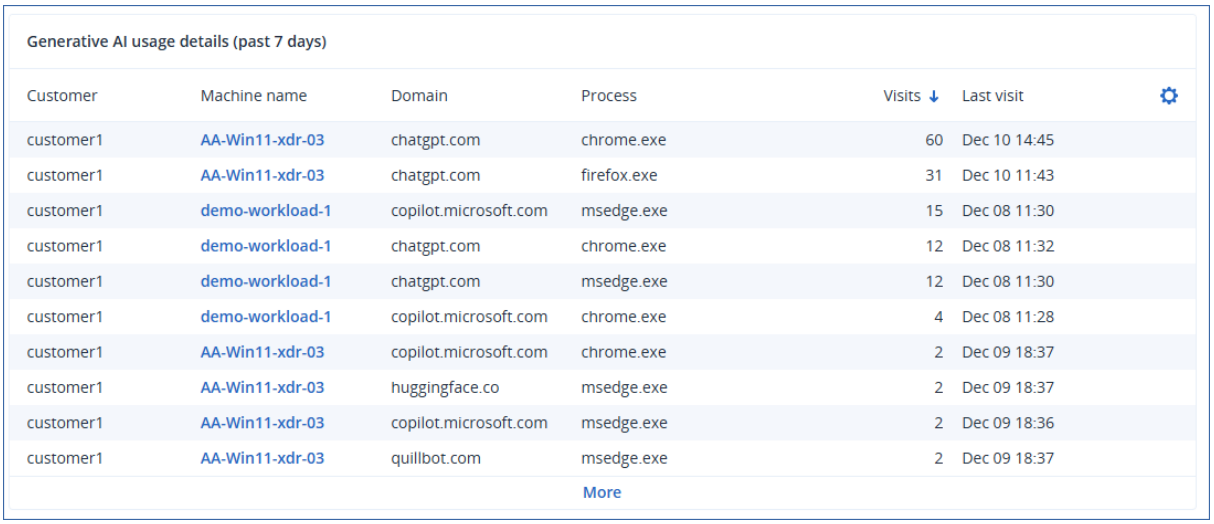
Résumé de l'utilisation de l'intelligence artificielle générative (clients)

Ce widget est disponible au niveau partenaire. Il montre le résumé de l'utilisation de l'intelligence artificielle générative pour une période spécifiée.



Détails de l'utilisation de l'intelligence artificielle générative (7 derniers jours)

Ce widget montre les informations détaillées de l'utilisation de l'intelligence artificielle générative pour les 7 derniers jours.



Generative AI usage details (past 7 days)

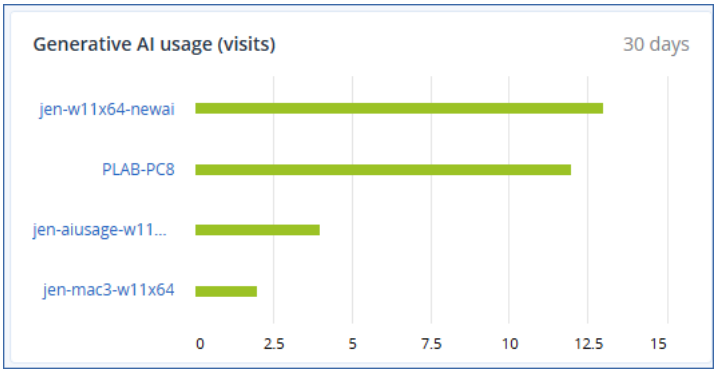
Customer	Machine name	Domain	Process	Visits ↓	Last visit
customer1	AA-Win11-xdr-03	chatgpt.com	chrome.exe	60	Dec 10 14:45
customer1	AA-Win11-xdr-03	chatgpt.com	firefox.exe	31	Dec 10 11:43
customer1	demo-workload-1	copilot.microsoft.com	msedge.exe	15	Dec 08 11:30
customer1	demo-workload-1	chatgpt.com	chrome.exe	12	Dec 08 11:32
customer1	demo-workload-1	chatgpt.com	msedge.exe	12	Dec 08 11:30
customer1	demo-workload-1	copilot.microsoft.com	chrome.exe	4	Dec 08 11:28
customer1	AA-Win11-xdr-03	copilot.microsoft.com	chrome.exe	2	Dec 09 18:37
customer1	AA-Win11-xdr-03	huggingface.co	msedge.exe	2	Dec 09 18:37
customer1	AA-Win11-xdr-03	copilot.microsoft.com	msedge.exe	2	Dec 09 18:36
customer1	AA-Win11-xdr-03	quillbot.com	msedge.exe	2	Dec 09 18:37

More

© Acronis International GmbH, 2003-2026

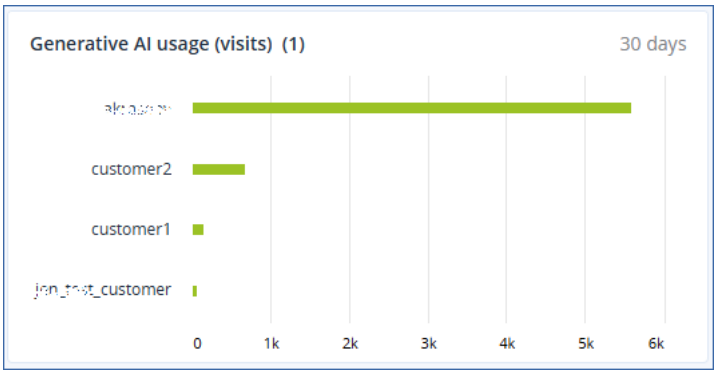
Utilisation de l'intelligence artificielle générative (visites par terminal)

Ce widget est disponible au niveau client. Il montre les statistiques de l'utilisation de l'intelligence artificielle générative par terminal.



Utilisation de l'intelligence artificielle générative (visites par client)

Ce widget est disponible au niveau partenaire. Il montre les statistiques de l'utilisation de l'intelligence artificielle générative par client.



Widget de carte de protection des données

La carte de protection des données vous permet d'obtenir des informations détaillées sur le nombre, la taille, l'emplacement et le statut de protection de tous les fichiers que vous considérez importants (en fonction de leurs extensions de fichier). La carte fournit une vue en arbre, et vous pouvez développer et réduire l'arborescence.

Remarque
L'option **Carte de protection des données** est désactivée par défaut dans les plans de protection nouvellement créés.

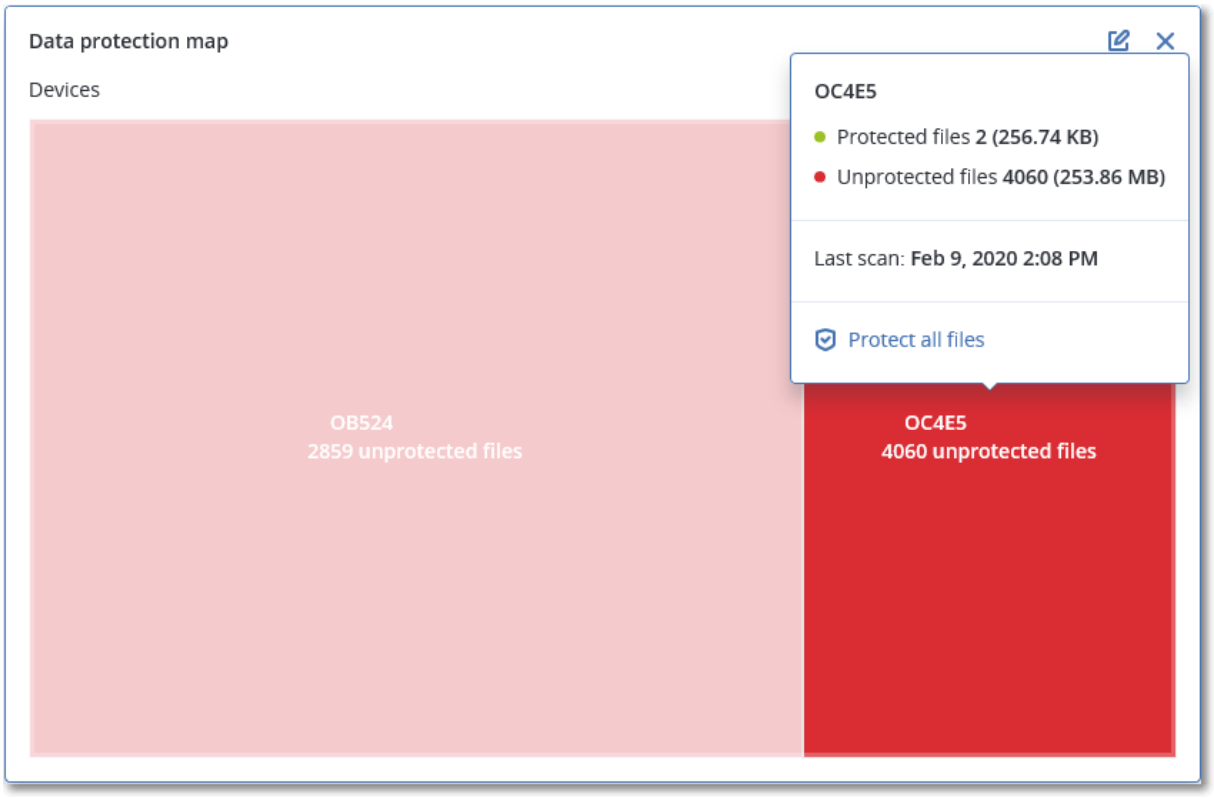
La taille de chaque bloc dans la carte dépend du nombre total et de la taille des fichiers qui appartiennent au client, à l'unité d'organisation ou à l'ordinateur que le bloc représente.

© Acronis International GmbH, 2003-2026

Les blocs peuvent indiquer le statut de protection des fichiers dans l'entité qu'ils représentent. Le statut est basé sur le plan de sauvegarde actuellement appliqué sur l'entité (emplacement ou ordinateur) :

- **Élevé** – tous les fichiers avec les extensions spécifiées par vous sont sauvegardés.
- **Moyenne** – 1-20% des fichiers ne sont pas sauvegardés.
- **Faible** – 21-50% des fichiers ne sont pas sauvegardés.
- **Critique** – 51-100% des fichiers ne sont pas sauvegardés.

Sur le tableau de bord de surveillance d'un tenant client, dans le widget Carte de protection des données, vous pouvez trouver des informations sur le statut de protection des fichiers importants par ordinateur.



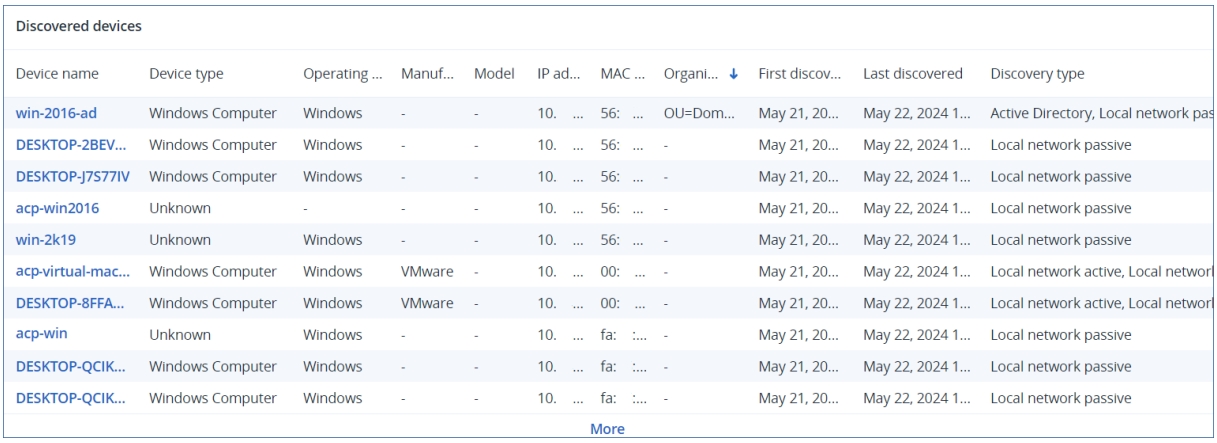
Vous pouvez survoler chaque bloc coloré pour afficher plus d'informations sur le nombre de fichiers non protégés et leur emplacement. Pour les protéger, cliquez sur **Protéger tous les fichiers**.

Vous pouvez aussi télécharger un rapport détaillé au format CSV.

Widget Terminaux découverts

Le widget de tableau **Terminaux découverts** affiche des informations détaillées sur les terminaux des réseaux de l'organisation qui ont été découverts par analyse active et passive. Les informations sur les terminaux incluent le type de terminal, son fabricant, le système d'exploitation, l'adresse IP, l'adresse MAC, la date de la découverte, etc.

© Acronis International GmbH, 2003-2026



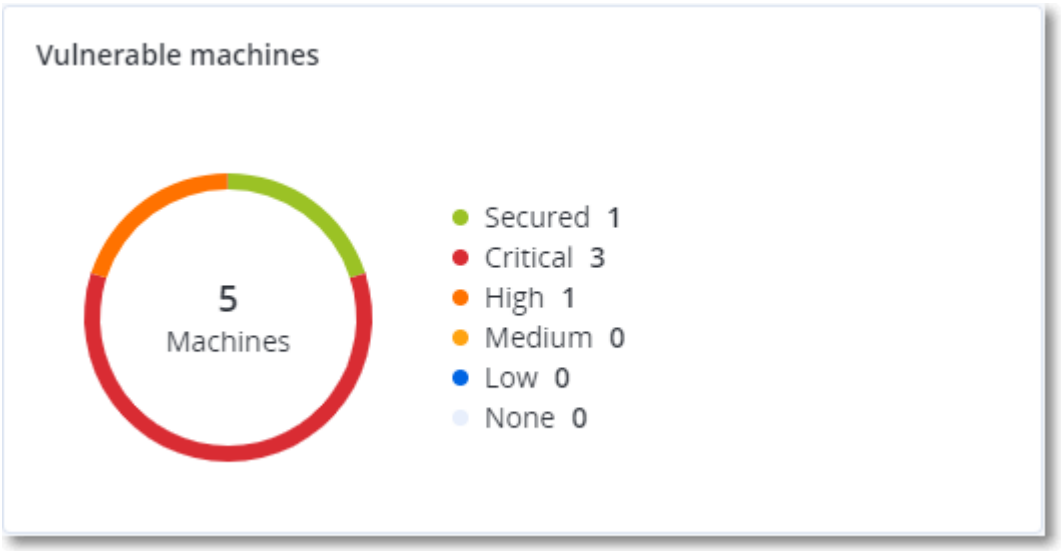
Widgets d'évaluation des vulnérabilités

Machines vulnérables

Ce widget affiche les ordinateurs vulnérables en les classant en fonction de la gravité de leur vulnérabilité.

La vulnérabilité découverte peut présenter l'un des niveaux de gravité suivants, d'après le système d'évaluation des vulnérabilités (CVSS) v3.0 :

- Sécurisé : aucune vulnérabilité n'a été trouvée
- Critique : 9,0 – 10,0 CVSS
- Élevé : 7,0 – 8,9 CVSS
- Moyen : 4,0 – 6,9 CVSS
- Faible : 0,1 – 3,9 CVSS
- Aucun : 0,0 CVSS

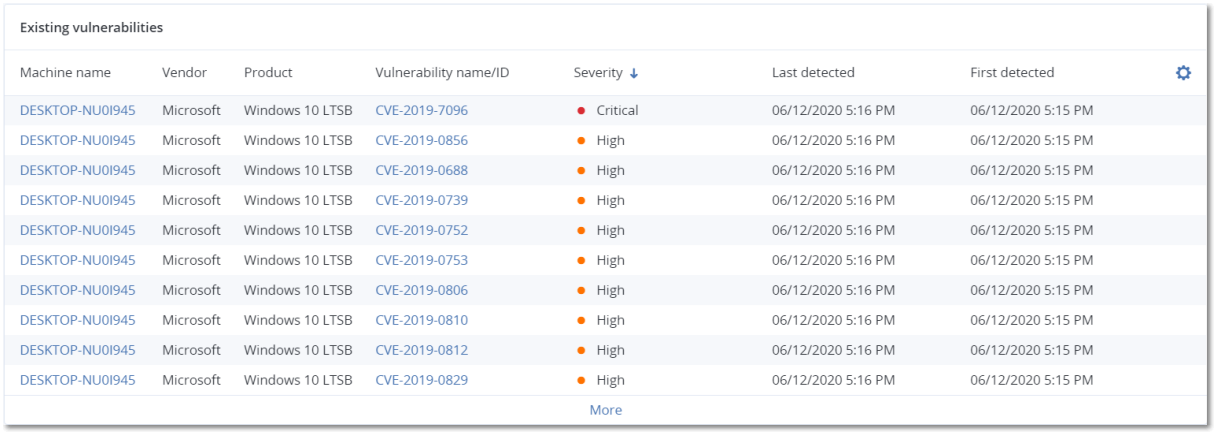


© Acronis International GmbH, 2003-2026

Vulnérabilités existantes

Ce widget affiche les vulnérabilités existant actuellement sur les machines. Dans le widget **Vulnérabilités existantes**, il existe deux colonnes affichant la date et l'heure de la dernière modification :

- **Première détection** : date et heure à laquelle une vulnérabilité a initialement été détectée sur une machine.
- **Dernière détection** : date et heure à laquelle une vulnérabilité a été détectée sur une machine pour la dernière fois.



Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

Widgets d'installation des correctifs

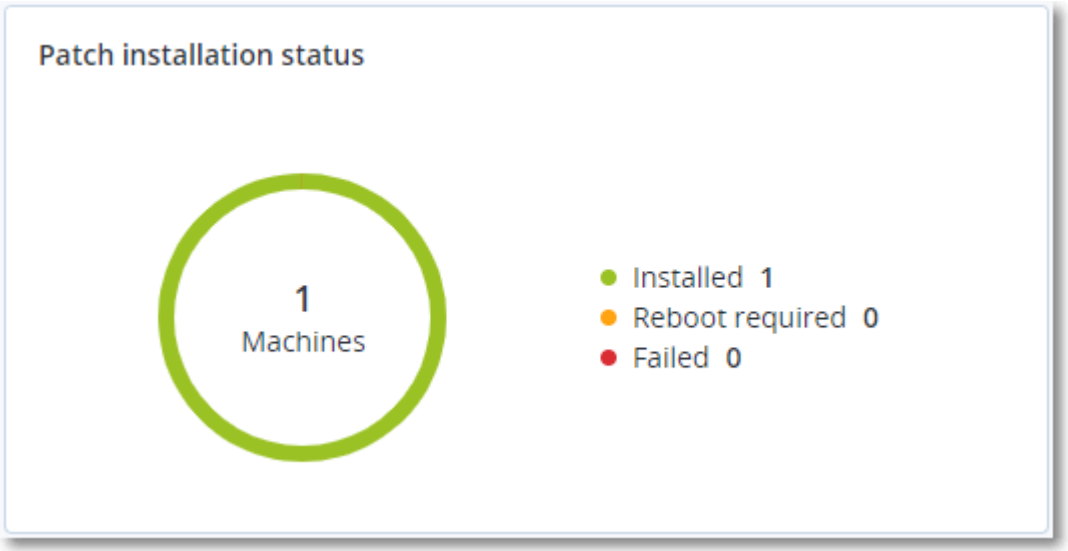
Il existe quatre widgets en lien avec la fonctionnalité de gestion des correctifs.

Statut d'installation des correctifs

Ce widget affiche le nombre de machines, en les regroupant par statut d'installation des correctifs.

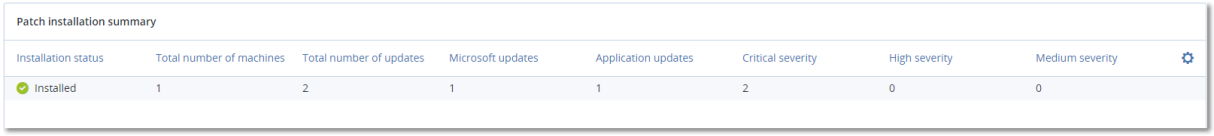
- **Installé :** tous les correctifs disponibles sont installés sur une machine.
- **Redémarrage nécessaire :** après l'installation des correctifs, un redémarrage est requis pour une machine.
- **Échec :** l'installation des correctifs sur une machine a échoué.

© Acronis International GmbH, 2003-2026



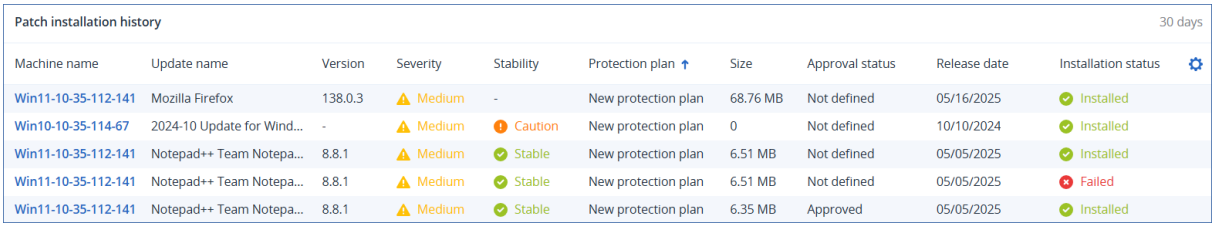
Résumé d'installation des correctifs

Ce widget affiche le résumé des correctifs sur les machines, en les regroupant par statut d'installation des correctifs.



Historique d'installation des correctifs

Ce widget affiche des informations détaillées au sujet des correctifs sur les machines.

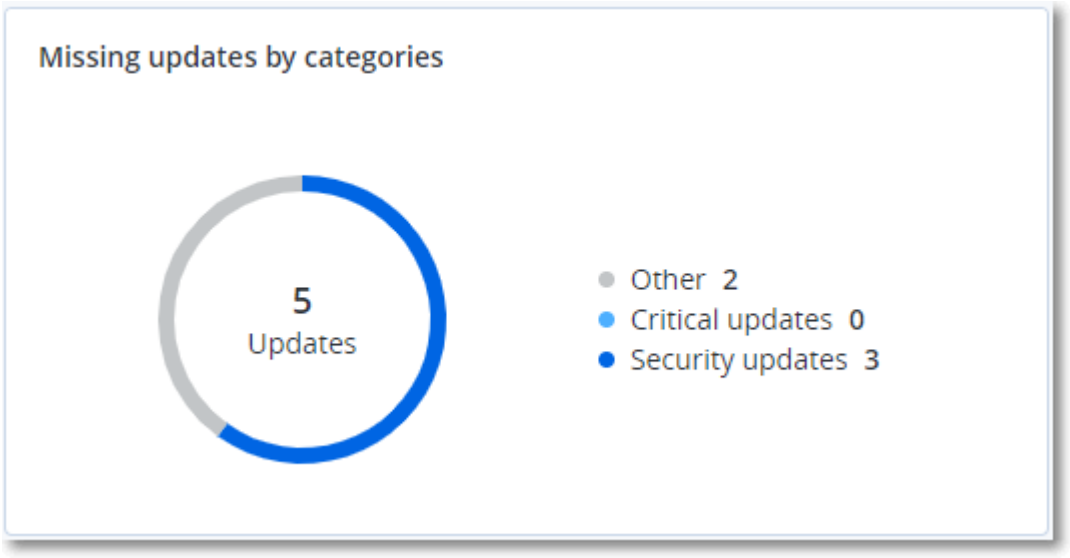


Mises à jour manquantes, par catégorie

Ce widget affiche le nombre de mises à jour manquantes, en les classant par catégorie Les catégories suivantes sont répertoriées :

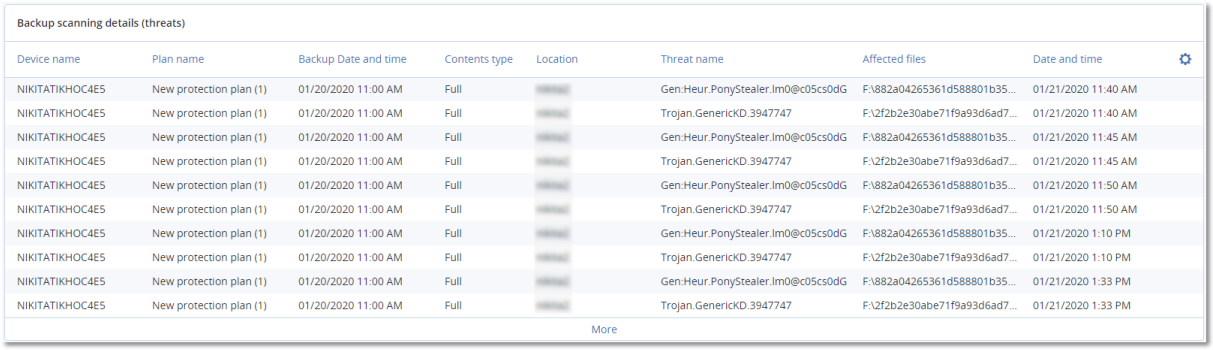
- Mises à jour de sécurité
- Mises à jour critiques
- Autre

© Acronis International GmbH, 2003-2026



Détails de l'analyse de la sauvegarde

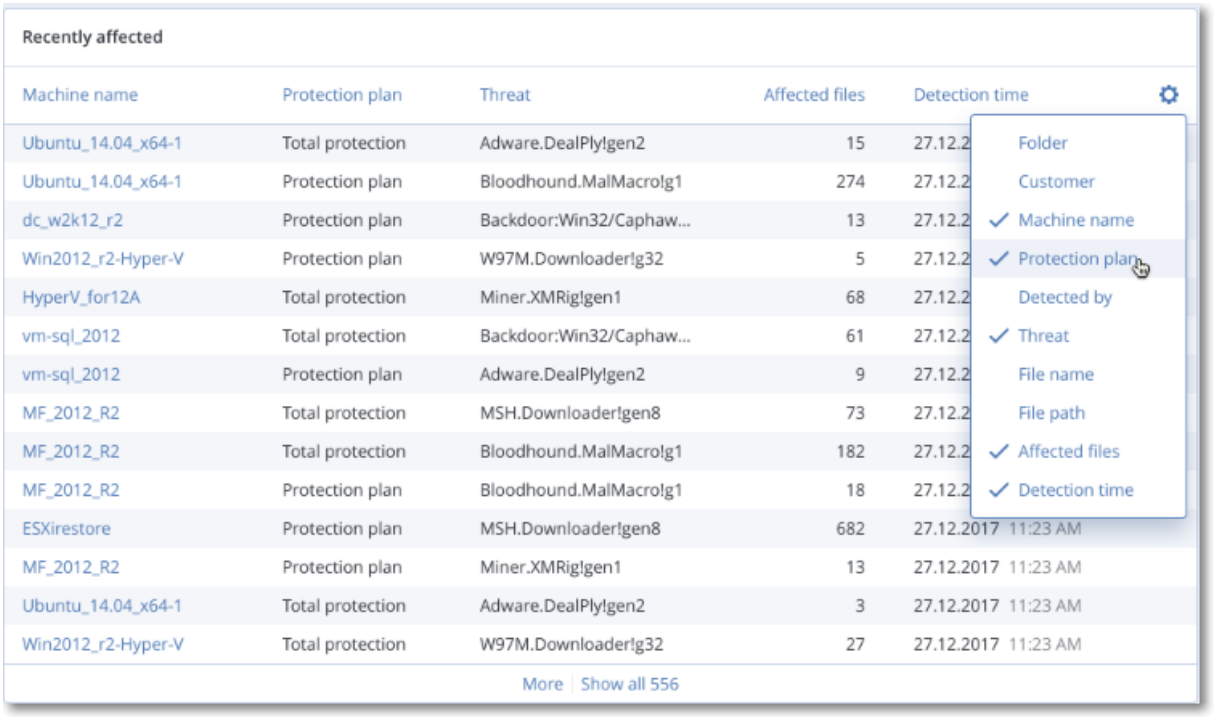
Ce widget affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.



Affectés récemment

Ce widget montre des informations détaillées au sujet des ressources touchées par des menaces telles que des virus, des malwares et des ransomwares. Vous y trouverez des informations concernant les menaces détectées, l'heure de détection et le nombre de fichiers touchés.

© Acronis International GmbH, 2003-2026



Téléchargement de données pour les ressources récemment affectées

Vous pouvez télécharger les données pour les ressources récemment affectées, générer un fichier CSV et l'envoyer aux destinataires que vous spécifiez.

Pour télécharger les données pour les ressources récemment affectées

1. Dans le widget **Affectés récemment**, cliquez sur **Télécharger les données**.
2. Dans le champ **Période**, saisissez le nombre de jours pendant lequel vous souhaitez télécharger des données. Le nombre maximum de jours que vous pouvez entrer est 200.
3. Dans le champ **Destinataires**, saisissez l'adresse e-mail de toutes les personnes qui recevront un e-mail avec un lien pour télécharger le fichier CSV.
4. Cliquez sur **Télécharger**.

   Le système commence à générer le fichier CSV avec les données pour les ressources qui ont été affectées au cours de la période que vous avez spécifiée. Quand le fichier CSV est prêt, le système envoie un e-mail aux destinataires. Chaque destinataire peut ensuite télécharger le fichier CSV.

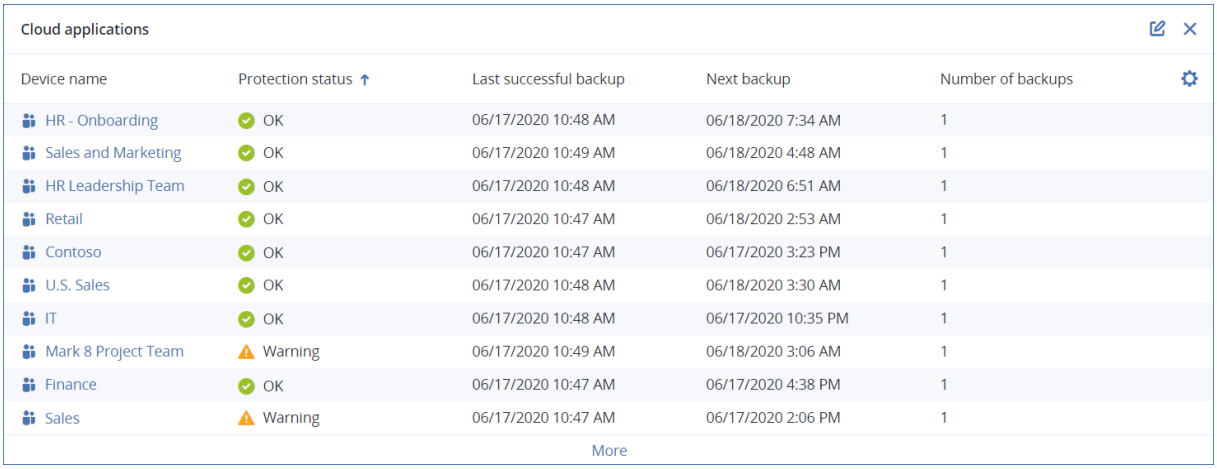
Applications dans le Cloud

Ce widget affiche des informations détaillées concernant les ressources de Cloud à Cloud :

- Utilisateurs Microsoft 365 (boîte aux lettres, OneDrive)
- Groupes Microsoft 365 (boîte aux lettres, site de groupe)
- Dossiers publics Microsoft 365
- Collections de sites Microsoft 365

© Acronis International GmbH, 2003-2026

- Microsoft 365 Teams
- Utilisateurs Google Workspace (Gmail, Google Drive)
- Drive partagés Google Workspace



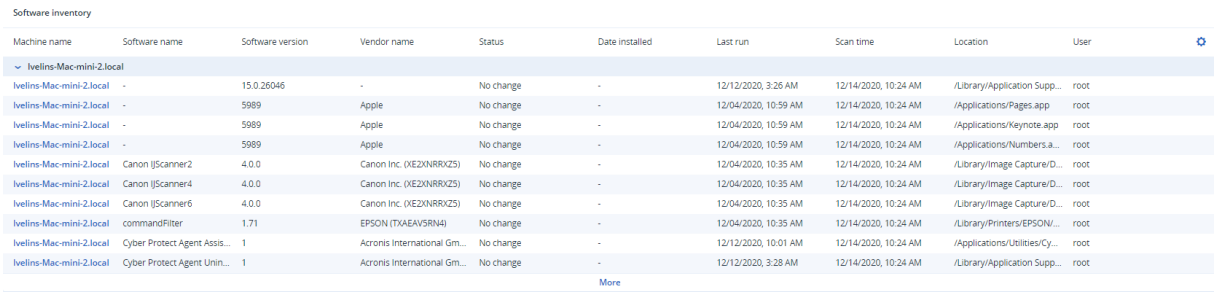
Vous trouverez des ressources de Cloud à Cloud supplémentaires dans les widgets suivants :

- Activités
- Liste des activités
- 5 dernières alertes
- Historique des alertes
- Résumé des alertes actives
- Résumé de l'historique des alertes
- Détails de l'alerte active
- Résumé des emplacements

Widgets de logiciels

Widget d'inventaire du logiciel

Le widget de tableau **Inventaire du logiciel** contient des informations détaillées concernant tout le logiciel installé sur les terminaux physiques Windows et macOS de votre organisation.

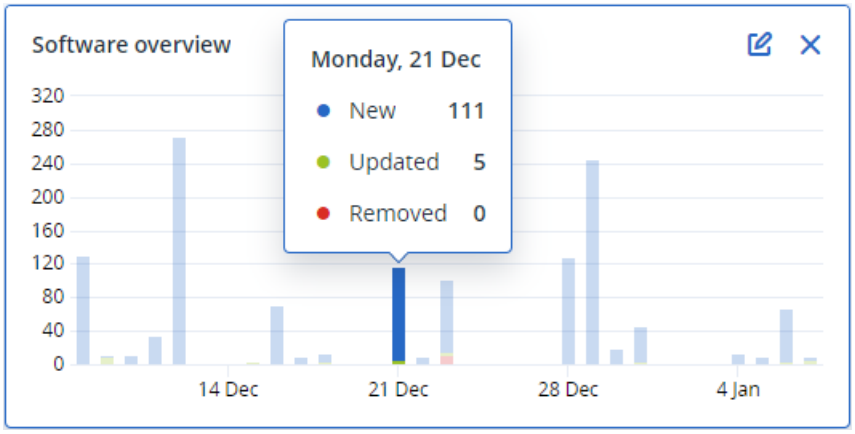


© Acronis International GmbH, 2003-2026

Vous pouvez filtrer les informations dans le widget par nom d'ordinateur, nom de logiciel, nom de fournisseur et statut.

Remarque
Dans les filtres **Nom de la machine**, **Nom du logiciel** et **Nom du fournisseur**, vous pouvez sélectionner jusqu'à 20 valeurs.

Le widget **Aperçu du logiciel** contient le nombre de nouvelles applications ou d'applications mises à jour et supprimées sur les terminaux physiques Windows et macOS de votre organisation sur une période donnée (7 jours, 30 jours ou le mois en cours).



Lorsque vous passez le pointeur sur une barre en particulier, une infobulle contenant les informations suivantes s'affiche :

Nouvelles – le nombre d'applications nouvellement installées.

Mises à jour – le nombre d'applications mises à jour.

Supprimées – le nombre d'applications supprimées.

Lorsque vous cliquez sur la partie de la barre correspondant à un certain statut, vous êtes redirigé vers la page **Gestion de logiciel** -> **Inventaire du logiciel**. Les informations de cette page sont filtrées en fonction de la date et du statut correspondants.

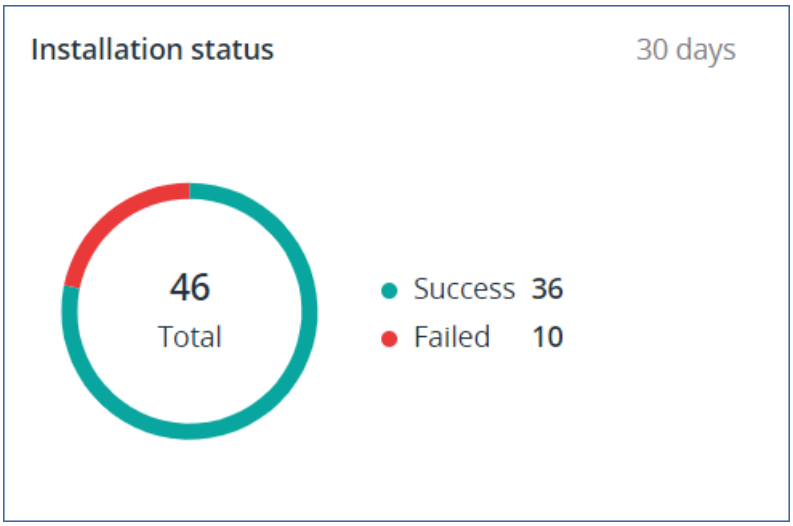
Vous pouvez filtrer les informations dans le widget par nom de terminal.

Remarque
Dans le filtre **Nom du terminal**, vous pouvez sélectionner jusqu'à 20 valeurs.

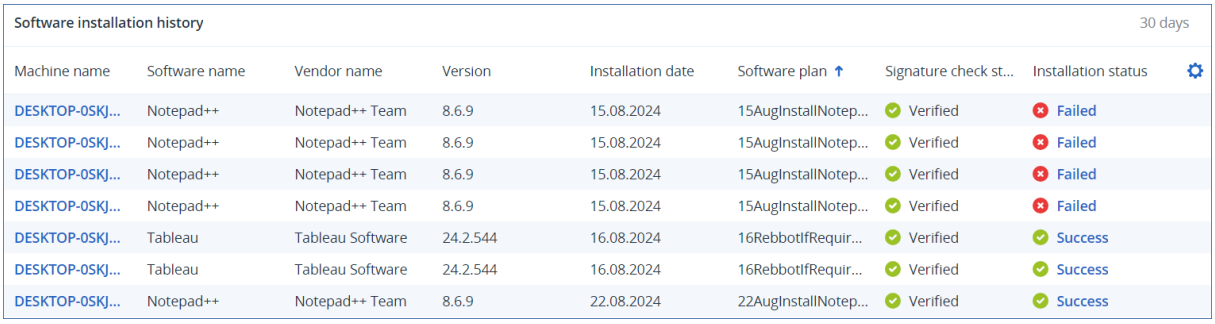
Widgets d'installation de logiciels

Le widget **Statut d'installation** affiche le nombre total d'activités d'installation, regroupées par statut. En cliquant sur un segment du graphique en anneau, vous êtes redirigé vers la page **Activités**, où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.

© Acronis International GmbH, 2003-2026



Le widget **Historique des installations de logiciels** fournit des informations détaillées sur le statut des installations à distance de logiciels sur vos terminaux gérés. En cliquant sur un statut dans la colonne **Statut d'installation**, vous êtes redirigé vers la page **Activités**, où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.

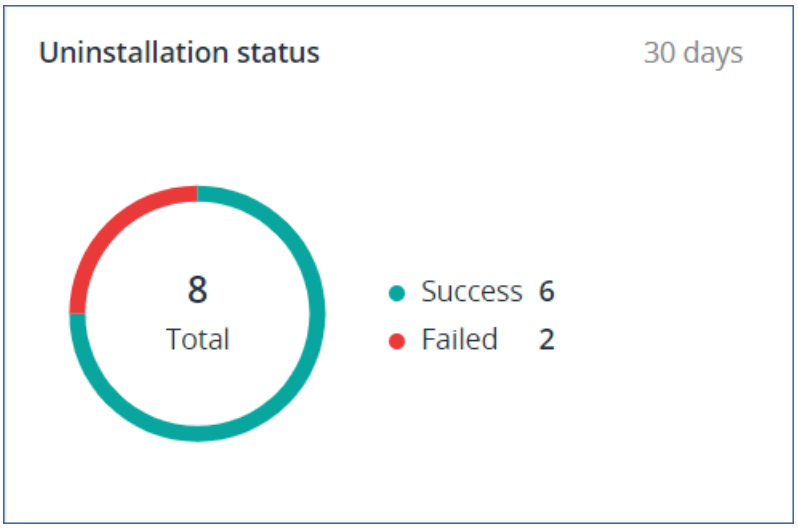


Machine name	Software name	Vendor name	Version	Installation date	Software plan	Signature check st...	Installation status
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Tableau	Tableau Software	24.2.544	16.08.2024	16RebbotIfRequir...	Verified	Success
DESKTOP-0SKJ...	Tableau	Tableau Software	24.2.544	16.08.2024	16RebbotIfRequir...	Verified	Success
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	22.08.2024	22AugInstallNotep...	Verified	Success

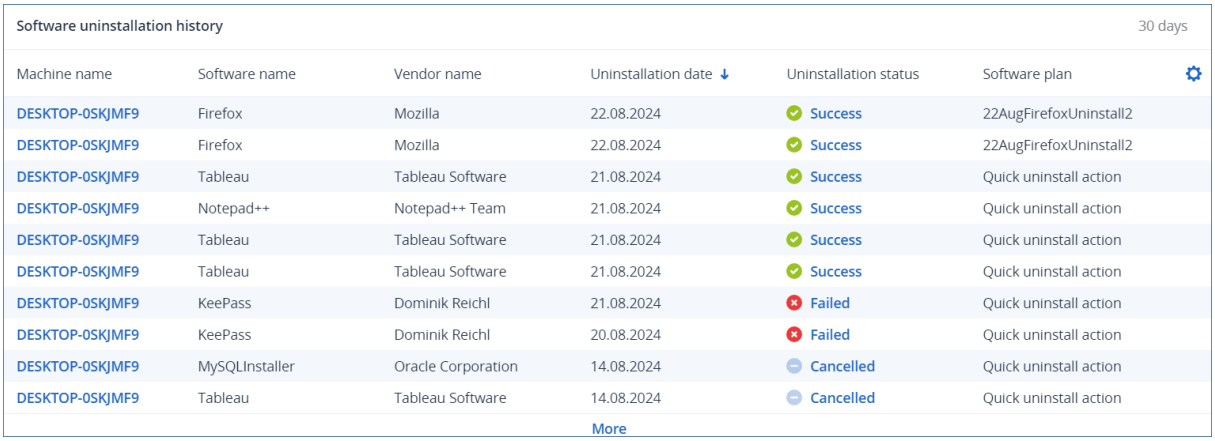
Widgets de désinstallation des logiciels

Le widget **Statut de désinstallation** affiche le nombre total d'activités de désinstallation, regroupées par statut. En cliquant sur un segment du graphique en anneau, vous êtes redirigé vers la page **Activités**, où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.

© Acronis International GmbH, 2003-2026



Le widget **Historique des désinstallations de logiciels** fournit des informations détaillées sur le statut des désinstallations à distance de logiciels sur vos terminaux gérés. En cliquant sur un statut dans la colonne **Statut de désinstallation**, vous êtes redirigé vers la page **Activités**, où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.


Software uninstallation history — 30 days

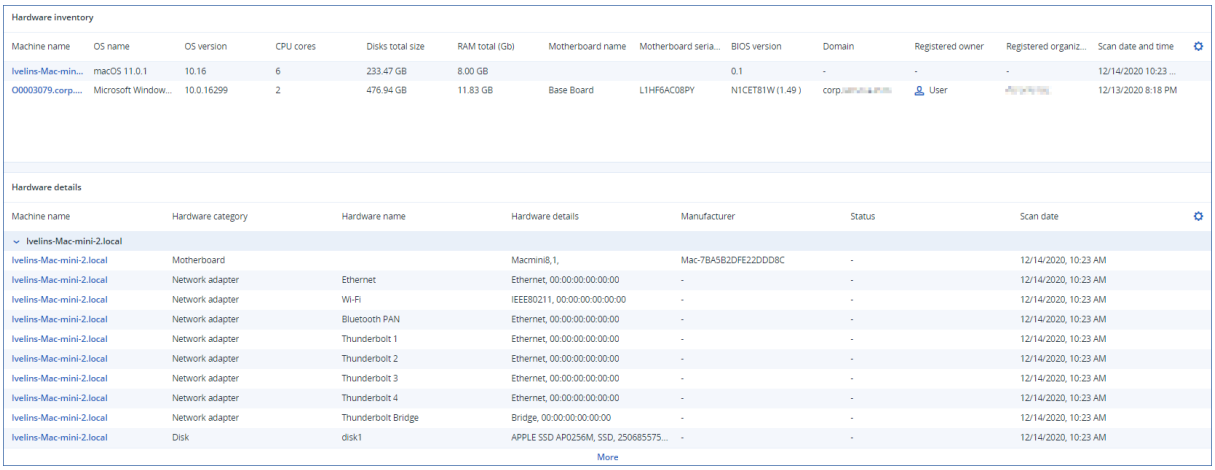
Machine name	Software name	Vendor name	Uninstallation date ↓	Uninstallation status	Software plan
DESKTOP-0SKJMF9	Firefox	Mozilla	22.08.2024	Success	22AugFirefoxUninstall2
DESKTOP-0SKJMF9	Firefox	Mozilla	22.08.2024	Success	22AugFirefoxUninstall2
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Notepad++	Notepad++ Team	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	KeePass	Dominik Reichl	21.08.2024	Failed	Quick uninstall action
DESKTOP-0SKJMF9	KeePass	Dominik Reichl	20.08.2024	Failed	Quick uninstall action
DESKTOP-0SKJMF9	MySQLInstaller	Oracle Corporation	14.08.2024	Cancelled	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	14.08.2024	Cancelled	Quick uninstall action

More

Widgets d'inventaire du matériel

Les widgets de tableau **Inventaire du matériel** et **Détails du matériel** contiennent des informations concernant tout le matériel installé sur les terminaux physiques et virtuels Windows et macOS de votre organisation.

© Acronis International GmbH, 2003-2026



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.	User		12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

Le widget de tableau **Modifications apportées au matériel** contient des informations concernant le matériel ajouté, supprimé et modifié sur les terminaux physiques et virtuels Windows et macOS de votre organisation sur une période donnée (7 jours, 30 jours ou le mois en cours).



Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Vous pouvez filtrer les résultats affichés dans les widgets d'inventaire matériel.

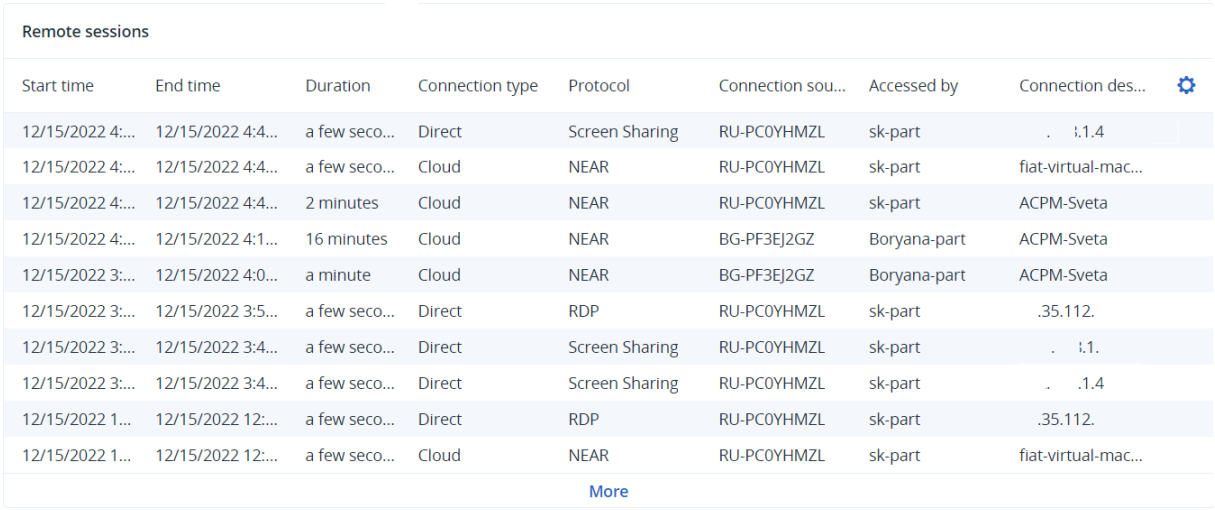
Remarque

Dans le filtre **Nom de la machine**, vous pouvez sélectionner jusqu'à 20 valeurs.

Widget Sessions distantes

Ce widget affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers.

© Acronis International GmbH, 2003-2026


Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

Protection intelligente

Flux de menaces

Le centre opérationnel de cyber protection Acronis (CPOC) génère des alertes de sécurité qui sont envoyées uniquement aux régions géographiques concernées. Ces alertes de sécurité fournissent des informations sur les malwares, les vulnérabilités, les catastrophes naturelles, la santé publique, et d'autres types d'événements mondiaux qui peuvent avoir un impact sur la protection des données. Le flux de menaces vous informe des menaces potentielles et vous permet de les éviter.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Certaines alertes de sécurité peuvent être résolues en suivant un ensemble d'actions spécifiques fournies par les experts de la sécurité. D'autres alertes de sécurité vous informent simplement de menaces à venir, mais ne vous recommandent pas d'actions de réparation.

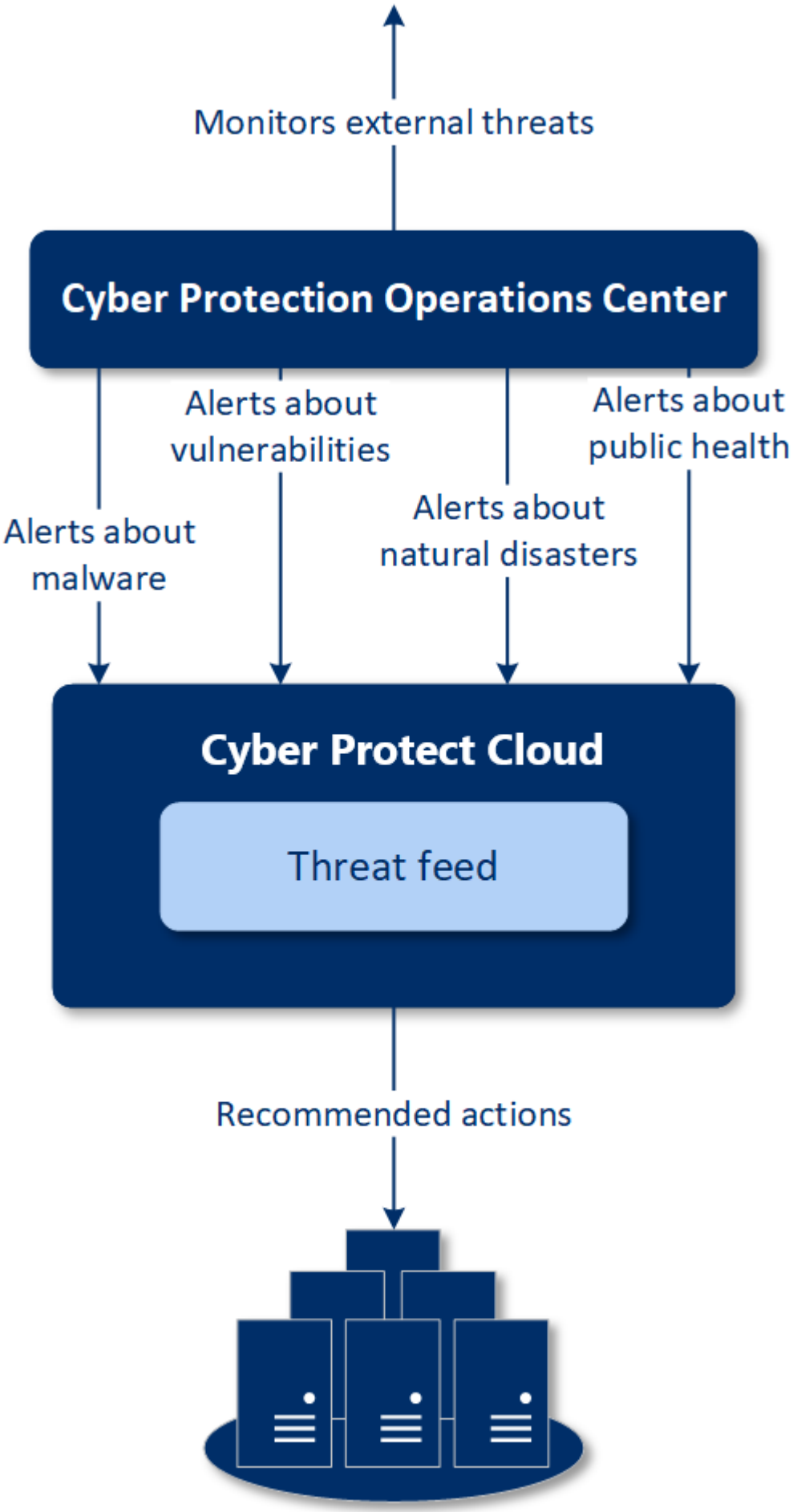
Remarque
Les alertes de malware sont générées uniquement pour les ordinateurs sur lesquels l'agent de protection antimalware est installé.

Fonctionnement

Le centre opérationnel de cyber protection Acronis surveille les menaces externes et génère des alertes concernant les menaces liées aux malwares, aux vulnérabilités, aux catastrophes naturelles et à la santé publique. Vous pourrez consulter toutes ces alertes dans la console Cyber Protect, dans la section **Flux de menaces**. Selon le type d'alerte, vous pouvez exécuter les actions de réparation recommandées respectives.

La procédure principale de ce flux de menaces est illustrée dans le diagramme ci-dessous.

© Acronis International GmbH, 2003-2026



© Acronis International GmbH, 2003-2026

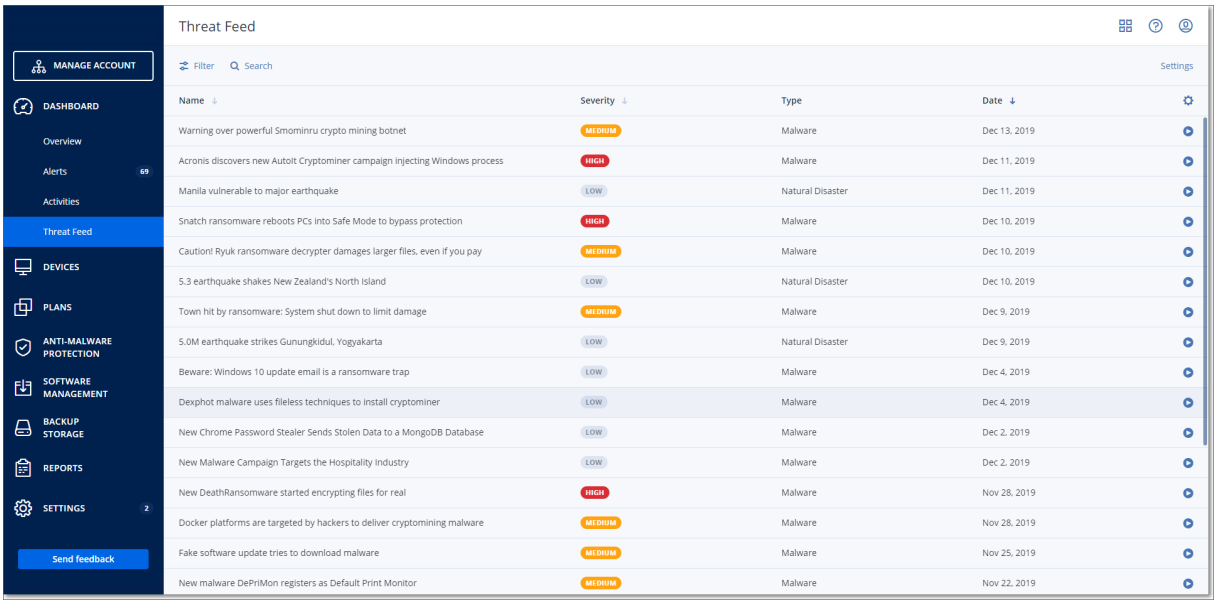
Pour exécuter les actions recommandées suite aux alertes envoyées par le centre opérationnel de cyber protection Acronis, procédez comme suit :

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Flux de menaces** pour vérifier s'il existe des alertes de sécurité.
2. Sélectionnez une alerte dans la liste, puis consultez les détails fournis.
3. Cliquez sur **Démarrer** pour lancer l'assistant.
4. Sélectionnez les actions que vous souhaitez effectuer, ainsi que les machines auxquelles ces actions doivent être appliquées. Les actions suivantes peuvent être suggérées :
   - **Évaluation des vulnérabilités :** pour analyser les machines à la recherche de vulnérabilités.
   - **Gestion des correctifs :** pour installer des correctifs sur les machines sélectionnées.
   - **Protection antimalware :** pour exécuter une analyse complète des machines sélectionnées.

     Remarque
     Cette action est disponible uniquement pour les machines sur lesquelles l'agent de protection antimalware est installé.

   - **Sauvegarde de machines protégées ou non protégées :** pour sauvegarder des ressources protégées/non protégées.
     Si aucune sauvegarde n'existe déjà pour la ressource (dans tous les emplacements accessibles, cloud et locaux) ou si les sauvegardes existantes sont chiffrées, le système crée une sauvegarde complète avec le format de nom suivant :
     `%workload_name%-Remediation`
     Par défaut, la destination de la sauvegarde est le stockage Cyber Protect Cloud, mais vous pouvez configurer un autre emplacement avant de commencer l'opération.
     Si une sauvegarde non chiffrée existe déjà, le système crée une sauvegarde incrémentielle dans l'archive existante.
5. Cliquez sur **Démarrer**.
6. Sur la page **Activités**, vérifiez que l'activité a bien été effectuée.

© Acronis International GmbH, 2003-2026



Suppression de toutes les alertes

Le nettoyage automatique du flux des menaces est effectué après les périodes suivantes :

- Catastrophes naturelles : 1 semaine
- Vulnérabilités : 1 mois
- Malwares : 1 mois
- Santé publique : 1 semaine

Carte de la protection des données

Avec la carte de protection des données, vous pouvez :

- Obtenez des informations détaillées concernant les données stockées (classification, emplacements, statut de protection et informations supplémentaires) sur vos ressources.
- Vérifiez si les données sont protégées. Les données sont considérées comme protégées si un plan de protection avec le module de sauvegarde activé est appliqué à la ressource.
- Effectuer des actions relatives à la protection des données.

Remarque
L'option **Carte de protection des données** est désactivée par défaut dans les plans de protection nouvellement créés.

Fonctionnement

1. En premier lieu, vous créez un plan de protection avec le module Carte de la protection des données activé.

© Acronis International GmbH, 2003-2026

2. Ensuite, une fois le plan exécuté et vos données découvertes et analysées, vous obtiendrez une représentation visuelle de la protection des données dans le widget Carte de la protection des données.

Vous pouvez également accéder à **Terminaux** > **Carte de la protection des données** et y trouver des informations concernant les fichiers non protégés par terminal.

Vous pouvez prendre des mesures pour protéger les fichiers non protégés détectés sur les terminaux.

Gestion des fichiers non protégés détectés

Pour protéger les fichiers importants qui ont été détectés comme non protégés, procédez comme suit :

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Carte de la protection des données**.
   Dans la liste des terminaux, vous trouverez des informations générales concernant le nombre de fichiers non protégés, la taille de ces fichiers par terminal, ainsi que la date de dernière découverte.
   Pour protéger les fichiers sur une machine particulière, cliquez sur l'icône en forme de points de suspension, puis sur **Protéger tous les fichiers**. Vous serez redirigé vers la liste de plans dans laquelle vous pouvez créer un plan de protection avec le module de sauvegarde activé.
   Pour supprimer de la liste le terminal particulier qui possède des fichiers non protégés, cliquez sur **Masquer jusqu'à la prochaine découverte de données**.
2. Pour afficher des informations plus détaillées sur les fichiers non protégés sur un terminal en particulier, cliquez sur le nom du terminal.
   Vous verrez le nombre de fichiers non protégés par extension de fichier et par emplacement. Dans le champ de recherche, définissez les extensions de fichier pour lesquelles vous souhaitez obtenir des informations relatives aux fichiers non protégés.
3. Pour protéger les fichiers non protégés, cliquez sur **Protéger tous les fichiers**. Vous serez redirigé vers la liste de plans dans laquelle vous pouvez créer un plan de protection avec le module de sauvegarde activé.

Pour obtenir des informations relatives aux fichiers non protégés sous la forme d'un rapport, cliquez sur **Télécharger le rapport détaillé au format CSV**.

Paramètres de la carte de protection des données

Pour apprendre à créer un plan de protection avec le module de carte de protection des données, reportez-vous à la section « Création d'un plan de protection ».

Remarque
L'option **Carte de protection des données** est désactivée par défaut dans les plans de protection nouvellement créés.

Vous pouvez définir les paramètres suivants pour le module de carte de protection des données.

© Acronis International GmbH, 2003-2026

Planification

Vous pouvez définir différents paramètres afin de créer le planning selon laquelle la tâche relative à la carte de protection des données sera effectuée.

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements suivants	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.

© Acronis International GmbH, 2003-2026

Champs	Description
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte utilisateur dont la connexion au système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez**

© Acronis International GmbH, 2003-2026

Champs	Description
	quand même la tâche au bout de : spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

Extensions et règles d'exception

Dans l'onglet **Extensions**, vous pouvez définir la liste des extensions de fichier qui seront considérées comme importantes lors de la découverte de données, et dont le statut de protection sera vérifié. Pour définir des extensions, utilisez le format suivant :

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Dans l'onglet **Règles d'exception**, vous pouvez définir les fichiers et dossiers dont le statut de protection ne doit pas être vérifié lors de la découverte de données.

- **Fichiers et dossiers cachés :** si cette option est sélectionnée, les fichiers et dossiers cachés seront ignorés lors de l'examen des données.
- **Fichiers et dossiers système :** si cette option est sélectionnée, les fichiers et dossiers système seront ignorés lors de l'examen des données.

Onglet Activités

L'onglet **Activités** offre une vue d'ensemble des activités des 90 derniers jours.

Pour filtrer les activités dans le tableau de bord

1. Dans le champ **Nom du terminal**, spécifiez l'ordinateur sur lequel l'activité est exécutée.
2. Dans la liste déroulante **Statut**, sélectionnez le statut. Par exemple, « a réussi », « a échoué », « en cours », « annulée ».
3. Dans la liste déroulante **Actions à distance**, sélectionnez l'action. Par exemple, application de plan, suppression de sauvegardes, installation de mises à jour logicielles.
4. Dans le champ **Plus récent**, définissez la période d'activités. Par exemple, les activités les plus récentes, les activités des dernières 24 heures ou les activités pendant une période spécifique au cours des 90 derniers jours.
5. Si vous accédez à l'onglet **Activités** en tant qu'administrateur partenaire, vous pouvez filtrer les activités pour un client spécifique que vous gérez.

Pour personnaliser la vue de l'onglet **Activités**, cliquez sur l'icône en forme d'engrenage, puis sélectionnez les colonnes que vous souhaitez afficher. Pour consulter la progression des activités en temps réel, sélectionnez la case **Actualiser automatiquement**.

Pour annuler une activité en cours d'exécution, cliquez sur son nom, puis, dans l'écran **Détails**, cliquez sur **Annuler**.

© Acronis International GmbH, 2003-2026

Vous pouvez effectuer une recherche parmi les activités répertoriées selon les critères suivants :

- Nom du terminal
  Il s'agit de l'ordinateur sur lequel l'activité est exécutée.
- Démarrée par
  Il s'agit du compte qui a démarré l'activité.

Les activités Bureau à distance peuvent être filtrées à l'aide des propriétés suivantes :

- Création du plan
- Application du plan
- Révocation du plan
- Suppression du plan
- Connexion à distance
  - Connexion Bureau à distance dans le cloud via RDP
  - Connexion Bureau à distance dans le cloud via NEAR
  - Connexion Bureau à distance dans le cloud via le partage d'écran Apple
  - Connexion Bureau à distance via le client Web
  - Connexion Bureau à distance via Assistance rapide
  - Connexion Bureau à distance directe via RDP
  - Connexion Bureau à distance directe via le partage d'écran Apple
  - Transfert de fichiers
  - Transfert de fichiers via Assistance rapide
- Action à distance
  - Arrêt d'une ressource
  - Redémarrage d'une ressource
  - Déconnexion d'un utilisateur distant sur la ressource
  - Vidage de la corbeille d'un utilisateur sur la ressource
  - Mise en veille d'une ressource

Cyber Protect Monitor

Vous pouvez installer Cyber Protect Monitor en tant que composant supplémentaire que vous sélectionnez lors de l'installation de l'agent pour Windows ou de l'agent pour Mac. Cyber Protect Monitor affiche des informations sur l'état de protection de l'ordinateur sur lequel l'agent pour Windows ou l'agent pour Mac est installé.

Vous pouvez utiliser Cyber Protect Monitor pour configurer le chiffrement de sauvegarde et les paramètres du serveur proxy, et pour discuter avec les techniciens.

Cyber Protect Monitor prend en charge les systèmes d'exploitation suivants.

© Acronis International GmbH, 2003-2026

- Avec l'agent pour Windows
  - Windows 10 version 1809 et ultérieure
  - Windows Server 2019 et versions ultérieures
- Avec l'agent pour Windows (hérité)
  - Windows 7 et versions ultérieures
  - Windows Server 2008 R2 et versions ultérieures
- Avec Agent pour Mac
  - Toutes les versions de macOS prises en charge par l'Agent pour Mac, à l'exception de macOS 10.x et macOS 11.x.

Lorsque l'agent pour File Sync & Share est installé sur l'ordinateur, Cyber Protect Monitor permet d'accéder au service File Sync & Share. La fonctionnalité File Sync & Share est accessible après une phase d'intégration obligatoire au cours de laquelle les utilisateurs se connectent à leur propre compte File Sync & Share et sélectionnent un dossier de synchronisation personnel. Pour plus d'informations sur l'agent pour File Sync & Share, voir le guide de l'utilisateur Cloud Cyber Files.

Important
Cyber Protect Monitor est accessible aux utilisateurs qui ne disposent peut-être pas de droits d'administration pour Cyber Protection ou le service File Sync & Share.

Le tableau ci-dessous résume les opérations disponibles pour les utilisateurs ne disposant pas de droits d'administration.

Agents installés	Les utilisateurs peuvent	Les utilisateurs ne peuvent pas
Agent pour Windows ou agent pour Mac	• Appliquer le plan de protection par défaut à leurs ordinateurs • Vérifier l'état de protection de leur ordinateur • Recevoir des notifications de Active Protection • Interrompre temporairement la sauvegarde de leur ordinateur • Configurer les paramètres du serveur proxy • Modifier les paramètres de chiffrement de la sauvegarde	• Appliquer des plans de protection personnalisés • Gérer les plans de protection déjà appliqués

© Acronis International GmbH, 2003-2026

Agents installés	Les utilisateurs peuvent	Les utilisateurs ne peuvent pas
	Avertissement ! La modification des paramètres de chiffrement dans Cyber Protect Monitor écrase les paramètres du plan de protection et affecte toutes les sauvegardes de l'ordinateur. Cette opération peut entraîner l'échec de certains plans de protection. Pour plus d'informations, voir "Chiffrement" (p. 596). Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe. • Discuter avec un technicien	
Agent pour Windows (hérité)	• Appliquer le plan de protection par défaut à leurs ordinateurs • Vérifier l'état de protection de leur ordinateur • Recevoir des notifications de Active Protection • Interrompre temporairement la sauvegarde de leur ordinateur • Configurer les paramètres du serveur proxy • Modifier les paramètres de chiffrement de la sauvegarde **Avertissement !** La modification des paramètres de chiffrement dans Cyber Protect Monitor écrase les paramètres du plan de protection et affecte toutes les sauvegardes de l'ordinateur. Cette opération peut entraîner l'échec de certains plans de protection. Pour plus d'informations, voir "Chiffrement" (p. 596). Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.	• Appliquer des plans de protection personnalisés • Gérer les plans de protection déjà appliqués
Agent pour Windows et agent	• Synchroniser le contenu de leur dossier de synchronisation local et de	• Modifier les types de fichiers qui ne peuvent pas être synchronisés

© Acronis International GmbH, 2003-2026

Agents installés	Les utilisateurs peuvent	Les utilisateurs ne peuvent pas
pour Sync and Share Agent pour Mac et agent pour Sync and Share	leur compte File Sync & Share • Interrompre les opérations de synchronisation • Modifier le dossier de synchronisation • Vérifier les types de fichiers qui ne peuvent pas être synchronisés • Discuter avec un technicien	

Configuration des paramètres de serveur proxy dans Cyber Protect Monitor

Vous pouvez configurer les paramètres de serveur proxy dans Cyber Protect Monitor. La configuration aura une incidence sur tous les agents installés sur l'ordinateur.

Pour configurer les paramètres du serveur proxy

1. Ouvrez Cyber Protect Monitor, puis cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit.
2. Cliquez sur **Paramètres**, puis cliquez sur **Proxy**.
3. Activez le commutateur **Utiliser un serveur proxy**, puis saisissez l'adresse et le port du serveur proxy.
4. [Si l'accès au serveur proxy est protégé par un mot de passe] Activez le commutateur **Mot de passe requis**, puis saisissez le nom d'utilisateur et le mot de passe nécessaires pour accéder au serveur proxy.
   Le mot de passe peut inclure des caractères alphanumériques minuscules et majuscules, ainsi que les caractères spéciaux suivants :
   ```
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` } | { ~
   ```
5. Cliquez sur **Enregistrer**.
   Les paramètres du serveur proxy sont enregistrés dans le fichier `http-proxy.yaml`.

Chats dans Monitor

À partir de votre terminal, vous pouvez discuter avec des techniciens ou des administrateurs dans la console Cyber Protect. De cette manière, vous pouvez bénéficier d'une assistance en temps réel pour les problèmes.

Démarrer un chat dans Cyber Protect Monitor

Vous pouvez utiliser Cyber Protect Monitor pour discuter avec des techniciens du tenant dans lequel votre ressource est enregistrée dans la console Cyber Protect. Vous pouvez démarrer une nouvelle

© Acronis International GmbH, 2003-2026

session de chat ou répondre dans des sessions de chat qui ont été démarrées dans la console. Monitor affiche des notifications de bureau lorsque vous avez de nouveaux messages dans le chat.

Pour démarrer une nouvelle session de chat à partir de la surveillance

1. Ouvrez Cyber Protect Monitor.
2. Cliquez sur l'icône de chat.
   Une fenêtre de chat s'ouvre.
3. Dans le champ de texte, saisissez votre message.
4. Pour envoyer le message, cliquez sur l'icône flèche ou appuyez sur Entrée.
   Votre message est envoyé à la console Cyber Protect. La session de chat sera affectée à un technicien ou un administrateur qui vous aidera.

Remarque
Les sessions de chat sont automatiquement fermées si un utilisateur est inactif pendant 15 minutes.

Actions supplémentaires avec les chats dans Cyber Protect Monitor

Si vous avez une session de chat active dans Cyber Protect Monitor, vous pouvez effectuer les actions suivantes : modifier un message, supprimer un message, rechercher un mot-clé ou un message, ou mettre fin au chat.

Modifier le message

Vous pouvez modifier tout message que vous avez envoyé dans la session de chat.

Pour modifier un message dans la session de chat

1. Dans Monitor, dans la fenêtre de chat, localisez le message que vous souhaitez modifier.
2. Survolez le message, puis cliquez sur l'icône de crayon qui apparaît.
3. Modifiez le message, puis cliquez sur **Enregistrer**.
   Les modifications sont enregistrées. Le message est marqué comme **Édité**.

Supprimer le message

Vous pouvez supprimer tout message que vous avez envoyé dans le chat.

Pour supprimer un message dans la session de chat

1. Dans Monitor, dans la fenêtre de chat, localisez le message que vous souhaitez supprimer.
2. Survolez le message, puis cliquez sur l'icône de la corbeille qui apparaît.
3. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Recherche dans le chat

Vous pouvez rechercher certains messages ou mots clés dans les sessions de chat ou afficher l'historique des chats pour une date spécifique.

© Acronis International GmbH, 2003-2026

Pour effectuer une recherche dans la session de chat

1. Dans Monitor, dans la fenêtre de discussion, cliquez sur l'icône de boucle.
2. [Facultatif] Pour voir l'historique du chat pour une date spécifique, cliquez sur l'icône de calendrier, puis sélectionnez la date.

   Remarque
   Seules les dates pour lesquelles l'historique du chat est disponible sont activées pour la sélection.

   Le système affiche l'historique du chat à partir de la date que vous avez sélectionnée.
3. [Facultatif] Dans le champ de recherche, tapez le mot-clé ou le message que vous souhaitez trouver.
   Le système affiche le nombre de résultats correspondant à la recherche. Vous pouvez utiliser les flèches pour passer au résultat suivant ou précédent.

Terminer le chat

Vous pouvez mettre fin à la session de chat à tout moment.

Pour mettre fin à la session de chat

1. Dans Monitor, ouvrez la fenêtre de discussion.
2. Cliquez sur **Terminer le chat**.
3. Dans la fenêtre de confirmation, cliquez sur **Fin**.
   La session de chat est terminée.

Activation ou désactivation des notifications de chat dans Cyber Protect Monitor

Vous pouvez activer les notifications de chat et voir une notification de bureau lorsque vous recevez de nouveaux messages de chat. En cliquant sur la notification, la fenêtre de chat s'ouvre directement.

Si vous ne souhaitez pas voir les notifications de bureau concernant les nouveaux messages de chat, vous pouvez désactiver les notifications de discussion.

Activer les notifications

Pour activer les notifications de chat

1. Ouvrez Cyber Protect Monitor.
2. Cliquez sur **Paramètres**.
3. Cliquez sur **Notifications de chat**.
4. Sélectionnez **Notifications de bureau**, puis cliquez sur **Enregistrer**.

Désactiver les notifications

© Acronis International GmbH, 2003-2026

Pour désactiver les notifications de chat

1. Ouvrez Cyber Protect Monitor.
2. Cliquez sur **Paramètres**.
3. Cliquez sur **Notifications de chat**.
4. Effacer les **Notifications de bureau**, puis cliquez sur **Enregistrer**.

Rapports

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Un rapport au sujet des opérations peut inclure n'importe quel ensemble de widgets du tableau de bord. Tous les widgets présentent le résumé pour l'ensemble de l'entreprise.

En fonction du type de widget, le rapport inclut les données pour une période ou pour le moment de la navigation ou de la génération de rapport. Consultez "Données rapportées en fonction du type de widget" (p. 382).

Tous les widgets historiques présentent les données pour le même intervalle de temps. Vous pouvez modifier cela dans les paramètres de rapport.

Vous pouvez utiliser des rapports par défaut ou créer un rapport personnalisé.

Vous pouvez télécharger un rapport ou l'envoyer par e-mail au format Excel (XLSX) ou PDF.

L'ensemble de rapports par défaut dépend de l'édition du service Cyber Protection que vous possédez. Les rapports par défaut sont répertoriés ci-dessous :

Nom du rapport	Description
Score #CyberFit par machine	Affiche le score #CyberFit basé sur l'évaluation des indicateurs et des configurations de sécurité pour chaque machine, ainsi que des recommandations d'amélioration.
Alertes	Affiche les alertes survenues pendant une période donnée.
Détails de l'analyse de la sauvegarde	Affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.
Activités quotidiennes	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Carte de la protection des données	Affiche des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants présents sur des machines.
Menaces détectées	Affiche les détails des machines affectées en les classant par nombre de menaces bloquées, ainsi que le nombre de machines saines et vulnérables.

© Acronis International GmbH, 2003-2026

Machines découvertes	Affiche toutes les machines trouvées dans le réseau de l'organisation.
Prévision de l'état de santé du disque	Affiche des prévisions concernant le moment où votre disque dur/SSD tombera en panne, ainsi que l'état actuel des disques.
Vulnérabilités existantes	Affiche les vulnérabilités existantes pour le système d'exploitation et les applications dans votre organisation. Le rapport affiche également les détails des machines affectées dans votre réseau pour chaque produit répertorié.
Protection de l'intelligence artificielle générative	Affiche les informations de synthèse sur la protection de l'intelligence artificielle générative pour une période donnée.
Inventaire du logiciel	Affiche des informations concernant le logiciel installé sur les terminaux de votre entreprise. **Remarque** Le rapport peut contenir jusqu'à 20 ressources à la fois.
Inventaire matériel	Affiche des informations concernant le matériel disponible sur les terminaux de votre entreprise. **Remarque** Le rapport peut contenir jusqu'à 20 ressources à la fois.
Résumé de la gestion des correctifs	Affiche le nombre de correctifs manquants, installés et applicables. Vous pouvez explorer les rapports pour obtenir des informations sur les correctifs manquants/installés, ainsi que sur tous les systèmes
Résumé	Affiche des informations résumées au sujet des terminaux protégés pendant une période donnée.
Activités hebdomadaires	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Sessions distantes	Affiche les informations concernant les sessions Bureau à distance et transfert de fichiers.

Remarque
Les données d'utilisation du stockage local sont signalées uniquement au niveau de l'unité et du tenant client. Les utilisateurs ne reçoivent pas d'informations sur l'utilisation du stockage local dans les rapports récapitulatifs.

Actions relatives aux rapports

Ajouter

Pour ajouter un nouveau rapport

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Au bas de la liste des rapports disponibles, cliquez sur **Ajouter un rapport**.
3. [Pour ajouter un rapport prédéfini] Cliquez sur le nom du rapport prédéfini.
4. [Pour ajouter un rapport personnalisé] Cliquez sur **Personnalisé**, puis ajoutez des widgets au rapport.
5. [Facultatif] Glissez-déplacez les widgets pour les réorganiser.

Affichage

Pour afficher un rapport

- Pour afficher un rapport, cliquez sur son nom.

Modifier

Pour modifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez modifier.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Paramètres**.
4. Modifiez le rapport, puis cliquez sur **Enregistrer**.

Supprimer

Pour supprimer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez supprimer.
3. Dans l'angle supérieur droit de l'écran, cliquez sur l'icône représentant des points de suspension (...), puis sélectionnez **Supprimer le rapport**.
4. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Planification

Pour planifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez planifier.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Paramètres**.
4. A côté de **Planifié**, activez le commutateur.
   - Spécifiez l'adresse e-mail des destinataires.
   - Sélectionnez le format du rapport.

© Acronis International GmbH, 2003-2026

- **Remarque**
  Vous pouvez exporter jusqu'à 1 000 éléments dans un fichier PDF et jusqu'à 10 000 éléments dans un fichier XLSX. Les horodatages des fichiers PDF et XLSX utilisent l'heure locale de votre ordinateur.

- Sélectionnez la langue du rapport.
- Configurez la planification.

5. Cliquez sur **Enregistrer**.

Télécharger

Pour télécharger un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Télécharger**.
4. Sélectionnez le format du rapport.

Un fichier du format sélectionné est téléchargé sur votre ordinateur.

Si vous avez sélectionné **Excel et PDF**, un fichier ZIP est téléchargé sur votre ordinateur.

Envoyer

Pour envoyer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Envoyer**.
4. Spécifiez l'adresse e-mail des destinataires.
5. Sélectionnez le format du rapport.
6. Cliquez sur **Envoyer**.

Exporter la structure

Pour exporter la structure des rapports

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Dans le coin supérieur droit de l'écran, cliquez sur l'icône représentant des points de suspension (...), puis sur **Exporter**.

En conséquence, la structure du rapport est enregistrée sur votre ordinateur en tant que fichier JSON.

Vider les données

© Acronis International GmbH, 2003-2026

Pour vider les données du rapport

Vous pouvez exporter toutes les données d'une période personnalisée, sans les filtrer, vers un fichier CSV et envoyer ce fichier CSV à un destinataire par e-mail. Le fichier CSV ne contient que les données relatives aux widgets inclus dans le rapport.

Remarque
Vous pouvez exporter jusqu'à 150 000 éléments dans un fichier CSV. Les horodatages dans ce fichier CSV utilisent le temps universel coordonné (UTC).

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport dont vous souhaitez vider les données.
3. Dans le coin supérieur droit de l'écran, cliquez sur l'icône représentant des points de suspension (...), puis sur **Vider les données**.
4. Spécifiez l'adresse e-mail des destinataires.
5. Dans la zone **Plage de temps**, spécifiez la période personnalisée pour laquelle vous souhaitez vider les données.

   Remarque
   La préparation des fichiers CSV pour de plus longues périodes prend plus de temps.

6. Cliquez sur **Envoyer**.

Données rapportées en fonction du type de widget

Les widgets du tableau de bord peuvent être classés selon deux catégories, selon le type de données qu'ils présentent :

- Les widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.
- Les widgets qui affichent les données historiques.

Lorsque vous configurez une plage de dates dans les paramètres de rapport afin d'effectuer un vidage mémoire des données d'une certaine période, la plage de dates sélectionnée s'applique uniquement aux widgets qui affichent des données historiques. Elle n'est pas applicable aux widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.

Le tableau suivant énumère les widgets et leurs plages de données.

Nom du widget	Données affichées dans le widget et les rapports
Score #CyberFit par machine	Actuelles
5 dernières alertes	Actuelles

© Acronis International GmbH, 2003-2026

Détails des alertes actives	Actuelles
Résumé des alertes actives	Actuelles
Activités	Historiques
Liste des activités	Historiques
Historique des alertes	Historiques
Statistiques des tactiques d'attaque	Historiques
Détails de l'analyse de la sauvegarde (menaces)	Historiques
État de la sauvegarde	Historiques, dans les colonnes **Total des exécutions** et **Nombre d'exécutions réussies** Actuelles, dans toutes les autres colonnes
URL bloquées	Actuelles
Applications dans le Cloud	Actuelles
Cyberprotection	Actuelles
Carte de la protection des données	Historiques
Terminaux	Actuelles
Terminaux découverts	Actuelles
Vue d'ensemble de l'état de santé du disque	Actuelles
Intégrité de disque par terminaux physiques	Actuelles
Vulnérabilités existantes	Historiques
Modifications apportées au matériel	Historiques
Détails du matériel	Actuelles
Inventaire matériel	Actuelles
Résumé de l'historique des alertes	Historiques
Historique de gravité de l'incident	Historiques
Résumé des emplacements	Actuelles
Mises à jour manquantes, par catégorie	Actuelles
Non protégé	Actuelles

© Acronis International GmbH, 2003-2026

Historique d'installation des correctifs	Historiques
Statut d'installation des correctifs	Historiques
Résumé d'installation des correctifs	Historiques
État de protection	Actuelles
Affectés récemment	Historiques
Sessions distantes	Historiques
Résolution des incidents de sécurité	Historiques
Temps moyen de réparation des incidents de sécurité	Historiques
Inventaire du logiciel	Actuelles
Aperçu du logiciel	Historiques
Statut de la menace	Actuelles
Machines vulnérables	Actuelles
Statut réseau des ressources	Actuelles

© Acronis International GmbH, 2003-2026

Gestion des ressources dans la console Cyber Protect

Cette section décrit le mode de gestion de vos ressources dans la console Cyber Protect.

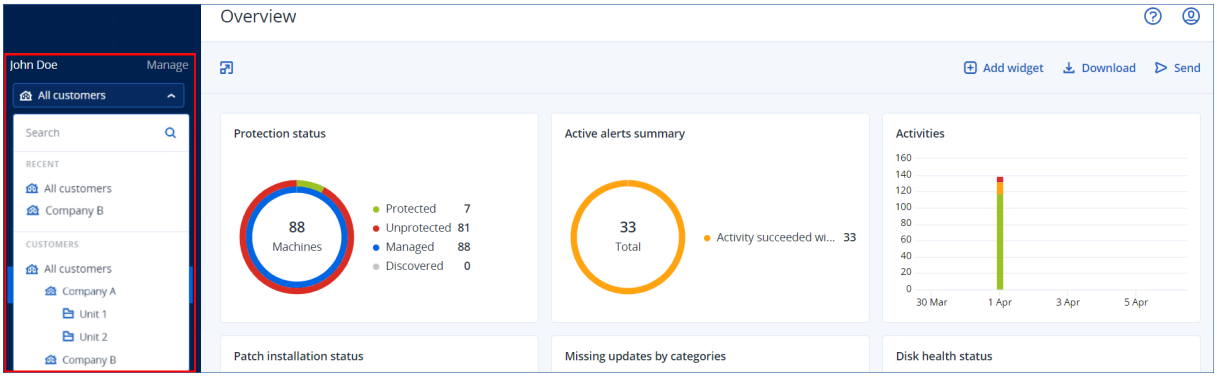
La console Cyber Protect

Dans la console Cyber Protect, vous pouvez gérer les ressources et les plans, modifier les paramètres de protection, configurer des rapports ou examiner votre stockage des sauvegardes.

La console Cyber Protect vous donne accès à des services ou fonctionnalités supplémentaires tels que la solution de synchronisation et de partage de fichiers, la protection antivirus et antimalware et le filtrage des adresses URL, la gestion des correctifs, le contrôle des terminaux et l'évaluation des vulnérabilités. Le type et le nombre de ces services et fonctionnalités varient selon votre licence Cyber Protection.

Pour afficher le tableau de bord qui vous fournit les informations les plus importantes concernant votre protection, accédez à **Surveillance** > **Vue d'ensemble**.

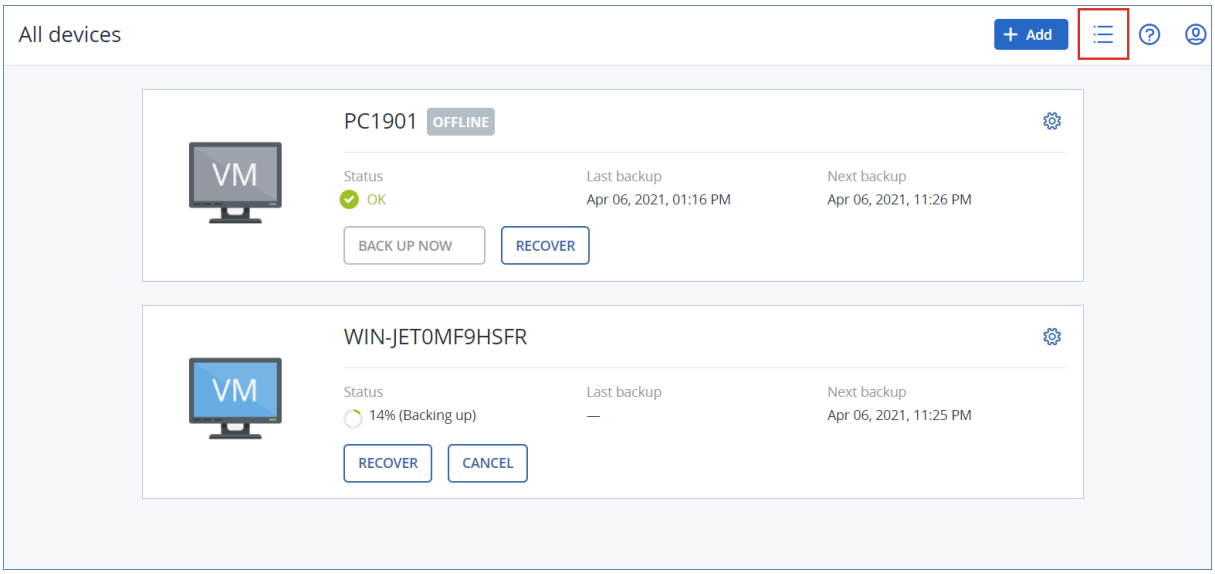
Selon vos autorisations d'accès, vous pouvez gérer la protection d'un ou de plusieurs tenants clients ou divisions dans un tenant. Pour changer de niveau dans la hiérarchie, utilisez la liste déroulante du menu de navigation. Seuls les niveaux auxquels vous avez accès sont affichés. Pour accéder au Portail de gestion, cliquez sur **Gérer**.



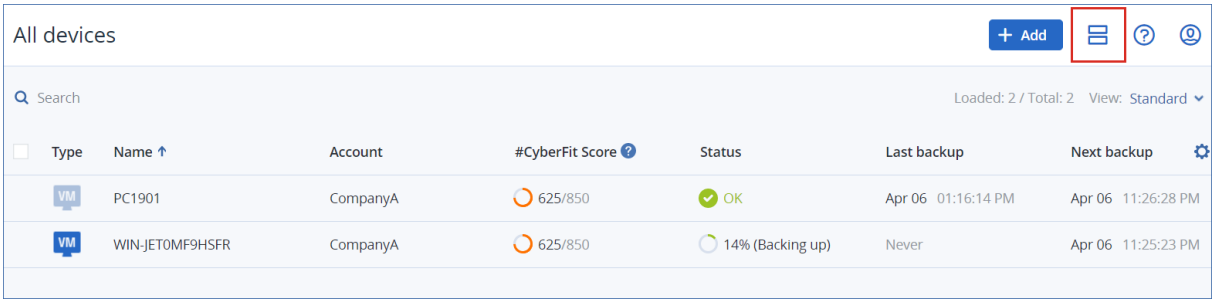
La section **Terminaux** est disponible en mode d'affichage simple et en mode d'affichage tableau. Pour passer de l'un à l'autre, cliquez sur l'icône correspondante dans l'angle supérieur droit.

Le mode d'affichage simple affiche uniquement quelques ressources.

© Acronis International GmbH, 2003-2026



Le mode d'affichage tableau est activé automatiquement lorsque le nombre de ressources devient plus important.



Les deux modes d'affichage donnent accès aux mêmes fonctionnalités et aux mêmes opérations. Ce document explique comment accéder aux différentes opérations depuis le mode d'affichage tableau.

Lorsqu'une ressource passe en ligne ou hors ligne, un certain temps est nécessaire avant que son état soit modifié dans la console Cyber Protect. L'état de la ressource est vérifié toutes les minutes. Si l'agent installé sur l'ordinateur correspondant n'est pas en train de transférer des données, et que cinq vérifications consécutives ne donnent aucun résultat, la ressource apparaît hors ligne. La ressource apparaît à nouveau en ligne lorsqu'elle répond à une vérification d'état ou commence à transférer des données.

Nouveautés de la console Cyber Protect

Lorsque les nouvelles fonctionnalités de Cyber Protect Cloud sont disponibles, vous voyez une fenêtre pop-up indiquant une brève description de ces fonctionnalités lors de la connexion à la console Cyber Protect.

Vous pouvez également consulter la description des nouvelles fonctionnalités en cliquant sur le lien **Nouveautés** en bas à gauche de la fenêtre principale de la console Cyber Protect.

En l'absence de nouvelles fonctionnalités, le lien **Nouveautés** n'est pas affiché.

© Acronis International GmbH, 2003-2026

Niveaux d'administration dans la console Cyber Protect

Cyber Protect Cloud prend en charge l'administration aux niveaux suivants :

- Niveau de partenaire (**Tous les clients**)

  Ce niveau est uniquement disponible pour les administrateurs partenaires qui gèrent des tenants clients.
- Niveau client

  Ce niveau est disponible pour les administrateurs clients et les administrateurs partenaires qui gèrent des tenants clients.
- Niveau unité

  Ce niveau est disponible pour les administrateurs d'unité, les administrateurs client du tenant parent et les administrateurs partenaire qui gèrent le tenant client parent.

Les administrateurs peuvent gérer des objets, tels que des plans ou des ressources, dans leurs propres tenants et dans leurs tenants enfants, avec les limitations suivantes :

- Les tenants clients peuvent restreindre l'accès des administrateurs partenaires.
- Les unités peuvent toujours être accessibles par les administrateurs clients et les administrateurs partenaires qui gèrent le tenant client parent.

Les administrateurs ne peuvent pas voir ou accéder aux objets à un niveau supérieur à leur propre tenant.

Par exemple, les administrateurs clients peuvent gérer les plans de protection à la fois au niveau tenant client et au niveau unité. Les administrateurs d'unité peuvent gérer uniquement leurs propres plans de protection au niveau unité. Ils ne peuvent pas gérer les plans de protection au niveau tenant client, ni les plans de protection créés par l'administrateur client au niveau unité. Pour plus d'informations, voir "Plans à différents niveaux d'administration" (p. 240).

Sélection d'un niveau d'administration

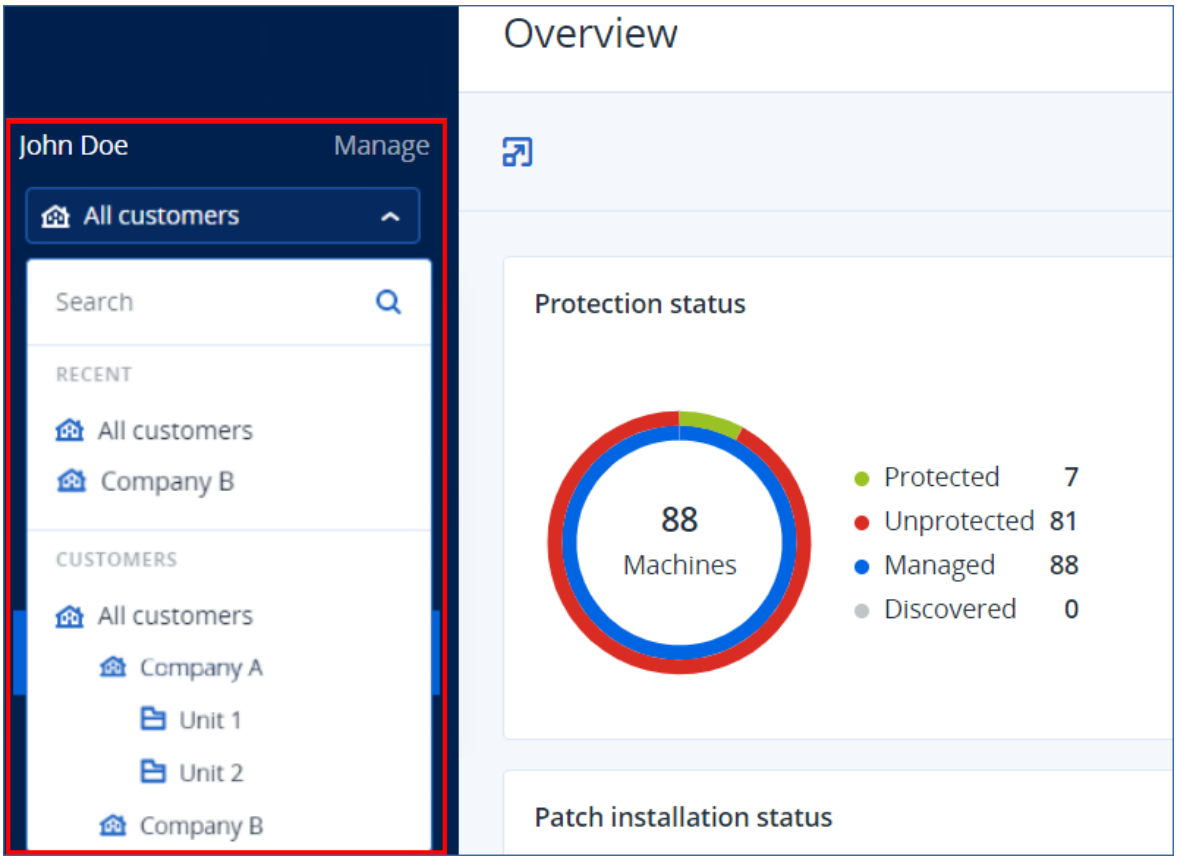
Les administrateurs qui gèrent plusieurs tenants et peuvent accéder au Portail de gestion peuvent sélectionner le niveau d'administration dans la console Cyber Protect.

Pour sélectionner un niveau d'administration

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Dans le menu de navigation à gauche, cliquez sur la flèche à côté du nom du tenant.
3. Sélectionnez l'une des options suivantes :
   - [Pour les administrateurs partenaires] Pour travailler au niveau du partenaire, sélectionnez **Tous les clients**.

© Acronis International GmbH, 2003-2026

- Pour travailler au niveau du client ou de l'unité, sélectionnez le nom d'un client ou d'une unité.



Utilisation de la console Cyber Protect au niveau **Tous les clients**

Les administrateurs de partenaire peuvent utiliser la console Cyber Protect au niveau du partenaire (**Tous les clients**).

À ce niveau, les administrateurs partenaires peuvent effectuer des actions avec des ressources de différents clients. Par exemple, un administrateur partenaire peut appliquer le même plan à plusieurs ressources de différents clients.

Au niveau du partenaire (**Tous les clients**), la console Cyber Protect fournit une vue personnalisée. Par exemple, les onglets **Alertes** et **Activités** fournissent des filtres supplémentaires liés aux partenaires, tandis que les onglets **Terminaux** et **Gestion** fournissent un accès uniquement aux fonctionnalités ou objets qui sont accessibles aux administrateurs partenaires.

Onglet Alertes

Les administrateurs partenaires peuvent voir les alertes de tous leurs clients gérés, les rechercher et les filtrer selon les critères suivants :

- Terminal
- Client
- Plan

Onglet Activités

© Acronis International GmbH, 2003-2026

Les administrateurs partenaires peuvent voir les activités de tous les tenants gérés ou les activités d'un tenant spécifique.

Les activités peuvent être filtrées par client, statut, temps et type.

Les types d'activités suivants sont automatiquement présélectionnés au niveau partenaire :

- Application du plan
- Création du plan de protection
- Plan de protection
- Révocation du plan
- Création de script

Onglet Terminaux

Les administrateurs partenaires peuvent voir les ressources de tous les tenants gérés, sélectionner des ressources de différents tenants et créer des groupes de terminaux.

Important
Au niveau du partenaire (**Tous les clients**), vous ne pourrez peut-être pas effectuer toutes les opérations disponibles au niveau du client. Pour effectuer une opération qui n'est pas prise en charge au niveau du partenaire, accédez au niveau du client.

Onglet Gestion

Les plans disponibles sont regroupés par type.

Dans **Gestion** > **Plans de protection**, les administrateurs partenaires peuvent voir les plans utilisés dans les tenants clients qu'ils gèrent et filtrer ces plans par statut, client et date de création. Les administrateurs partenaires peuvent créer de nouveaux plans au niveau partenaire. Pour plus d'informations sur les plans à différents niveaux, voir "Plans à différents niveaux d’administration" (p. 240).

Onglet Gestion de logiciel

Si l'analyse de l'inventaire des logiciels est activée pour les ressources des clients, vous pouvez voir les résultats de l'analyse des logiciels.

Visualisation des ressources de clients spécifiques

Au niveau du partenaire, vous pouvez afficher les ressources avec agents qui appartiennent à chaque tenant client géré.

Pour visualiser les ressources d'un client spécifique

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Dans l'arborescence, cliquez sur **Machines avec des agents** pour développer la liste.
3. Cliquez sur le nom du client dont vous souhaitez consulter et gérer les ressources.

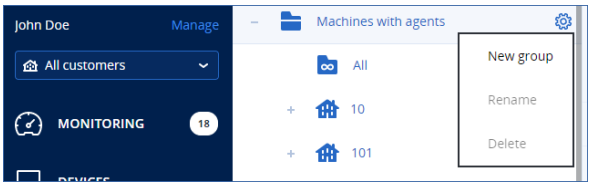
© Acronis International GmbH, 2003-2026

Création d'un groupe statique de terminaux au niveau du partenaire

Vous pouvez créer des groupes statiques de terminaux au niveau du partenaire (**Tous les terminaux**).

Pour créer un groupe statique de terminaux au niveau du partenaire

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur l'icône en forme d'engrenage située à côté de **Machines avec des agents**, puis cliquez sur **Nouveau groupe**.



3. Spécifiez le nom du groupe.
4. Ajoutez une description.
5. Cliquez sur **OK**.

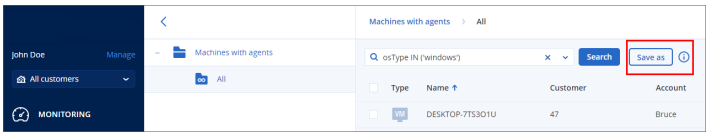
Création d'un groupe dynamique de terminaux au niveau du partenaire

Vous pouvez créer des groupes dynamiques de terminaux au niveau du partenaire (**Tous les terminaux**).

Créer un groupe dynamique de terminaux au niveau du partenaire

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Dans l'arborescence, cliquez sur **Machines avec des agents** pour développer la liste.
3. Cliquez sur **Tous**.
4. Dans le champ de recherche, spécifiez les critères selon lesquels vous souhaitez créer un groupe de terminaux dynamique, puis cliquez sur **Rechercher**.

   Pour en savoir plus sur les critères de recherche disponibles, voir "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 430) et "Rechercher des attributs pour les ressources de cloud à cloud" (p. 429).
5. Cliquez sur **Enregistrer sous**, puis spécifiez le nom du groupe.



6. [Facultatif] Ajoutez une description.
7. Cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

Découverte automatique des ordinateurs au niveau du partenaire

Vous pouvez effectuer une découverte automatique des ordinateurs au niveau du partenaire (**Tous les clients**).

Prérequis

Au moins un ordinateur avec agent de protection est installé dans le réseau local ou dans le domaine Active Directory de votre client.

Important
Seuls les agents installés sur des ordinateurs Windows peuvent être des agents de découverte. S'il n'existe aucun agent de découverte dans l'environnement de vos clients, vous ne pourrez pas utiliser l'option **Terminaux multiples** dans le panneau **Ajouter des terminaux**.

La découverte automatique n'est pas prise en charge pour l'ajout de contrôleurs de domaine en raison des autorisations supplémentaires requises pour le fonctionnement du service de l'agent.

L'installation à distance des agents n'est prise en charge uniquement pour les ordinateurs exécutant Windows (Windows XP n'est pas pris en charge). Pour l'installation à distance sur un ordinateur exécutant Windows Server 2012 R2, la mise à jour Windows KB2999226 doit être installée.

Pour effectuer la découverte automatique des ordinateurs au niveau du tenant partenaire

Rechercher dans Active Directory

Pour ajouter plusieurs terminaux depuis Active Directory

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Découvrir des terminaux**.
   L'assistant de découverte s'ouvre.
4. Sélectionnez un tenant client, puis l'agent de découverte qui effectuera la recherche des ordinateurs.

   Remarque
   Un agent de découverte est une ressource sur laquelle un agent de protection est installé.
   L'agent de découverte doit être un membre du domaine Active Directory.
   Vous pouvez sélectionner un agent associé au tenant sélectionné.

5. Sélectionnez **Rechercher dans Active Directory**, puis cliquez sur **Suivant**.
6. Dans la fenêtre **Rechercher dans Active Directory**, sélectionnez le mode de recherche des ordinateurs, puis cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

Option	Description
Dans une liste d'unités organisationnelles	Sélectionnez le groupe de machines à ajouter.
Par demande de dialecte LDAP.	Servez-vous d'une demande de dialecte LDAP pour sélectionner les machines. **Base de recherche** définit où chercher, alors que **Filtre** vous permet de spécifier les critères pour la sélection de la machine.

7. Dans la liste des ordinateurs découverts, sélectionnez les ordinateurs que vous souhaitez ajouter, puis cliquez sur **Suivant**.
   L'onglet **Sélectionner une option d'intégration** s'ouvre. Les options d'intégration suivantes sont disponibles.

Option	Description
Intégration automatique complète via Active Directory	Cette option utilise un contrôleur de domaine dans lequel un agent de découverte est installé pour intégrer des terminaux découverts à partir d'Active Directory. Aucune préconfiguration manuelle des terminaux n'est requise.
Préconfiguration manuelle et intégration automatique	Cette option nécessite la préconfiguration manuelle des terminaux et utilise un agent de découverte pour intégrer les terminaux découverts.
Ajouter en tant que machines non gérées	Cette option ajoute les terminaux découverts à la console en tant que terminaux non gérés, sans installer d'agent de protection sur ces terminaux.

8. En fonction de l'option d'intégration que vous sélectionnez, effectuez les opérations suivantes :
   - Si vous avez sélectionné **Intégration automatique complète via Active Directory**, effectuez les étapes 4 à 13 de la procédure correspondante.
   - Si vous avez sélectionné **Préconfiguration manuelle et intégration automatique**, suivez les étapes 4 à 11 de la procédure correspondante.
   - Si vous avez sélectionné **Ajouter en tant que machines non gérées**, sélectionnez le compte utilisateur sous lequel vous souhaitez enregistrer les terminaux, puis cliquez sur **Ajouter**.

Analyser le réseau local

Pour découvrir plusieurs terminaux en analysant le réseau local

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Découvrir des terminaux**.
   L'assistant de découverte s'ouvre.

© Acronis International GmbH, 2003-2026

4. Sélectionnez un tenant client, puis l'agent de découverte qui effectuera la recherche des ordinateurs.
5. Cliquez sur **Analyser le réseau local**.

   La découverte active de terminaux démarre. Vous êtes redirigé vers l'écran **Terminaux découverts** > **Réseau local**. Lorsque l'analyse est terminée, une notification s'affiche ; elle indique le nombre de terminaux découverts lors de l'analyse et inclut un lien vers la liste des terminaux où vous pouvez voir des détails supplémentaires à leur sujet.

Manuellement ou par importation d'un fichier

Pour ajouter plusieurs terminaux manuellement ou par importation d'un fichier

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. Dans **Terminaux multiples**, cliquez sur **Découvrir des terminaux**.

   L'assistant de découverte s'ouvre.
4. Sélectionnez un tenant client, puis l'agent de découverte qui effectuera la recherche des ordinateurs.
5. Cliquez sur **Spécifier manuellement ou importer à partir d'un fichier**.
6. Ajoutez des ordinateurs en utilisant l'une des options suivantes.
   - Pour ajouter des ordinateurs manuellement :
     a. Dans le champ **Ajouter un ordinateur**, saisissez l'adresse IPv4 ou le nom d'hôte de l'ordinateur.
     b. Répétez l'étape précédente pour chaque ordinateur à ajouter.
   - Pour ajouter des ordinateurs par importation d'un fichier :
     a. Cliquez sur **Importer la liste des ordinateurs depuis un fichier**.
     b. Dans la fenêtre **Importer la liste des ordinateurs depuis un fichier**, déposez le fichier texte contenant la liste des ordinateurs ou cliquez sur **Parcourir**, accédez au fichier, sélectionnez-le, puis cliquez sur **Ouvrir**.

        Le fichier doit contenir des adresses IP ou des noms d'hôte, un par ligne. Voici un exemple du contenu du fichier :

        ```
        156.85.34.10
        156.85.53.32
        156.85.53.12
        EN-L00000100
        EN-L00000101
        ```

   Après l'ajout manuel ou l'importation d'ordinateurs à partir d'un fichier, l'agent essaie d'envoyer une commande ping aux ordinateurs ajoutés et de définir leur disponibilité.
7. Cliquez sur **Suivant**.

   L'onglet **Sélectionner une option d'intégration** s'ouvre. Les options d'intégration suivantes sont disponibles.

© Acronis International GmbH, 2003-2026

Option	Description
Intégration automatique complète via Active Directory	Cette option utilise un contrôleur de domaine dans lequel un agent de découverte est installé pour intégrer des terminaux découverts à partir d'Active Directory. Aucune préconfiguration manuelle des terminaux n'est requise.
Préconfiguration manuelle et intégration automatique	Cette option nécessite la préconfiguration manuelle des terminaux et utilise un agent de découverte pour intégrer les terminaux découverts.
Ajouter en tant que machines non gérées	Cette option ajoute les terminaux découverts à la console en tant que terminaux non gérés, sans installer d'agent de protection sur ces terminaux.

8. En fonction de l'option d'intégration que vous sélectionnez, effectuez les opérations suivantes :
   - Si vous avez sélectionné **Intégration automatique complète via Active Directory**, effectuez les étapes 4 à 13 de la procédure correspondante.
   - Si vous avez sélectionné **Préconfiguration manuelle et intégration automatique**, suivez les étapes 4 à 11 de la procédure correspondante.
   - Si vous avez sélectionné **Ajouter en tant que machines non gérées**, sélectionnez le compte utilisateur sous lequel vous souhaitez enregistrer les terminaux, puis cliquez sur **Ajouter**.

Création d'un plan global d'exclusions antivirus et antimalware

Le plan d'exclusions antivirus et antimalware globales (exclusions globales) vous permet de créer une liste d'éléments de confiance au niveau du partenaire. Les administrateurs partenaires peuvent ajouter des fichiers, des dossiers, des processus ou des hachages à un seul plan et l'appliquer à toutes les ressources des clients. Le plan d'exclusions globales gère efficacement les listes d'éléments de confiance pour les tenants clients en éliminant le besoin de modifier manuellement chaque plan de protection individuel.

Pour créer un plan global d'exclusions antivirus et antimalware

1. Dans le portail de gestion, accédez à **Surveillance** > **Utilisation**.
2. Sous **Cyber Protect**, sélectionnez **Protection**, puis cliquez sur **Gérer le service**.
3. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
4. Cliquez sur **Création d'un plan**.
   Le modèle de plan de protection s'ouvre.
5. Développez le module **Exclusions de la protection antivirus et antimalware globale**.
6. Sélectionnez l'option **Exclusions**.
   La fenêtre **Exclusions globales d'antivirus et d'antimalware** s'ouvre.
7. Dans la section **Éléments de confiance**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :

© Acronis International GmbH, 2003-2026

- Pour définir des fichiers, dossiers ou processus comme étant fiables, sélectionnez l'option **Fichier/dossier/processus**. La fenêtre **Ajouter un fichier/dossier/processus** s'ouvre.
  - Dans le champ **Fichier/dossier/processus**, saisissez le chemin d'accès de chaque processus, dossier ou fichier sur une nouvelle ligne.
  - Cochez la case **Ajouter en tant que fichier/dossier** pour définir le fichier/dossier comme étant fiable.
    Exemples de description de dossier : `D:\folder\`, `/home/Folder/folder2`, `F:\`
  - Cochez la case **Ajouter en tant que processus** pour définir un processus comme étant fiable. Les processus sélectionnés seront exclus de la surveillance.

    Vous pouvez spécifier le chemin d'accès complet à un processus ou utiliser un caractère générique. Par exemple, pour exclure tous les processus dans le dossier `Temp`, vous pouvez entrer `C:\Windows\Temp\*.exe`.

    Les chemins d'accès du réseau local sont pris en charge. Par exemple, `\\localhost\folderpath\file.exe`
- Pour ajouter des hachages MD5 à la liste des éléments de confiance, sélectionnez l'option **Hachage**. La fenêtre **Ajoutez le hachage** s'ouvre.
  - Vous pouvez insérer ici des hachages MD5 sur des lignes séparées afin qu'ils soient inclus comme éléments fiables dans la liste Exclusions de protection. Sur la base de ces hachages, Cyber Protection exclura de la surveillance les processus qu'ils décrivent.

8. Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre modification dans la liste des éléments de confiance. Par exemple, raisons et objectifs de l'exclusion, horodatages, etc.

   Remarque
   Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

9. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Remarque

- Vous pouvez créer autant de plans d'exclusions globaux que vous le souhaitez et les appliquer aux ressources de vos clients directs.
- Les plans actifs sont appliqués de manière cumulative.
- Si le même élément apparaît dans plusieurs plans, il ne sera pas dupliqué.
- Un élément sera toujours de confiance s'il existe dans la liste des éléments de confiance sous un plan d'exclusions global et dans la liste des éléments bloqués sous le module d'exclusions de protection.

Utilisation de caractères génériques pour définir des exclusions

Pour définir des exclusions, vous pouvez utiliser les caractères génériques * et ?. L'astérisque (*) remplace zéro ou plusieurs caractères. Le point d'interrogation (?) remplace exactement un caractère. Les variables d'environnement, telles que `%AppData%`, ne peuvent pas être utilisées.

© Acronis International GmbH, 2003-2026

Vous pouvez utiliser un caractère générique (*) pour ajouter des éléments aux listes d'exclusion.

- Les caractères génériques peuvent être utilisés au milieu ou à la fin d'une description.

Exemple des caractères génériques acceptés dans des descriptions :

```
C:\*.pdf
```

```
D:\folders\file.*
```

```
C:\Users\*\AppData\Roaming
```

- Les caractères génériques ne peuvent pas être utilisés au début d'une description.

Exemples de caractères génériques non acceptés dans les descriptions :

```
*.docx
```

```
*:\folder\
```

Utilisation de variables pour définir des exclusions

Vous pouvez également utiliser des variables pour ajouter des éléments à la liste des exclusions globales, avec les restrictions suivantes :

- Pour Windows, seules les variables SYSTEM sont prises en charge. Les variables propres à l'utilisateur, par exemple `%USERNAME%` ou `%APPDATA%` ne sont pas prises en charge. Les variables avec `{username}` ne sont pas prises en charge. Pour plus d'informations, voir https://ss64.com/nt/syntax-variables.html.
- Pour macOS, les variables d'environnement ne sont pas prises en charge.
- Pour Linux, les variables d'environnement ne sont pas prises en charge.

Exemples de formats pris en charge :

- `%WINDIR%\Media`
- `%public%`
- `%CommonProgramFiles%\Acronis\`

Ressources

Une ressource correspond à tout type de ressource protégée ; il peut s'agir, par exemple, d'une machine physique, d'une machine virtuelle, d'une boîte aux lettres ou d'une instance de base de données. Dans la console Cyber Protect, la ressource est affichée comme étant un objet auquel vous pouvez appliquer un plan (de protection, de sauvegarde ou de création de script).

Certaines ressources nécessitent l'installation d'un agent de protection ou le déploiement d'une appliance virtuelle. Vous pouvez installer les agents à l'aide de l'interface graphique ou de l'interface de ligne de commande (installation sans assistance). Vous pouvez utiliser l'installation sans

© Acronis International GmbH, 2003-2026

assistance pour automatiser la procédure d'installation. Pour plus d'informations sur l'installation des agents de protection, voir "Installation et déploiement d'agents Cyber Protection" (p. 37).

Une appliance virtuelle est une machine virtuelle prête à l'emploi qui contient un agent de protection. Avec une appliance virtuelle, vous pouvez sauvegarder d'autres machines virtuelles du même environnement sans y installer d'agent de protection (sauvegarde sans agent). Les appliances virtuelles sont disponibles dans des formats propres à l'hyperviseur tels que .ovf, .ova ou .qcow. Pour plus d'informations sur les plates-formes de virtualisation qui prennent en charge la sauvegarde sans agent, consultez "Plates-formes de virtualisation prises en charge" (p. 526).

Important
Les agents doivent être en ligne au moins une fois tous les 30 jours. Sinon, leurs plans sont révoqués et les ressources ne sont plus protégées.

Le tableau ci-dessous récapitule les types de ressources et leurs agents respectifs.

Type de ressource	Agent	Exemples (liste non exhaustive)
Machines physiques	Un agent de protection est installé sur chaque machine protégée.	Poste de travail Ordinateur portable Serveur
Machines virtuelles	Selon la plate-forme de virtualisation, les méthodes de sauvegarde suivantes peuvent être disponibles : • Sauvegarde avec agent : un agent de protection est installé sur chaque machine protégée. • Sauvegarde sans agent : un agent de protection est installé uniquement sur l'hôte de l'hyperviseur, sur une machine virtuelle dédiée, ou est déployé sous forme d'appliance virtuelle. Cet agent sauvegarde toutes les machines virtuelles de l'environnement.	Machine virtuelle VMware Machine virtuelle Hyper-V Machine virtuelle basée sur un noyau (KVM) et gérée par oVirt Machines virtuelles VMware Cloud Director (vCD)*
Ressources Microsoft 365 Business Ressources Google Workspace	Ces ressources sont sauvegardées par un agent cloud ne nécessitant aucune installation. Pour utiliser l'agent cloud, vous devez ajouter votre organisation Microsoft 365 ou Google Workspace à la console Cyber Protect. En outre, un agent local pour Office 365 est disponible. Il nécessite une installation et ne peut être utilisé que pour sauvegarder les boîtes aux lettres Exchange Online. Pour plus d'informations sur les différences entre l'agent local et l'agent	Boîte aux lettres Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Site SharePoint Boîte aux lettres Google Google Drive

© Acronis International GmbH, 2003-2026

Type de ressource	Agent	Exemples (liste non exhaustive)
	dans le cloud, voir "Protection des données Microsoft 365" (p. 844).	
Applications	Les données d'applications spécifiques sont sauvegardées par des agents dédiés tels que l'agent pour SQL, l'agent pour Exchange, l'agent pour MySQL/MariaDB ou l'agent pour Active Directory.	Bases de données SQL Server Bases de données MySQL/MariaDB Base de données Oracle Active Directory
Terminaux mobiles	Une application mobile est installée sur les terminaux protégés.	Terminaux Android ou iOS
Sites Web	Les sites Web sont sauvegardés par un agent cloud ne nécessitant aucune installation.	Sites Web accessibles via les protocoles SFTP ou SSH

Pour plus d'informations sur l'agent nécessaire et sur son emplacement d'installation, voir "De quel agent ai-je besoin ?" (p. 41)

* Pour plus d'informations sur l'intégration de VMware Cloud Director avec Cyber Protect Cloud, consultez le guide de l'administrateur partenaire.

Ajout de ressources à la console Cyber Protect

Pour démarrer la protection de vos ressources, commencez par ajouter ces ressources à la console Cyber Protect.

Remarque
Les types de ressources que vous pouvez ajouter dépendent des quotas de service de votre compte. Si un type de ressource spécifique est manquant, il est grisé dans le volet **Ajouter des terminaux**.

Un administrateur partenaire peut activer les quotas de service requis dans le portail de gestion. Pour plus d'informations, voir "Informations pour les administrateurs partenaires" (p. 403).

Pour ajouter une ressource

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Terminaux** > **Tous les terminaux**, puis cliquez sur **Ajouter**.
   Le panneau **Ajouter des terminaux** s'ouvre à droite.
3. Sélectionnez le canal de publication.

© Acronis International GmbH, 2003-2026

4. Cliquez sur le type de ressource que vous souhaitez ajouter, puis suivez les instructions pour la ressource que vous avez sélectionnée.

Le tableau suivant récapitule les types de ressources et les actions requises.

Ressources à ajouter	Action requise	Procédure à suivre
Plusieurs ordinateurs Windows	Exécutez une découverte automatique dans votre environnement. Pour exécuter la découverte automatique, vous avez besoin d'au moins un ordinateur sur lequel est installé un agent de protection dans votre réseau local ou votre domaine Active Directory. Cet agent est utilisé comme agent de découverte.	"Ajout de plusieurs terminaux" (p. 184)
Postes de travail Windows Serveurs Windows	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation d'agents de protection sous Windows" (p. 74)
Postes de travail macOS	Installez l'agent pour macOS.	"Installation des agents de protection sous macOS" (p. 71) ou "Installation et désinstallation d'agents de protection dans macOS" (p. 99)
Serveurs Linux	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 69) ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92)
Terminaux mobiles (iOS, Android)	Installez l'application mobile.	"Protection des terminaux mobiles" (p. 840)
Ressources de cloud à cloud		
Microsoft 365 Business	Ajoutez votre organisation Microsoft 365 à la console Cyber Protect et utilisez l'agent cloud pour protéger les boîtes	"Protection des données Microsoft 365" (p. 844)

© Acronis International GmbH, 2003-2026

Ressources à ajouter	Action requise	Procédure à suivre
	aux lettres Exchange Online, les fichiers OneDrive, Microsoft Teams, ainsi que les sites SharePoint. Vous pouvez également installer l'agent local pour Office 365. Il ne fournit que la sauvegarde des boîte aux lettres Exchange Online. Pour plus d'informations sur les différences entre l'agent local et l'agent cloud, voir "Protection des données Microsoft 365" (p. 844).	
Google Workspace	Ajoutez votre organisation Google Workspace à la console Cyber Protect et utilisez l'agent cloud pour protéger les boîtes aux lettres Gmail et les fichiers Google Drive.	"Protection des données Google Workspace" (p. 917)
Machines virtuelles		
VMware ESXi (Broadcom)	Déployez l'agent pour VMware (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour VMware (appliance virtuelle)" (p. 138)
	Installez l'agent pour VMware (Windows).	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation d'agents de protection sous Windows" (p. 74)
Virtuozzo Hybrid Infrastructure	Déployez l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)" (p. 145)
Microsoft Hyper-V	Installez l'agent pour Hyper-V.	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation d'agents de protection sous Windows" (p. 74)
Virtuozzo Hybrid Server	Installez l'agent pour Virtuozzo.	"Installation des agents de protection sous Linux" (p. 69)

© Acronis International GmbH, 2003-2026

Ressources à ajouter	Action requise	Procédure à suivre
		ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92)
KVM	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation d'agents de protection sous Windows" (p. 74)
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 69) ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92)
Red Hat Virtualization (oVirt)	Déployez l'agent pour oVirt (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour oVirt (appliance virtuelle)" (p. 157)
Citrix Hypervisor/XenServer	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation d'agents de protection sous Windows" (p. 74)
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 69) ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92)
Nutanix AHV	Déployer l'agent pour Nutanix AHV.	"Déploiement de l'agent pour Nutanix AHV" (p. 167)
Oracle VM	Installez l'agent pour Windows.	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation

© Acronis International GmbH, 2003-2026

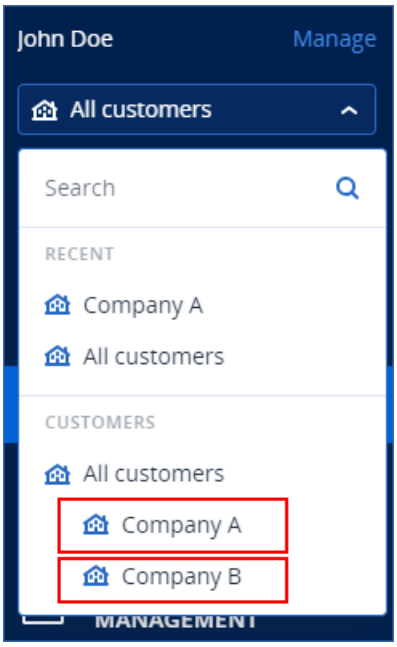
Ressources à ajouter	Action requise	Procédure à suivre
		d'agents de protection sous Windows" (p. 74)
	Installez l'agent pour Linux.	"Installation des agents de protection sous Linux" (p. 69) ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92)
Oracle LWM (oVirt)	Déployez l'agent pour oVirt (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour oVirt (appliance virtuelle)" (p. 157)
Scale Computing HyperCore	Déployez l'agent pour Scale Computing HC3 (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour Scale Computing HC3 (appliance virtuelle)" (p. 141)
Proxmox VE	Installer l'agent pour Proxmox (offre groupée avec l'agent pour Linux, 64 bits)	"Installation des agents de protection sous Linux" (p. 69) ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92)
Stockage en réseau		
Synology	Déployez l'agent pour Synology (appliance virtuelle) dans votre environnement.	"Déploiement de l'agent pour Synology" (p. 171)
Applications		
Microsoft SQL Server	Installez l'agent pour SQL.	"Installation des agents de protection sous Windows" (p. 64) ou "Installation et désinstallation d'agents de protection sous Windows" (p. 74)
Microsoft Exchange Server	Installez l'agent pour Exchange.	
Microsoft Active Directory	Installez l'agent pour Active Directory.	
Base de données Oracle	Installez l'agent pour Oracle.	"Sauvegarde d'Oracle Database" (p. 946)

Pour plus d'informations sur les agents de protection disponibles et sur leur emplacement d'installation, voir "De quel agent ai-je besoin ?" (p. 41)

© Acronis International GmbH, 2003-2026

Informations pour les administrateurs partenaires

- Un type de ressource peut manquer dans le panneau **Ajouter des terminaux** si un quota de service requis n'est pas activé dans le portail de gestion. Pour plus d'informations sur les quotas de service requis en fonction des ressources, voir la section Activation ou désactivation des éléments d'offre dans le Guide de l'administrateur partenaire.
- En tant qu'administrateur partenaire, vous ne pouvez pas ajouter de ressources au niveau **Tous les clients**. Pour ajouter une ressource, sélectionnez un tenant client.



Suppression de ressources de la console Cyber Protect

Vous pouvez supprimer de la console Cyber Protect les ressources que vous n'avez plus besoin de protéger. La procédure dépend du type de ressource.

Vous pouvez également désinstaller l'agent sur la ressource protégée. Lorsque vous désinstallez un agent, la ressource protégée est supprimée automatiquement de la console Cyber Protect.

Important
Lorsque vous supprimez une ressource de la console Cyber Protect, tous les plans appliqués à cette ressource sont révoqués. La suppression d'une ressource ne supprime aucun plan ni sauvegarde, et ne désinstalle pas l'agent de protection.

Le tableau suivant récapitule les types de ressources et les actions requises.

Ressources à supprimer	Actions requises	Procédure à suivre
Machines physiques et virtuelles		
Machines physiques ou	1. Supprimez la	"Pour supprimer une ressource de la console

© Acronis International GmbH, 2003-2026

Ressources à supprimer	Actions requises	Procédure à suivre
virtuelles sur lesquelles un agent de protection est installé	ressource de la console Cyber Protect. 2. [Facultatif] Désinstallez l'agent de protection.	Cyber Protect" (p. 405) (Ressource avec agent de protection)
Machines virtuelles sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent)	1. Dans la console Cyber Protect, supprimez l'ordinateur sur lequel l'agent de protection est installé. Toutes les machines virtuelles sauvegardées par cet agent sont supprimées automatiquement de la console. 2. [Facultatif] Désinstallez l'agent de protection.	"Pour supprimer une ressource de la console Cyber Protect" (p. 405) (Ressource sans agent de protection)
Ressources de cloud à cloud		
Ressources Microsoft 365 Business Ressources Google Workspace	Supprimez l'organisation Microsoft 365 ou Google Workspace de la console Cyber Protect. Toutes les ressources de cette organisation sont supprimées automatiquement de la console.	"Pour supprimer une ressource de la console Cyber Protect" (p. 405) (Ressource cloud à cloud)
Terminaux mobiles		
Terminaux Android Terminaux iOS	1. Supprimez le terminal mobile de la console Cyber Protect. 2. [Facultatif] Sur le terminal mobile,	"Pour supprimer une ressource de la console Cyber Protect" (p. 405) (Terminal mobile)

© Acronis International GmbH, 2003-2026

Ressources à supprimer	Actions requises	Procédure à suivre
	désinstallez l'application.	
Stockage en réseau		
Synology	1. Supprimez la ressource de la console Cyber Protect. 2. [Facultatif] Désinstallez l'agent de protection.	"Pour supprimer une ressource de la console Cyber Protect" (p. 405) (Ressource avec agent de protection)
Applications		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Base de données Oracle	1. Dans la console Cyber Protect, supprimez l'ordinateur sur lequel l'agent de protection est installé. Les objets sauvegardés par cet agent sont supprimés automatiquement de la console. 2. [Facultatif] Désinstallez l'agent de protection.	"Pour supprimer une ressource de la console Cyber Protect" (p. 405) (Ressource sans agent de protection)
Sites Web	Supprimez le site Web de la console Cyber Protect.	"Pour supprimer une ressource de la console Cyber Protect" (p. 405) (Site Web)

Pour supprimer une ressource de la console Cyber Protect

Ressource avec agent de protection

Vous pouvez supprimer ce type de ressource directement.

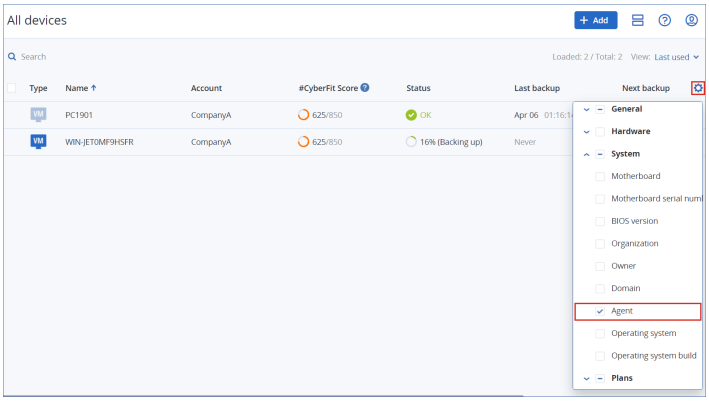
1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cochez la case à côté de la ou des ressources à supprimer.
3. Dans le panneau **Actions**, cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.
5. [Facultatif] Désinstallez l'agent en suivant les indications de "Désinstallation d'agents" (p. 72).

© Acronis International GmbH, 2003-2026

Ressource sans agent de protection

Pour supprimer ce type de ressource, vous devez supprimer l'ordinateur sur lequel l'agent de protection est installé.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans l'angle supérieur droit, cliquez sur l'icône en forme d'engrenage, puis cochez la case **Agent**.



   La colonne **Agent** apparaît.
3. Dans la colonne **Agent**, cochez le nom de l'ordinateur sur lequel l'agent de protection est installé.
4. Dans la console Cyber Protect, cochez la case située à côté de l'ordinateur sur lequel l'agent de protection est installé.
5. Dans le panneau **Actions**, cliquez sur **Supprimer**.
6. Confirmez votre choix en cliquant sur **Supprimer**.
7. [Facultatif] Désinstallez l'agent en suivant les indications de "Désinstallation d'agents" (p. 72).

Ressource cloud à cloud

Pour supprimer les ressources sauvegardées par l'agent cloud, supprimez l'organisation Microsoft 365 ou Google Workspace de la console Cyber Protect.

1. Dans la console Cyber Protect, sélectionnez **Terminaux** > **Microsoft 365** ou **Terminaux** > **Google Workspace**.
2. Cliquez sur le nom de votre organisation Microsoft 365 ou Google Workspace.
3. Dans le panneau **Actions**, cliquez sur **Supprimer le groupe**.
4. Cliquez sur **Supprimer** pour confirmer votre action.

Terminal mobile

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cochez la case à côté de la ressource à supprimer.
3. Dans le panneau **Actions**, cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.
5. [Facultatif] Sur le terminal mobile, désinstallez l'application.

© Acronis International GmbH, 2003-2026

Site Web

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cochez la case à côté de la ressource à supprimer.
3. Dans le panneau **Actions**, cliquez sur **Supprimer**.
4. Confirmez votre choix en cliquant sur **Supprimer**.

Types de ressources

Types de ressources

Icône	Description
	Groupe de disponibilité de l'agent
	AA pool
	Passerelle de stockage Acronis Backup
	Acronis cloud
	Carnet d'adresses
	Toutes les ressources
	Téléphone Android
	Boîte aux lettres d'archive
	Acronis Storage Node
	Bande Acronis Storage Node

© Acronis International GmbH, 2003-2026

Icône	Description
	Acronis secure zone
	Fichier audio
	Plan de sauvegarde
	Plan de réplication de sauvegarde
	Calendrier
	Plan de catalogage
	CD/DVD
	Bande de nettoyage
	Plan de nettoyage
	Cloud
	Cluster
	Cluster de calcul
	CommuniGate
	Contacts

© Acronis International GmbH, 2003-2026

Icône	Description
	Convertir en plan de machine virtuelle
	Client
	Centre de données
	Cluster de base de données
	Cluster de base de données actif
	Bureau Linux
	Bureau Windows
	Disque
	Lecteur
	Serveur de reprise d’activité après sinistre
	Groupes dynamiques
	ECP Veil
	Lecteur vide
	Logement vide

© Acronis International GmbH, 2003-2026

Icône	Description
	Fichier chiffré
	Cluster ESX
	ESX temporaire
	ESX inconnu
	L'événement
	Fichier Excel
	Cluster Microsoft Exchange
	Fichier
	Dossier
	Dossiers clients
	Abonnés
	Suivis
	Pool libre
	FTP

© Acronis International GmbH, 2003-2026

Icône	Description
	Google
	Google drive
	Groupe
	Cluster Hyper-V
	Hyper-V inconnu
	Fichier image
	Plan d'inventaire
	IPhone
	Ordinateur portable
	Portable Linux
	Portable Windows
	Groupe de bibliothèque
	J'aime
	Mac 1

© Acronis International GmbH, 2003-2026

Icône	Description
	Mac 2
	Mac air
	Machine
	Ordinateur dans un environnement virtuel
	Programme de mise à jour
	Mac mini
	Mac Pro
	Support
	Message
	Microsoft
	Microsoft 365
	Microsoft Exchange
	Microsoft Exchange office
	Microsoft OneNote

© Acronis International GmbH, 2003-2026

Icône	Description
	Fichier Microsoft OneNote
	Fichier Microsoft PowerPoint
	Base de données Microsoft SQL Server
	Groupe de bases de données Microsoft SQL Server
	Instance Microsoft SQL Server
	Microsoft Teams
	Fichier Microsoft Word
	Mobile
	Network attached storage (NAS)
	Partage de réseau
	Bande réseau
	NFS
	Fichier Notary
	Conteneur Odin

© Acronis International GmbH, 2003-2026

Icône	Description
	Conteneur Odin (en cours d'exécution)
	Groupe Odin
	Oracle VM
	Partenaire
	PCS temporaire
	Fichier PDF
	Photos
	Envoi de données physiques
	Pool
	Groupe de pool
	Postgre SQL
	Publications
	Profil
	Bande protégé

© Acronis International GmbH, 2003-2026

Icône	Description
	QNAP
	Doublons de serveurs de restauration
	Moteur Red Hat Virtualization (oVirt)
	Rappels
	Réplica
	Réplica (en cours d'exécution)
	Liste des ressources
	Cluster Scale Computing HC3
	Script
	Serveur
	Prise de connecteur
	Cluster SQL
	Synology
	Tablette

© Acronis International GmbH, 2003-2026

Icône	Description
	Tablette Android
	Tablette Apple
	Bande
	Bibliothèque de bandes
	Tâche
	Fichier texte
	Unité
	Encadré inconnu
	Ordinateur de configuration inconnu
	Pool non reconnu
	Utilisateur
	Plan de validation
	vCenter server
	Fichier vidéo

© Acronis International GmbH, 2003-2026

Icône	Description
	Vidéos
	Appliance virtuelle
	Application virtuelle
	Machine virtuelle Azure
	Machine virtuelle Azure (en cours d'exécution)
	Machine virtuelle ECP Veil
	Machine virtuelle ECP Veil (en cours d'exécution)
	Machine virtuelle HCI
	Machine virtuelle HCI (en cours d'exécution)
	Machine virtuelle Hyper-V
	Machine virtuelle Hyper-V (en cours d'exécution)
	Démarrage de la machine virtuelle Hyper-V
	Machine virtuelle KVM
	Machine virtuelle KVM (en cours d'exécution)

© Acronis International GmbH, 2003-2026

Icône	Description
	Machine virtuelle Odin
	Machine virtuelle Odin (en cours d'exécution)
	Machine virtuelle Red Hat Virtualization (oVirt)
	Machine virtuelle Red Hat Virtualization (oVirt) (en cours d'exécution)
	Machine virtuelle Scale Computing HC3
	Machine virtuelle Scale Computing HC3 (en cours d'exécution)
	Machine virtuelle Scale Computing HC3 réplica
	Machine virtuelle Scale Computing HC3 réplica (en cours d'exécution)
	Machine virtuelle VMware
	Machine virtuelle VMware (en cours d'exécution)
	Démarrage de la machine virtuelle VMware
	Plate-forme Virtuozzo infrastructure
	Machine virtuelle et modèles

© Acronis International GmbH, 2003-2026

Icône	Description
	Plan de réplication de machine virtuelle
	Site Web
	Bande WORM
	Fichier Zip

Groupes du terminal

Grâce aux groupes de terminaux, vous pouvez protéger plusieurs ressources semblables avec un plan de groupe. Le plan est appliqué au groupe dans son intégralité et ne peut pas être révoqué d'un membre du groupe.

Une ressource peut être membre de plusieurs groupes. Une ressource incluse dans un groupe de terminaux peut toujours être protégée par différents plans.

Vous ne pouvez ajouter à un groupe de terminaux que des ressources du même type. Par exemple, sous **Hyper-V**, vous ne pouvez créer que des groupes de machines virtuelles Hyper-V. Sous **Machines avec des agents**, vous ne pouvez créer que des groupes de machines avec des agents installés.

Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

Groupes par défaut et groupes personnalisés

Groupes par défaut

Une fois qu'une ressource est enregistrée dans la console Cyber Protect, elle apparaît dans l'un des groupes root (superutilisateur) par défaut dans l'onglet **Terminaux**, par exemple, **Machines avec des agents**, **Microsoft 365** ou **Hyper-V**.

Toutes les ressources autres que de cloud à cloud enregistrées sont également répertoriées dans le groupe root (superutilisateur) **Tous les terminaux**. Un groupe root (superutilisateur) par défaut distinct portant le nom du tenant contient toutes les ressources autres que de cloud à cloud et toutes les unités de ce tenant.

© Acronis International GmbH, 2003-2026

Vous ne pouvez pas supprimer ou modifier les groupes root (superutilisateur), ni leur appliquer des plans.

Certains des groupes root (superutilisateur) contiennent un ou plusieurs niveaux de sous-groupes par défaut, par exemple, **Machines avec des agents** > **Tous**, **Microsoft 365** > votre organisation > **Équipes** > **Toutes les équipes**, **Google Workspace** > votre organisation > **Lecteurs partagés** > **Tous les disques partagés**.

Vous ne pouvez ni modifier ni supprimer les sous-groupes par défaut.

Groupes personnalisés

La protection de toutes les ressources d'un groupe par défaut n'est peut-être pas très pratique, car certaines ressources nécessitent une planification de protection ou des paramètres de protection différents.

Dans certains des groupes root (superutilisateur), par exemple dans **Machines avec des agents**, **Microsoft 365** ou **Google Workspace**, vous pouvez créer des sous-groupes personnalisés. Ces sous-groupes peuvent être statiques ou dynamiques.

Vous pouvez modifier, renommer ou supprimer n'importe quel groupe personnalisé.

Groupes statiques et dynamiques

Vous pouvez créer le type de groupes personnalisés suivant :

- Statique
- Dynamique

Groupes statiques

Les groupes statiques contiennent des ressources ajoutées manuellement.

Le contenu d'un groupe statique change uniquement lorsque vous ajoutez ou supprimez une ressource explicitement.

Exemple : Vous créez un groupe statique pour le service comptable de votre entreprise, puis ajoutez les ordinateurs des comptables à ce groupe manuellement. Lorsque vous appliquez un plan de groupe, les ordinateurs de ce groupe sont protégés. Si un nouveau comptable est embauché, vous devrez ajouter son ordinateur au groupe statique manuellement.

Groupes dynamiques

Les groupes dynamiques contiennent des ressources qui correspondent à des critères spécifiques. Vous définissez ces critères par avance en créant une requête de recherche qui comprend des attributs (par exemple, `osType`), leurs valeurs (par exemple, `Windows`) et des opérateurs de recherche (par exemple, `IN`).

© Acronis International GmbH, 2003-2026

Par conséquent, vous pouvez créer un groupe dynamique pour tous les ordinateurs dont le système d'exploitation est Windows ou un groupe dynamique contenant tous les utilisateurs de votre organisation Microsoft 365 dont les adresses e-mail commencent par `john`.

Toutes les ressources disposant des attributs et valeurs nécessaires sont ajoutées automatiquement au groupe, et toute ressource perdant un attribut ou une valeur nécessaire est supprimée automatiquement du groupe.

Exemple 1 : Les noms d'hôte des ordinateurs appartenant au service comptable comportent le mot « comptabilité ». Vous recherchez les ordinateurs dont les noms contiennent le mot « comptabilité », puis enregistrez les résultats de la recherche en tant que groupe dynamique. Vous appliquez ensuite un plan de protection au groupe. Si un nouveau comptable est embauché, le nom de son ordinateur contiendra le mot « comptabilité » et cet ordinateur sera ajouté automatiquement au groupe dynamique dès que vous l'enregistrez dans la console Cyber Protect.

Exemple 2 : Le service comptable forme une unité d'organisation (UO) Active Directory séparée. Vous indiquez l'UO de comptabilité comme étant un attribut nécessaire, puis enregistrez les résultats de la recherche en tant que groupe dynamique. Vous appliquez ensuite un plan de protection au groupe. Si un nouveau comptable est embauché, son ordinateur est ajouté au groupe dynamique dès qu'il est ajouté à l'UO Active Directory, puis il est enregistré dans la console Cyber Protect (quel que soit l'ordre d'arrivée).

Groupes de cloud à cloud et groupes autres que de cloud à cloud

Les groupes de cloud à cloud contiennent des ressources Microsoft 365 ou Google Workspace qui sont sauvegardées par un agent cloud.

Les groupes autres que de cloud à cloud contiennent tous les autres types de ressources.

Plans pris en charge pour les groupes de terminaux

Le tableau suivant récapitule les plans que vous pouvez appliquer à un groupe de terminaux.

Groupe	Plans disponibles	Emplacement du plan
Ressources de cloud à cloud (ressources Microsoft 365 et Google Workspace)	Plan de sauvegarde	**Gestion** > **Sauvegarde d'applications dans le Cloud**
Ressources autres que de cloud à cloud	Plan de protection	**Gestion** > **Plans de protection**
	Plan de gestion à distance	**Gestion** > **Plans de gestion à distance**
	Plan de création de script	**Gestion** > **Plans de création de scripts**

Les ressources cloud telles que les utilisateurs Microsoft 365 ou Google Workspace, les partages OneDrive et Google Drive, Microsoft Teams ou les groupes Azure AD sont synchronisées dans la

© Acronis International GmbH, 2003-2026

console Cyber Protect immédiatement après que vous ajoutez une organisation Microsoft 365 ou Google Workspace à la console. Toutes les autres modifications apportées à une organisation sont synchronisées une fois par jour.

Si vous devez synchroniser une modification immédiatement, accédez depuis la console Cyber Protect à **Terminaux** > **Microsoft 365** ou **Terminaux** > **Google Workspace** respectivement, sélectionnez l'organisation nécessaire, puis cliquez sur **Actualiser**.

Création d'un groupe statique

Vous pouvez créer un groupe statique vide et lui ajouter des ressources.

Vous pouvez également sélectionner des ressources et créer un nouveau groupe statique à partir de votre sélection.

Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

Pour créer un groupe statique

Dans la fenêtre principale

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources pour lesquelles vous souhaitez créer un groupe statique.
2. [Facultatif] Pour créer un groupe imbriqué, accédez à un groupe statique existant.

   Remarque
   La création de groupes statiques imbriqués n'est pas disponible pour les ressources de cloud à cloud.

3. Cliquez sur **+ Nouveau groupe statique** en dessous de l'arborescence de groupe ou sur **Nouveau groupe statique** dans le volet **Actions**.
4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Ajoutez un commentaire pour le groupe.
6. Cliquez sur **OK**.

Dans l'arborescence du groupe

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources pour lesquelles vous souhaitez créer un groupe statique.
2. Cliquez sur l'icône en forme d'engrenage en regard du nom du groupe dans lequel vous souhaitez créer un nouveau groupe statique.

   Remarque
   La création de groupes statiques imbriqués n'est pas disponible pour les ressources de cloud à cloud.

© Acronis International GmbH, 2003-2026

3. Cliquez sur **Nouveau groupe statique**.
4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Ajoutez un commentaire pour le groupe.
6. Cliquez sur **OK**.

À partir de la sélection

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources pour lesquelles vous souhaitez créer un groupe statique.

   Remarque
   Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

2. Cochez les cases en regard des ressources pour lesquelles vous souhaitez créer un nouveau groupe, puis cliquez sur **Ajouter au groupe**.
3. Dans l'arborescence de dossiers, sélectionnez le niveau parent du nouveau groupe, puis cliquez sur **Nouveau groupe statique**.

   Remarque
   La création de groupes statiques imbriqués n'est pas disponible pour les ressources de cloud à cloud.

4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Ajoutez un commentaire pour le groupe.
6. Cliquez sur **OK**.
   Le nouveau groupe apparaît dans l'arborescence de dossiers.
7. Cliquez sur **Terminé**.

Ajout de ressources à un groupe statique

Vous pouvez sélectionner le groupe cible en premier, puis lui ajouter des ressources.

Vous pouvez également sélectionner les ressources en premier, puis les ajouter à un groupe.

Pour ajouter des ressources à un groupe statique

Sélection du groupe cible en premier

1. Cliquez sur **Terminaux**, puis accédez au groupe cible.
2. Sélectionnez le groupe cible, puis cliquez sur **Ajouter des terminaux**.
3. Dans l'arborescence de dossiers, sélectionnez le groupe contenant les ressources requises.
4. Cochez les cases en regard des ressources que vous souhaitez ajouter, puis cliquez sur **Ajouter**.

© Acronis International GmbH, 2003-2026

Sélection des ressources en premier

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe root (superutilisateur) contenant les ressources requises.
2. Cochez les cases en regard des ressources que vous souhaitez ajouter, puis cliquez sur **Ajouter au groupe**.
3. Dans l'arborescence de dossiers, sélectionnez le groupe cible, puis cliquez sur **Terminé**.

Création d'un groupe dynamique

Vous créez un groupe dynamique en recherchant des ressources ayant des attributs spécifiques dont vous définissez les valeurs dans une requête de recherche. Enregistrez ensuite les résultats de la recherche en tant que groupe dynamique.

Les attributs pris en charge pour la recherche et la création de groupes dynamiques diffèrent pour les ressources de cloud à cloud et les ressources non-cloud à cloud. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 430) et "Rechercher des attributs pour les ressources de cloud à cloud" (p. 429).

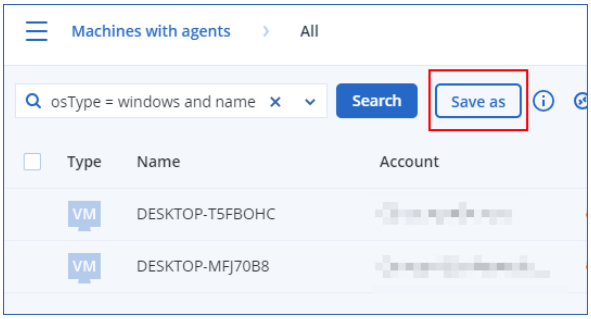
Les groupes dynamiques sont créés dans leurs groupes root (superutilisateur) respectifs. Les groupes dynamiques imbriqués ne sont pas pris en charge.

Vous ne pouvez pas créer de groupes de terminaux dans un groupe de type **Tout** tel que le groupe root (superutilisateur) **Tous les terminaux** ou dans des groupes intégrés tels que **Machines avec des agents** > **Tout**, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous les utilisateurs**.

Pour créer un groupe dynamique

Ressources autres que de cloud à cloud

1. Cliquez sur **Terminaux**, puis sélectionnez le groupe contenant les ressources pour lesquelles vous souhaitez créer un groupe dynamique.
2. Recherchez les ressources à l'aide des attributs et des opérateurs de recherche pris en charge.
   Vous pouvez utiliser plusieurs attributs et opérateurs dans une même requête. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 430).
3. Cliquez sur **Enregistrer sous** en regard du champ de recherche.



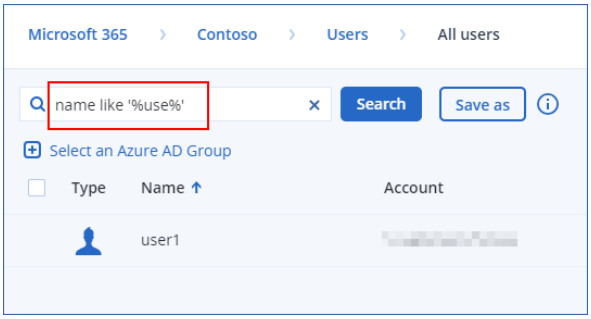
© Acronis International GmbH, 2003-2026

Remarque
Le bouton **Enregistrer sous** n'est pas disponible si vous n'êtes pas autorisé à créer un groupe dynamique à un niveau spécifique, par exemple dans le groupe racine **Terminaux** > **Tous les terminaux**.
Sélectionnez un autre niveau (par exemple, **Terminaux** > **Terminaux avec agents** > **Tous**), puis répétez les étapes ci-dessus. Avec cette recherche, vous pouvez créer un groupe dynamique dans **Terminaux avec agents**, et non dans **Terminaux avec agents** > **Tous**.

4. Indiquez le nom du nouveau groupe.
5. [Facultatif] Dans le champ **Commentaire**, ajoutez une description pour le nouveau groupe.
6. Cliquez sur **OK**.

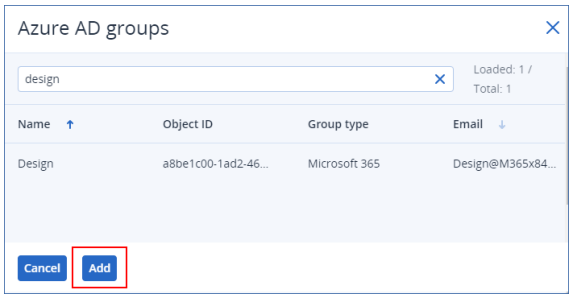
Ressources de cloud à cloud

1. Cliquez sur **Terminaux**, puis sélectionnez **Microsoft 365** ou **Google Workspace**.
2. Sélectionnez le groupe qui contient les ressources pour lesquelles vous souhaitez créer un nouveau groupe dynamique. Par exemple, **Utilisateurs** > **Tous les utilisateurs**.
3. Recherchez les ressources à l'aide des attributs et des opérateurs de recherche pris en charge, ou en sélectionnant des utilisateurs de Microsoft 365 dans un groupe Active Directory spécifique.
   Vous pouvez utiliser plusieurs attributs et opérateurs dans une même requête. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources de cloud à cloud" (p. 429).



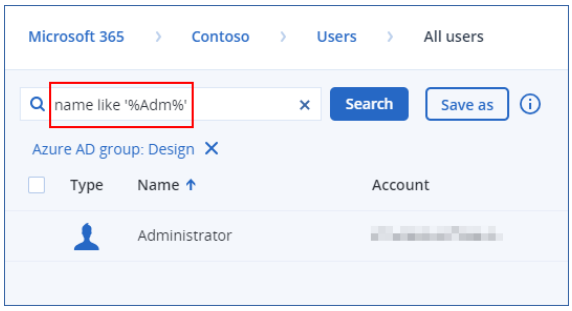
4. [Uniquement pour **Microsoft 365** > **Utilisateurs**] Pour sélectionner des utilisateurs dans un groupe Active Directory spécifique, procédez comme suit :
   a. Accédez à **Utilisateurs** > **Tous les utilisateurs**.
   b. Cliquez sur **Sélectionnez un groupe Azure AD**.
      La liste des groupes Active Directory de votre organisation s'affiche.
      Vous pouvez rechercher dans cette liste un groupe spécifique, ou trier les groupes par nom ou par adresse e-mail.
   c. Sélectionnez le groupe Active Directory souhaité, puis cliquez sur **Ajouter**.

© Acronis International GmbH, 2003-2026



d. [Facultatif] Pour inclure ou exclure des utilisateurs spécifiques du groupe Active Directory sélectionné, créez une requête de recherche à l'aide des attributs et opérateurs de recherche pris en charge.

   Vous pouvez utiliser plusieurs attributs et opérateurs dans une même requête. Pour plus d'informations sur les attributs pris en charge, voir "Rechercher des attributs pour les ressources de cloud à cloud" (p. 429).



5. Cliquez sur **Enregistrer sous** en regard du champ de recherche.

Remarque
Le bouton **Enregistrer sous** n'est pas disponible si vous n'êtes pas autorisé à créer un groupe dynamique à un niveau spécifique. Par exemple, dans **Microsoft 365** > votre organisation > **Utilisateurs**.

Sélectionnez un autre niveau (par exemple, **Microsoft 365** > votre organisation > **Utilisateurs** > **Tous**), puis répétez les étapes ci-dessus. Avec cette recherche, vous pouvez créer un groupe dynamique dans **Microsoft 365** > votre organisation > **Utilisateurs** >, et non dans **Utilisateurs** > **Tous**.

6. Indiquez le nom du nouveau groupe.
7. [Facultatif] Dans le champ **Commentaire**, ajoutez une description pour le nouveau groupe.
8. Cliquez sur **OK**.

Opérateurs de recherche

Le tableau suivant récapitule les opérateurs que vous pouvez utiliser dans vos requêtes de recherche.

Vous pouvez utiliser plusieurs opérateurs dans une même requête.

© Acronis International GmbH, 2003-2026

Opérateur	Pris en charge pour	Signification	Exemples
`AND`	Toutes les ressources	Opérateur de conjonction logique	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Toutes les ressources	Opérateur de disjonction logique	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Toutes les ressources	Opérateur de négation logique	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Toutes les ressources	Cet opérateur vérifie si une expression correspond à une valeur d'une liste.	`osType IN ('windows', 'linux')`
`NOT IN`	Toutes les ressources	Cet opérateur est l'opposé de l'opérateur `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wildcard pattern'`	Toutes les ressources	Cet opérateur vérifie si une expression correspond au modèle de caractères génériques.
		Vous pouvez utiliser les opérateurs de caractères génériques suivants :
		• * ou % L'astérisque et le symbole du pourcentage représentent zéro, un ou plusieurs caractères.
		• _ Le tiret bas représente un seul caractère.
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

`NOT LIKE 'wildcard pattern'`	Toutes les ressources	Cet opérateur est l'opposé de l'opérateur `LIKE`.
		Vous pouvez utiliser les opérateurs de caractères génériques suivants :
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

© Acronis International GmbH, 2003-2026

Opérateur	Pris en charge pour	Signification	Exemples
		• * ou % L'astérisque et le symbole du pourcentage représentent zéro, un ou plusieurs caractères. • _ Le tiret bas représente un seul caractère.	

`RANGE (<starting_value>, <ending_value>)`	Toutes les ressources	Cet opérateur vérifie si une expression est comprise dans une plage (inclusive) de valeurs.
		Les requêtes avec chaînes alphanumériques utilisent l'ordre de tri ASCII, mais ne font pas la différence entre les majuscules et les minuscules.
			`ip RANGE('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Avec cette requête, vous pouvez filtrer tous les noms commençant par A, B et C, tels qu'`Alice`, `Bob`, `Claire`. En revanche, seule la lettre D répond aux exigences. Par conséquent, les noms comportant plus de lettres tels que `Diana` ou `Don` ne seront pas inclus.
			Pour obtenir le même résultat, vous pouvez également utiliser la requête suivante :
			`name >= 'a' AND name <= 'd'`

= ou ==	Toutes les ressources	Opérateur *Égal à*	`osProductType = 'server'`
!= ou <>	Toutes les ressources	Opérateur *Différent de*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Ressources autres que de cloud à cloud	Opérateur *Inférieur à*	`memorySize < 1024`
>	Ressources autres que de cloud à cloud	Opérateur *Supérieur à*.	`diskSize > 300GB`
<=	Ressources autres que de cloud à cloud	Opérateur *Inférieur ou égal à*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Ressources	Opérateur *Supérieur ou*	`nextBackupTime >= '2022-08-11'`

© Acronis International GmbH, 2003-2026

Opérateur	Pris en charge pour	Signification	Exemples
	autres que de cloud à cloud	*égal à*	

Rechercher des attributs pour les ressources de cloud à cloud

Le tableau suivant récapitule les attributs que vous pouvez utiliser dans vos requêtes de recherche pour les ressources Microsoft 365 et Google Workspace.

Pour voir quels attributs vous pouvez utiliser dans les requêtes de recherche pour d'autres types de ressources, consultez "Rechercher des attributs pour les ressources autres que cloud à cloud" (p. 430).

Attribut	Signification	Utilisable dans	Exemples de requête de recherche	Pris en charge pour la création de groupe
`name`	Nom affiché d'une ressource Microsoft 365 ou Google Workspace	Toutes les ressources de cloud à cloud	`name = 'My Name'` `name LIKE '*nam*'`	Oui

`email`	Adresse e-mail d'un utilisateur ou d'un groupe Microsoft 365, ou d'un utilisateur Google Workspace	Microsoft 365 > Groupes
		Microsoft 365 > Utilisateurs
		Google Workspace > Utilisateurs
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				Oui

`siteName`	Nom d'un site associé à un groupe Microsoft 365	Microsoft 365 > Groupes	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Oui
`url`	Adresse Web d'un groupe Microsoft 365 ou d'un site SharePoint	Microsoft 365 > Groupes Microsoft 365 > Collections de sites	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Oui
`licensedByMsft`	Les utilisateurs qui	Microsoft 365 > Utilisateurs	`licensedByMsft = true`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Utilisable dans	Exemples de requête de recherche	Pris en charge pour la création de groupe
	ont une licence d'abonnement Microsoft 365 valide. Les utilisateurs licenciés peuvent utiliser les services Microsoft 365, tels qu'Exchange Online et OneDrive.		`licensedByMsft = false`	
`msftSignInBlocked`	Les utilisateurs qui ont été restreints de se connecter à Microsoft 365. Les utilisateurs bloqués ne peuvent pas utiliser les services Microsoft 365.	Microsoft 365 > Utilisateurs	`msftSignInBlocked = true` `msftSignInBlocked = false`	Oui

Rechercher des attributs pour les ressources autres que cloud à cloud

Le tableau suivant récapitule les attributs que vous pouvez utiliser dans vos requêtes de recherche pour les ressources autres que cloud à cloud.

Pour voir quels attributs vous pouvez utiliser dans les requêtes de recherche pour les ressource cloud à cloud, consultez "Rechercher des attributs pour les ressources de cloud à cloud" (p. 429).

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
Général			
`name`	Nom de la ressource, par exemple : • Nom d'hôte pour les	`name = 'en-00'`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	machines physiques • Nom des machines virtuelles • Nom de la base de données • Adresse électronique pour les boîtes aux lettres		
`id`	Identifiant du terminal. Pour afficher l'identifiant du terminal, sous **Terminaux**, sélectionnez le terminal, puis cliquez sur **Détails** > **Toutes les propriétés**. L'identifiant apparaît dans le champ `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Oui

`resourceType`	Type de ressource
	Valeurs possibles :
	• `'machine'`
	• `'exchange'`
	• `'mssql_server'`
	• `'mssql_instance'`
	• `'mssql_database'`
	• `'mssql_database_folder'`
	• `'msexchange_database'`
	• `'msexchange_storage_group'`
	• `'msexchange_mailbox.msexchange'`
	• `'msexchange_mailbox.office365'`
	• `'mssql_aag_group'`
	• `'mssql_aag_database'`
	• `'virtual_machine.vmww'`
	• `'virtual_machine.vmwesx'`
		`resourceType = 'machine'`
		`resourceType in ('virtual_center.vmwesx', 'machine')`
		Remarque
		Certains types de ressources, tels que MS SQL et MS Exchange, peuvent être pris en compte en tant que groupes de ressources. Si votre recherche ou votre requête de groupe dynamique ne renvoie pas les résultats attendus, essayez d'ajouter le préfixe `group.` au début du nom de la ressource. Voir "Type de groupe de ressources" (p. 433).
			Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• 'virtual_host.vmwesx' • 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • virtual_machine.vcd		

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `virtual_machine.ovirt` • `virtual_machine.azure` • `virtual_machine.nutanix` • `'bootable_media'`		

	Type de groupe de ressources
	
	Valeurs possibles :
	• `group.computers`
	• `group.mssql_server`
	• `group.mssql_instance`
	• `group.mssql_system_databases`
	• `group.mssql_database`
	• `group.mssql_aag_group`
	• `group.mssql_aag_replica`
	• `group.mssql_aag_database`
	• `group.msexchange_cluster`
	• `group.msexchange_server`
	• `group.msexchange_cas`
	• `group.msexchange_online_server`
	• `group.msexchange_infostore`
	• `group.msexchange_storage_group`
	• `group.msexchange_database`
	• `group.msexchange_mailboxes`
	• `group.social_resources`
	• `group.all`
	• `group.all_vcd_vms`
		`resourceType = 'group.mssql_server'`
		
		`resourceType in ('group.mssql_database', 'group.msexchange_database')`
			Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `group.vcd` • `group.vcenter` • `group.ovirt_vengine` • `group.veil_vengine` • `group.nutanix_vengine` • `group.datacenter` • `group.hosts_and_clusters` • `group.cluster` • `group.host` • `group.virtual_application` • `group.resource_pool` • `group.virtual_folder` • `group.vms_and_templates` • `group.vms_folder` • `group.virtual_project` • `group.nas_devices` • `group.vcd_organization` • `group.vcd_organizations` • `group.azure` • `group.azure_subscriptions` • `group.azure_subscription` • `group.azure_resource_group` • `group.azure_all_devices` • `group.externalrmm` • `group.mail_servers`		
`chassis`	Type de châssis. Valeurs possibles : • `laptop`	`chassis = 'laptop'` `chassis IN ('laptop', 'desktop')`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `desktop` • `server` • `other` • `unknown`		
`ip`	Adresse IP (uniquement pour les machines physiques).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Oui
`comment`	Commentaire pour un terminal. Il peut être spécifié automatiquement ou manuellement. Valeur par défaut : • Pour les machines physiques sous Windows, la description de l'ordinateur dans Windows est automatiquement copiée en tant que commentaire. Cette valeur est synchronisée toutes les 15 minutes. • Vide pour d'autres terminaux. **Remarque** La synchronisation automatique est désactivée si du texte est ajouté manuellement dans le champ de commentaire. Pour réactiver la synchronisation, effacez ce texte. Pour actualiser les commentaires automatiquement	`comment = 'important machine'` `comment = ''` (toutes les machines sans commentaire)	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe

	synchronisés pour vos ressources, redémarrez le service de machine gérée dans **Services Windows** ou exécutez les commandes suivantes dans l'invite de commandes :
	`net stop mms`
	`net start mms`
	Pour afficher un commentaire concernant un terminal, sous **Terminaux**, sélectionnez le terminal, cliquez sur **Détails**, puis localisez la section **Commentaire**.
	Pour ajouter ou modifier un commentaire manuellement, cliquez sur **Ajouter** ou **Modifier**.
	Pour les terminaux sur lesquels un agent de protection est installé, il existe deux champs de commentaire distincts :
	• Commentaire sur l'agent
	◦ Pour les machines physiques sous Windows, la description de l'ordinateur dans Windows est automatiquement copiée en tant que commentaire. Cette valeur est		

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	synchronisée toutes les 15 minutes. ◦ Vide pour d'autres terminaux. **Remarque** La synchronisation automatique est désactivée si du texte est ajouté manuellement dans le champ de commentaire. Pour réactiver la synchronisation, effacez ce texte. • Commentaires sur le terminal ◦ Si le commentaire sur l'agent est automatiquement spécifié, il est copié en tant que commentaire sur le terminal. Les commentaires sur l'agent ajoutés manuellement ne sont pas copiés en tant que commentaires sur le terminal. ◦ Les commentaires sur le terminal ne sont pas copiés en tant que commentaires sur l'agent. Concernant un terminal, l'un de ces champs de commentaire peut être rempli, ou les deux, ou		

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	encore les deux peuvent être laissés vierges. Si les deux commentaires sont spécifiés, le commentaire sur le terminal sera prioritaire. Pour afficher un commentaire sur un agent, sous **Paramètres** > **Agents**, sélectionnez un terminal avec l'agent, cliquez sur **Détails**, puis localisez la section **Commentaire**. Pour afficher un commentaire concernant un terminal, sous **Terminaux**, sélectionnez le terminal, cliquez sur **Détails**, puis localisez la section **Commentaire**. Pour ajouter ou modifier un commentaire manuellement, cliquez sur **Ajouter** ou **Modifier**.		
`isOnline`	Disponibilité de la ressource. Valeurs possibles : • `true` • `false`	`isOnline = true`	Non
`hasAsz`	Disponibilité de la zone sécurisée. Valeurs possibles : • `true` • `false`	`hasAsz = true`	Oui
`tzOffset`	Décalage UTC, en minutes.	`tzOffset = 120`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
		`tzOffset > 120` `tzOffset < 120`	
CPU, mémoire, disques			
`cpuArch`	Architecture du processeur. Valeurs possibles : • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Oui
`cpuName`	Nom du processeur.	`cpuName LIKE '%XEON%'`	Oui
`memorySize`	Taille de la mémoire RAM en mégaoctets.	`memorySize < 1024`	Oui
`diskSize`	Taille du disque dur en gigaoctets ou en mégaoctets (uniquement pour les machines physiques).	`diskSize < 300GB` `diskSize >= 3000000MB`	Non
Système d'exploitation			
`osName`	Nom du système d'exploitation.	`osName LIKE '%Windows XP%'`	Oui
`osType`	Type de système d'exploitation. Valeurs possibles : • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Oui
`osArch`	Architecture du système d'exploitation. Valeurs possibles : • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Oui
`osProductType`	Type de produit du système d'exploitation.	`osProductType = 'server'`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	Valeurs possibles : • `'dc'` Représente le contrôleur de domaine. **Remarque** Lorsque le rôle de contrôleur de domaine est affecté à un serveur Windows, la valeur `osProductType` passe de `server` à `dc`. Ces ordinateurs ne seront pas inclus dans les résultats de recherche pour `osProductType='server'`. • `'server'` • `'workstation'`		
`osSp`	Service Pack du système d'exploitation.	`osSp = 1`	Oui
`osVersionMajor`	Version majeure du système d'exploitation.	`osVersionMajor = 1`	Oui
`osVersionMinor`	Version mineure du système d'exploitation.	`osVersionMinor > 1`	Oui
Agent			
`agentVersion`	Version de l'agent de protection installé.	`agentVersion LIKE '12.0.*'`	Oui
`hostId`	Identifiant interne de l'agent de protection. Pour afficher l'identifiant de l'agent de protection, sous **Terminaux**, sélectionnez le terminal, puis cliquez **Détails** > **Toutes les**	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	propriétés. Vérifiez la valeur `id` de la propriété `agent`.		
`virtualType`	Type de machine virtuelle. Valeurs possibles : • `'vmwesx'` Machines virtuelles VMware • `'mshyperv'` Les machines virtuelles Hyper-V • `'pcs'` Machines virtuelles Virtuozzo • `'hci'` Machines virtuelles Virtuozzo Hybrid Infrastructure • `'scale'` Machines virtuelles Scale Computing HC3 • `'ovirt'` Machines virtuelles oVirt. • `'vcd'` VMware Cloud Director machines virtuelles	`virtualType = 'vmwesx'`	Oui
`insideVm`	Machine virtuelle avec un agent. Valeurs possibles : • `true` • `false`	`insideVm = true`	Oui
Emplacement			
`tenant`	Nom du tenant auquel appartient le terminal.	`tenant = 'Unit 1'`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
`tenantId`	Identificateur du tenant auquel appartient le terminal. Pour afficher l'identifiant du tenant, sous **Terminaux**, sélectionnez le terminal, puis cliquez **Détails** > **Toutes les propriétés**. L'identifiant apparaît dans le champ `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Oui
`ou`	Terminaux appartenant à l'unité organisationnelle Active Directory spécifiée.	`ou IN ('RnD', 'Computers')`	Oui
`customerUuid`	Les terminaux qui appartiennent à l'identifiant de tenant du **Client** spécifié.	`customerUuid = 'd96c5dde-5466-489d-9c74-df7dbd8c2148'`	Non
Statut			
`state`	État du terminal. Valeurs possibles : • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'`	`state = 'backup'`	Non

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `'resizeAsz'`		
status	État de protection. Valeurs possibles : • `ok` • `warning` • `error` • `critical` • `protected` • `notProtected`	`status = 'ok'` `status IN ('error', 'warning')`	Non
`protectedByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné. Pour voir l'identifiant du plan, sélectionnez un plan dans **Gestion** > **Plans de protection**, cliquez sur la barre dans la colonne **État**, puis cliquez sur le nom de l'état. Une nouvelle recherche avec l'identifiant du plan sera créée.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`okByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **OK**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`errorByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **Erreur**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`warningByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **Avertissement**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`runningByPlan`	Terminaux protégés par un plan de protection avec un	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	identifiant donné et un état **En cours d'exécution**.		
`interactionByPlan`	Terminaux protégés par un plan de protection avec un identifiant donné et un état **Intervention requise**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non

`lastBackupTime*`	Date et heure de la dernière sauvegarde réussie.
	Le format est « `AAAA-MM-JJ HH:MM` ».
		`lastBackupTime > '2023-03-11'`
		`lastBackupTime <= '2023-03-11 00:15'`
		`lastBackupTime is null`
			Non

`lastBackupTryTime*`	Heure de la dernière tentative de sauvegarde. Le format est « `AAAA-MM-JJ HH:MM` ».	`lastBackupTryTime >= '2023-03-11'`	Non
`nextBackupTime*`	Heure de la prochaine sauvegarde. Le format est « `AAAA-MM-JJ HH:MM` ».	`nextBackupTime >= '2023-08-11'`	Non

`lastVAScanTime*`	Date et heure de la dernière évaluation des vulnérabilités réussie.
	Le format est « `AAAA-MM-JJ HH:MM` ».
		`lastVAScanTime > '2023-03-11'`
		`lastVAScanTime <= '2023-03-11 00:15'`
		`lastVAScanTime is null`
			Oui

`lastVAScanTryTime*`	Heure de la dernière tentative d'évaluation des vulnérabilités. Le format est « `AAAA-MM-JJ HH:MM` ».	`lastVAScanTimeTryTime >= '2022-03-11'`	Oui
`nextVAScanTime*`	Heure de la prochaine évaluation des vulnérabilités. Le format est « `AAAA-MM-JJ HH:MM` ».	`nextVAScanTime <= '2023-08-11'`	Oui

© Acronis International GmbH, 2003-2026

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
`network_status`	Statut d'isolation réseau pour Endpoint Detection and Response (EDR). Valeurs possibles : • `connected` • `isolated`	`network_status= 'connected'`	Oui

Remarque
Si vous n'indiquez pas la valeur des heures et des minutes, l'heure de début est considérée comme étant AAAA-MM-JJ 00:00 et l'heure de fin est considérée comme étant AAAA-MM-JJ 23:59:59. Par exemple, `lastBackupTime = 2023-01-20` signifie que les résultats de recherche incluront toutes les sauvegardes de l'intervalle
`lastBackupTime >= 2023-01-20 00:00` et `lastBackupTime <= 2023-01-20 23:59:59`.

Modification d'un groupe dynamique

Vous modifiez un groupe dynamique en changeant la requête de recherche qui définit le contenu du groupe.

Dans les groupes dynamiques basés sur Active Directory, vous pouvez également modifier le groupe Active Directory.

Pour modifier un groupe dynamique

En modifiant la requête de recherche

1. Cliquez sur **Terminaux**, accédez au groupe dynamique que vous souhaitez modifier, puis sélectionnez-le.
2. Cliquez sur l'icône en forme d'engrenage située à côté du nom du groupe, puis sur **Modifier**. Vous pouvez également cliquer sur **Modifier** dans le volet **Actions**.
3. Modifiez la requête de recherche en changeant les attributs de recherche, leurs valeurs ou les opérateurs de recherche, puis cliquez sur **Rechercher**.
4. Cliquez sur **Enregistrer** en regard du champ de recherche.

En modifiant le groupe Active Directory

Remarque
Cette procédure s'applique aux groupes dynamiques basés sur Active Directory. Les groupes dynamiques basés sur Active Directory ne sont disponibles que dans **Microsoft 365** > **Utilisateurs**.

© Acronis International GmbH, 2003-2026

1. Cliquez sur **Terminaux**, accédez à **Terminaux** > **Microsoft 365** > votre organisation > **Utilisateurs**.
2. Sélectionnez le groupe dynamique que vous souhaitez modifier.
3. Cliquez sur l'icône en forme d'engrenage située à côté du nom du groupe, puis sur **Modifier**. Vous pouvez également cliquer sur **Modifier** dans le volet **Actions**.
4. Modifiez le contenu du groupe en effectuant l'une des opérations suivantes :
   - Modifiez le groupe Active Directory déjà sélectionné en cliquant sur son nom, puis en sélectionnant un nouveau groupe Active Directory dans la liste qui s'affiche.
   - Modifiez la requête de recherche, puis cliquez sur **Rechercher**.
     La requête de recherche est limitée au groupe Active Directory sélectionné.
5. Cliquez sur **Enregistrer** en regard du champ de recherche.

Vous pouvez également enregistrer vos modifications sans remplacer le groupe actuel. Pour enregistrer la configuration modifiée en tant que nouveau groupe, cliquez sur le bouton fléché en regard du champ de recherche, puis cliquez sur **Enregistrer sous**.

Remarque
Les groupes créés à l'aide de l'option **Enregistrer sous** héritent des critères de découverte du groupe dynamique d'origine. Ainsi, les nouveaux critères de découverte que vous configurez sont ajoutés aux critères hérités et enregistrés dans le nouveau groupe dynamique.

Seuls les groupes créés à partir de la catégorie de groupe **Tout** n'héritent pas des critères.

Suppression d'un groupe

Lorsque vous supprimez un groupe de terminaux, tous les plans appliqués à ce groupe sont révoqués. Les ressources du groupe ne sont plus protégées si aucun autre plan ne leur est appliqué.

Pour supprimer un groupe de terminaux

1. Cliquez sur **Terminaux**, puis accédez au groupe que vous souhaitez supprimer.
2. Cliquez sur l'icône en forme d'engrenage située à côté du nom du groupe, puis sur **Supprimer**.
3. Confirmez votre choix en cliquant sur **Supprimer**.

Application d'un plan à un groupe

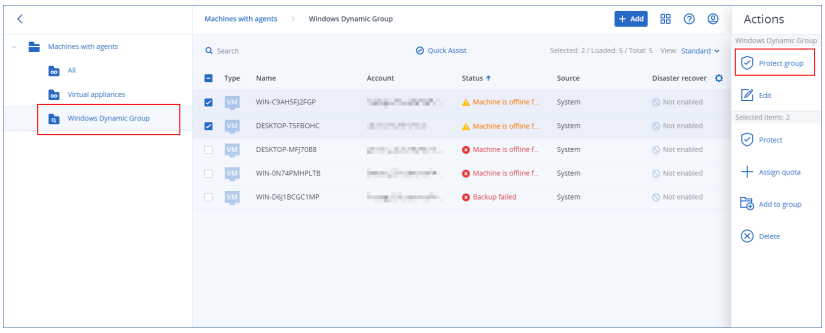
Vous pouvez appliquer un plan à un groupe en sélectionnant d'abord le groupe, puis en lui attribuant un plan.

Vous pouvez également ouvrir un plan pour le modifier, puis lui ajouter un groupe.

Pour appliquer un plan à un groupe

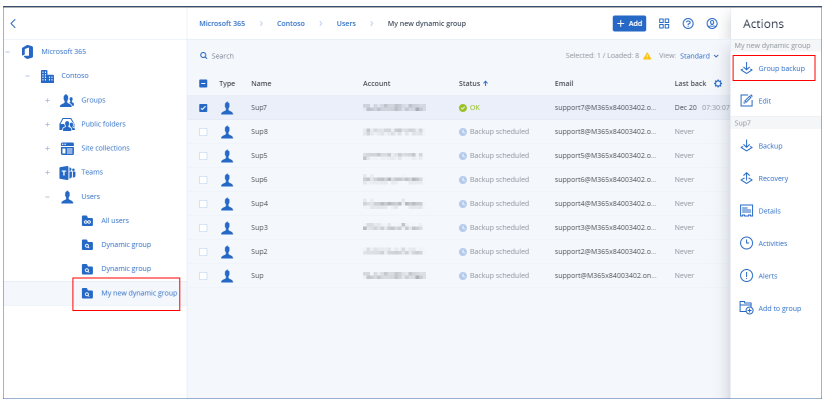
1. Cliquez sur **Terminaux**, puis accédez au groupe auquel vous souhaitez appliquer un plan.
2. [Pour les ressources autres que de cloud à cloud] Cliquez sur **Protéger un groupe**.

© Acronis International GmbH, 2003-2026



La liste des plans pouvant être appliqués s'affiche.

3. [Pour les ressources de cloud à cloud] Cliquez sur **Sauvegarde de groupe**.



La liste des plans de sauvegarde pouvant être appliqués s'affiche.

4. [Pour appliquer un plan existant] Sélectionnez le plan, puis cliquez sur **Appliquer**.
5. [Pour créer un nouveau plan] Cliquez sur **Création d'un plan**, sélectionnez le type de plan, puis créez le nouveau plan.

   Pour plus d'informations sur les types de plans disponibles et sur leur création, reportez-vous à "Plans pris en charge pour les groupes de terminaux" (p. 421).

Remarque
Les plans de sauvegarde appliqués aux groupes de terminaux cloud à cloud sont planifiés automatiquement pour s'exécuter une fois par jour. Vous ne pouvez pas exécuter ces plans à la demande en cliquant sur **Exécuter maintenant**.

Révocation d'un plan à partir d'un groupe

Vous pouvez révoquer un plan à partir d'un groupe en sélectionnant d'abord le groupe, puis en révoquant le plan.

Vous pouvez également ouvrir le plan pour le modifier, puis en supprimer le groupe.

Pour révoquer un plan à partir d'un groupe

1. Cliquez sur **Terminaux**, puis accédez au groupe depuis lequel vous souhaitez révoquer un plan.
2. [Pour les ressources autres que de cloud à cloud] Cliquez sur **Protéger un groupe**.
   La liste des plans appliqués au groupe s'affiche.

© Acronis International GmbH, 2003-2026

3. [Pour les ressources de cloud à cloud] Cliquez sur **Sauvegarde de groupe**.
   La liste des plans de sauvegarde appliqués au groupe s'affiche.
4. Sélectionnez le plan que vous souhaitez révoquer.
5. [Pour les ressources autres que de cloud à cloud] Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Retirer**.
6. [Pour les ressources de cloud à cloud] Cliquez sur l'icône représentant un engrenage, puis cliquez sur **Retirer**.

Utilisation du module de contrôle des terminaux

Dans le cadre des plans de protection du service Cyber Protection, le module de contrôle des terminaux[1] tire parti d'un sous-ensemble fonctionnel de l'agent de prévention des pertes de données[2] sur chaque ordinateur protégé afin de détecter et de prévenir la consultation et la transmission non autorisées de données via les canaux de l'ordinateur local. Il offre un contrôle précis d'un large éventail de voies de fuites de données, y compris l'échange de données à l'aide de supports amovibles, d'imprimantes, de terminaux virtuels et redirigés, et du presse-papiers Windows.

Ce module est disponible pour les éditions Cyber Protect Essentials, Cyber Protect Standard et Cyber Protect Advanced, sous licence en fonction de la ressource.

Remarque
Sur les ordinateurs Windows, les fonctionnalités de contrôle des terminaux nécessitent l'installation de l'agent de prévention des pertes de données. Celui-ci sera installé automatiquement pour les ressources protégées si le module **Contrôle des terminaux** est activé dans leurs plans de protection.

[1] Dans le cadre d'un plan de protection, le module de contrôle des terminaux tire parti d'un sous-ensemble fonctionnel de l'agent de prévention des pertes de données sur chaque ordinateur protégé afin de détecter et de prévenir la consultation et la transmission non autorisées de données via les canaux de l'ordinateur local. Cela comprend l'accès de l'utilisateur aux ports et périphériques, l'impression de documents, les opérations de copier-coller, le formatage des supports et les opérations d'éjection, ainsi que les synchronisations aux terminaux mobiles connectés localement. Le module de contrôle des terminaux offre un contrôle granulaire et contextuel sur les types de terminaux et de ports auxquels les utilisateurs peuvent accéder sur l'ordinateur protégé, ainsi que les actions que ces utilisateurs peuvent réaliser sur ces terminaux.

[2] Un composant client du système de prévention des pertes de données qui protège son ordinateur hôte contre l'utilisation, la transmission et le stockage non autorisés de données confidentielles, protégées ou sensibles en appliquant une combinaison de techniques d'analyse de contexte et de contenu et en mettant en œuvre des politiques de prévention des pertes de données gérées de manière centralisée. Cyber Protection propose un agent de prévention des pertes de données complet. Toutefois, la fonctionnalité de l'agent sur un ordinateur protégé est limitée à l'ensemble de fonctionnalités de prévention des pertes de données disponibles sous licence dans Cyber Protection, et dépend du plan de protection appliqué à cet ordinateur.

© Acronis International GmbH, 2003-2026

Le module de contrôle des terminaux s'appuie sur les fonctions de prévention des pertes de données[1] de l'agent afin d'imposer un contrôle contextuel de l'accès aux données et des opérations de transfert sur l'ordinateur protégé. Cela comprend l'accès de l'utilisateur aux ports et périphériques, l'impression de documents, les opérations de copier-coller, le formatage des supports et les opérations d'éjection, ainsi que les synchronisations aux terminaux mobiles connectés localement. L'agent de prévention des pertes de données comprend un framework pour tous les composants centraux de gestion et d'administration du module de contrôle des terminaux, et doit donc être installé sur chaque ordinateur à protéger avec le module de contrôle des terminaux. L'agent autorise, restreint ou refuse les actions des utilisateurs en fonction des paramètres de contrôle des terminaux qu'il reçoit de la part du plan de protection appliqué à l'ordinateur protégé.

Le module de contrôle des terminaux contrôle l'accès à différents périphériques, qu'ils soient utilisés directement sur des ordinateurs protégés ou redirigés dans des environnements de virtualisation hébergés sur des ordinateurs protégés. Il reconnaît les terminaux redirigés dans Microsoft Remote Desktop Server, Citrix XenDesktop/XenApp/XenServer et VMware Horizon. Il peut également contrôler les opérations de copies de données entre le presse-papiers du système d'exploitation invité exécuté sur VMware Workstation/Player, Oracle VM VirtualBox ou Windows Virtual PC, et le presse-papiers du système d'exploitation hôte exécuté sur l'ordinateur protégé.

Le module de contrôle des terminaux peut protéger les ordinateurs exécutant les systèmes d'exploitation suivants :

Contrôle des terminaux

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 – Windows Server 2022
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)

Remarque
Agent for Data Loss Prevention pour macOS ne prend en charge que les processeurs x64. Les processeurs Apple Silicon ARM ne sont pas supportés.

Prévention des pertes de données

[1]Un système de technologies intégrées et de mesures organisationnelles destinées à détecter et à prévenir la divulgation/consultation accidentelle ou intentionnelle de données confidentielles, protégées ou sensibles par des entités non autorisées, au sein ou en dehors de l'organisation, ou le transfert de telles données vers des environnements non dignes de confiance.

© Acronis International GmbH, 2003-2026

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 – Windows Server 2022

Remarque
Agent for Data Loss Prevention peut être installé sur des systèmes macOS non pris en charge, car il fait partie intégrante d'Agent for Mac. Dans ce cas, la console Cyber Protect indiquera que Agent for Data Loss Prevention est installé sur l'ordinateur, mais les fonctionnalités de contrôle des terminaux et de prévention des pertes de données ne fonctionneront pas. La fonctionnalité de contrôle des terminaux ne fonctionnera que sur les systèmes macOS supporté par Agent for Data Loss Prevention.

Limitation de l'utilisation de l'agent de prévention des pertes de données avec Hyper-V

N'installez pas l'agent de prévention des pertes de données sur des hôtes Hyper-V dans des clusters Hyper-V, car cela pourrait entraîner des problèmes d'écran bleu de la mort (BSOD), principalement dans les clusters Hyper-V avec des volumes partagés de cluster (CSV).

Si vous utilisez l'une des versions suivantes de l'agent pour Hyper-V, vous devez supprimer manuellement l'agent de prévention des pertes de données :

- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

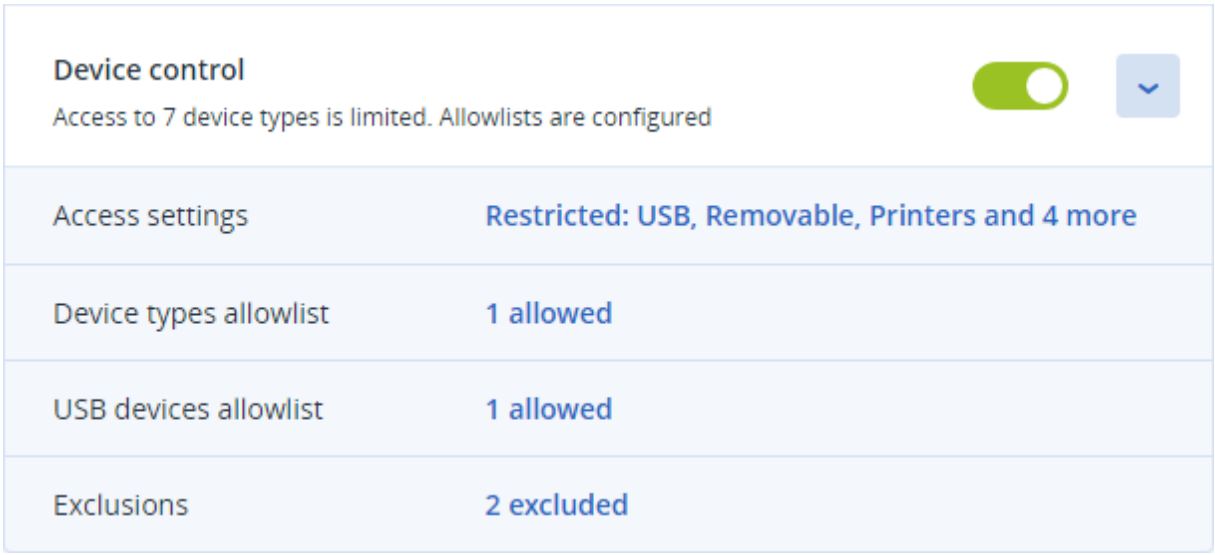
Pour supprimer l'agent de prévention des pertes de données, sur l'hôte Hyper-V, exécutez manuellement le programme d'installation et désélectionnez la case Agent pour empêcher les pertes de données, ou exécutez la commande suivante :

```
<installer_name> --remove-components=agentForDlp -quiet
```

Vous pouvez activer et configurer le module de contrôle des terminaux dans la section **Contrôle des terminaux** de votre plan de protection dans la console Cyber Protect. Pour obtenir des instructions, consultez les étapes pour activer ou désactiver le contrôle des terminaux.

© Acronis International GmbH, 2003-2026

La section **Contrôle des terminaux** affiche un résumé de la configuration du module :



- Paramètres d'accès : affiche un résumé des types de terminaux et des ports avec accès restreint (refusé ou en lecture seule), le cas échéant. Sinon, indique que tous les types de terminaux sont autorisés. Cliquez sur ce résumé pour consulter ou modifier les paramètres d'accès (consultez les étapes pour consulter ou modifier les paramètres d'accès).
- Liste d'autorisation des types de terminaux : affiche le nombre de sous-classes de terminaux autorisées en étant exclues du contrôle d'accès des terminaux, le cas échéant. Sinon, indique que la liste d'autorisation est vide. Cliquez sur ce résumé pour consulter ou modifier la sélection de sous-classes de terminaux autorisées (consultez les étapes pour exclure des sous-classes de terminaux du contrôle d'accès).
- Liste d'autorisation des terminaux USB : affiche le nombre de modèles/terminaux USB autorisés en étant exclus du contrôle d'accès des terminaux, le cas échéant. Sinon, indique que la liste d'autorisation est vide. Cliquez sur ce résumé pour consulter ou modifier la liste de modèles/terminaux USB (consultez les étapes pour exclure des terminaux USB individuels du contrôle d'accès).
- Exclusions : affiche le nombre d'exclusions de contrôle d'accès qui ont été définies pour le presse-papiers Windows, les captures d'écran, les imprimantes et les terminaux mobiles.

Utilisation du contrôle des terminaux

Cette section donne des instructions pas à pas pour effectuer des tâches de base lors de l'utilisation du module de contrôle des terminaux.

Activer ou désactiver le contrôle des terminaux

Vous pouvez activer le contrôle des terminaux lors de la création d'un plan de protection. Vous pouvez modifier un plan de protection existant afin d'activer ou de désactiver le contrôle des terminaux.

Pour activer ou désactiver le contrôle des terminaux

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Effectuez l'une des actions suivantes pour ouvrir le panneau du plan de protection :
   - Si vous souhaitez créer un plan de protection, sélectionnez un ordinateur à protéger, cliquez sur **Protection**, puis sur **Création d'un plan**.
   - Si vous souhaitez modifier un plan de protection existant, sélectionnez une machine protégée, cliquez sur **Protection**, sur les points de suspension (...) à côté du nom du plan de protection, puis sur **Modifier**.
3. Dans le panneau du plan de protection, accédez à la zone **Contrôle des terminaux**, et activez ou désactivez **Contrôle des terminaux**.
4. Effectuez l'une des actions suivantes pour appliquer vos modifications :
   - Si vous créez un plan de protection, cliquez sur **Créer**.
   - Si vous modifiez un plan de protection, cliquez sur **Enregistrer**.

Vous pouvez également accéder au panneau du plan de protection depuis l'onglet Gestion. Toutefois, cette fonctionnalité n'est pas disponible dans toutes les éditions du service Cyber Protection.

Activer l'utilisation du module de contrôle de terminaux sur macOS

Les paramètres de contrôle de terminaux d'un plan de protection ne deviennent effectifs qu'une fois le lecteur de contrôle de terminaux chargé sur la ressource protégée. Cette section décrit comment charger le lecteur de contrôle de terminaux pour permettre l'utilisation du module de contrôle de terminaux sur macOS. Cette opération ne doit être effectuée qu'une seule fois, mais requiert les privilèges administrateur sur l'ordinateur de terminal.

Versions de macOS prises en charge :

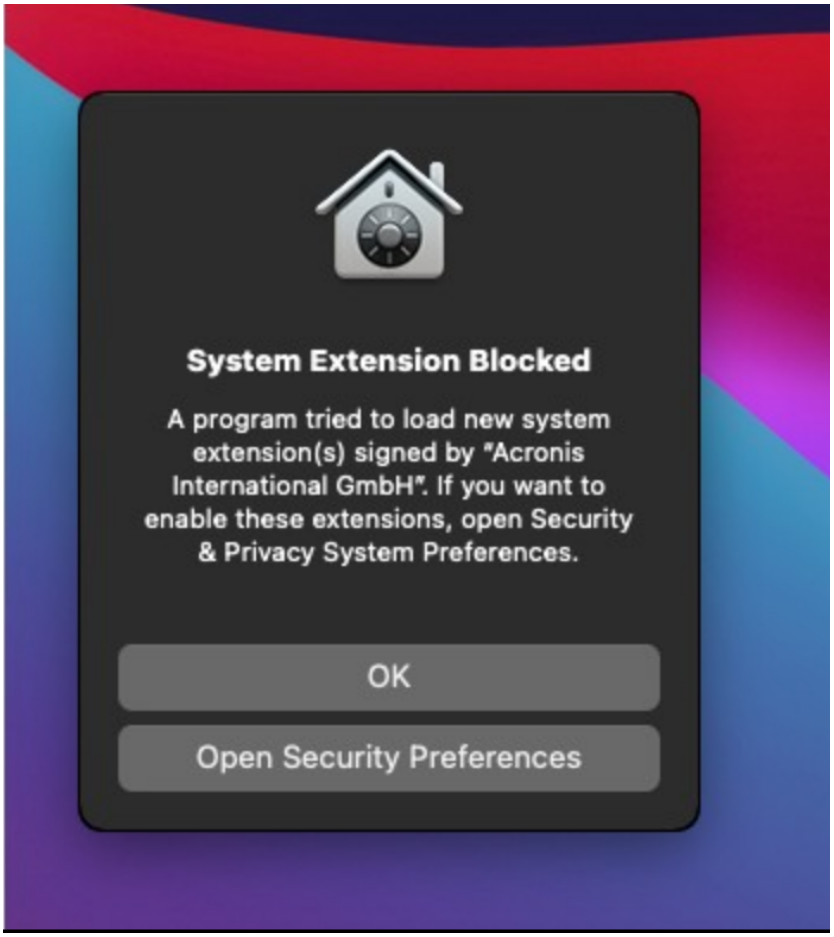
- macOS 10.15 (Catalina) et versions ultérieures
- macOS 11.2.3 (Big Sur) et versions ultérieures
- macOS 12.2 (Monterey) et versions ultérieures
- macOS 13.2 (Ventura) et versions ultérieures
- macOS 14 (Sonoma) et versions ultérieures
- macOS 15 (Sequoia) et versions ultérieures

Pour activer l'utilisation du module de contrôle de terminaux sur macOS

1. Installez l'agent pour Mac sur l'ordinateur que vous voulez protéger.
2. Dans le plan de protection, activez les paramètres de contrôle de terminaux.
3. Appliquez le plan de protection.

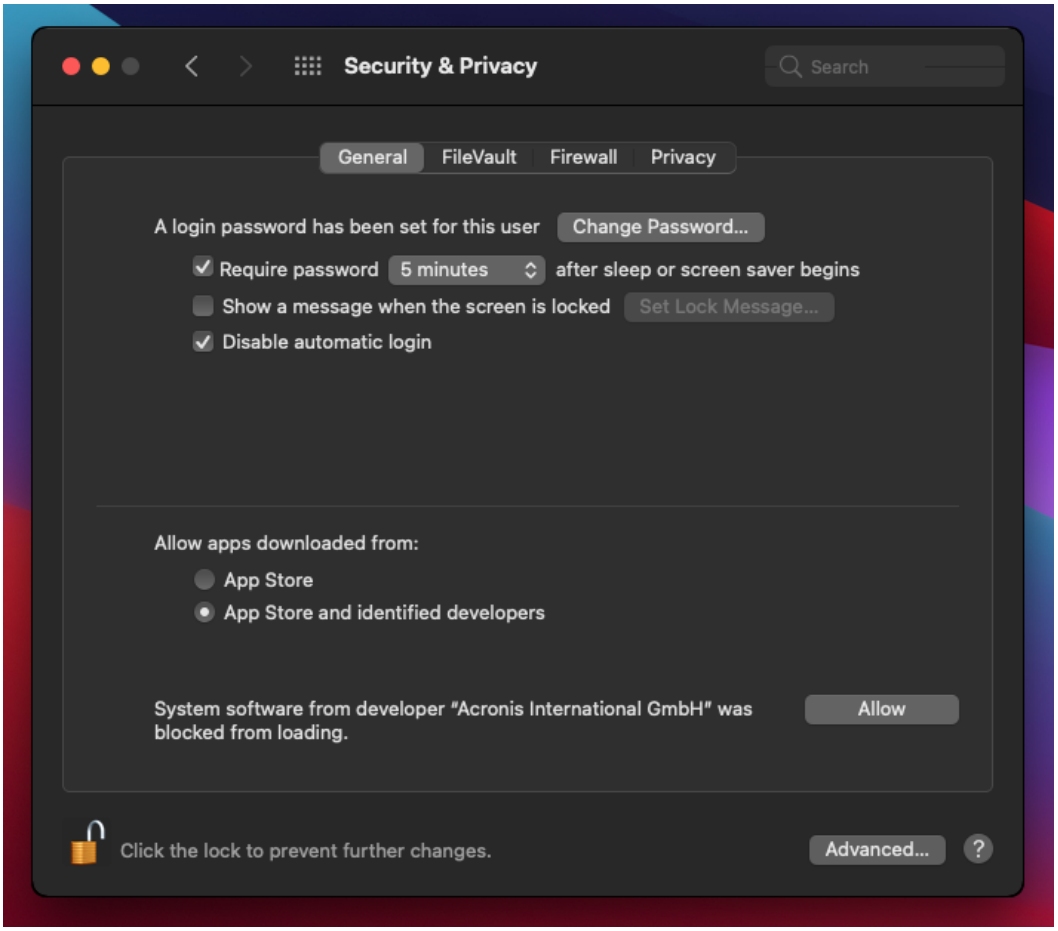
© Acronis International GmbH, 2003-2026

4. L'avertissement « Extension système bloquée » apparaît sur la ressource protégée. Cliquez sur **Ouvrir les préférences de sécurité**.



© Acronis International GmbH, 2003-2026

5. Dans le volet **Sécurité et confidentialité** qui s'affiche, sélectionnez **App Store et développeurs identifiés**, puis cliquez sur **Autoriser**.



6. Dans la boîte de dialogue qui apparaît, cliquez sur **Redémarrer** pour redémarrer la ressource et activer les paramètres de contrôle de terminaux.

Remarque
Si les paramètres sont désactivés par la suite, vous n'aurez pas à répéter ces étapes pour les réactiver.

Consulter ou modifier les paramètres d'accès

Dans le panneau du plan de protection, vous pouvez gérer les paramètres d'accès pour le module de contrôle des terminaux. Vous pouvez ainsi autoriser ou refuser l'accès à certains types de terminaux, ainsi qu'activer ou désactiver les notifications et les alertes.

Pour consulter ou modifier les paramètres d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Paramètres d'accès**.

© Acronis International GmbH, 2003-2026

3. Sur la page de gestion des paramètres d'accès qui apparaît, consultez ou modifiez les paramètres d'accès comme vous le souhaitez.

Remarque
Les paramètres d'accès configurés dans Contrôle des terminaux peuvent être remplacés lorsque Contrôle des terminaux et Data Loss Prevention sont utilisés conjointement pour protéger une ressource. Voir "Activation de Data Loss Prevention dans les plans de protection" (p. 1593).

Activer ou désactiver les notifications du système d'exploitation et les alertes de service

Lorsque vous gérez les paramètres d'accès, vous pouvez activer ou désactiver les notifications du système d'exploitation et les alertes de service, informant l'utilisateur des tentatives d'exécution d'actions non autorisées.

Pour activer ou désactiver les notifications du système d'exploitation

1. Suivez les étapes pour consulter ou modifier les paramètres d'accès.
2. Sur la page de gestion des paramètres d'accès, sélectionnez ou désélectionnez la case **Affichez des notifications du système d'exploitation aux utilisateurs finaux s'ils essaient d'utiliser un type de terminal ou de port bloqué**.

Pour activer ou désactiver les alertes de service

1. Suivez les étapes pour consulter ou modifier les paramètres d'accès.
2. Sur la page de gestion des paramètres d'accès, sélectionnez ou désélectionnez la case **Afficher une alerte** pour le ou les types de terminaux souhaités.

La case **Afficher une alerte** est disponible uniquement pour les types de terminaux avec accès restreint (Lecture seule ou Accès refusé), à l'exception des captures d'écran.

Exclure des sous-classes de terminaux du contrôle d'accès

Dans le panneau du plan de protection, vous pouvez choisir les sous-classes de terminaux à exclure du contrôle d'accès. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès du contrôle des terminaux.

Pour exclure des sous-classes de terminaux du contrôle d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des types de terminaux**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, consultez ou modifiez la sélection de sous-classes de terminaux à exclure du contrôle d'accès.

© Acronis International GmbH, 2003-2026

Exclure des terminaux USB particuliers du contrôle d'accès

Dans le panneau du plan de protection, vous pouvez spécifier des terminaux ou des modèles de terminaux USB à exclure du contrôle d'accès des terminaux. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès du contrôle des terminaux.

Pour exclure un terminal USB du contrôle d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des terminaux USB**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de sélection des terminaux USB qui apparaît, sélectionnez le ou les terminaux souhaités parmi ceux enregistrés dans la base de données des terminaux USB.
5. Cliquez sur le bouton **Ajouter à la liste d'autorisation**.

Pour arrêter d'exclure un terminal USB du contrôle d'accès

1. Ouvrez le panneau du plan de protection pour un plan de protection et activez le contrôle des terminaux dans ce plan (consultez les étapes pour activer ou désactiver le contrôle des terminaux).
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des terminaux USB**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, cliquez sur l'icône de suppression à la fin de l'élément de liste représentant le terminal souhaité.

Ajouter ou supprimer le terminal USB de la base de données

Pour exclure un terminal USB en particulier du contrôle d'accès, vous devez l'ajouter à la base de données des terminaux USB. Vous pouvez ensuite ajouter des terminaux à la liste d'autorisation en les sélectionnant depuis cette base de données.

Les procédures suivantes s'appliquent aux plans de protection pour lesquels la fonctionnalité de contrôle des terminaux est activée.

Pour ajouter des terminaux USB à la base de données

1. Ouvrir le plan de protection d'un terminal pour le modifier :

   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

© Acronis International GmbH, 2003-2026

Remarque
Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur le lien à côté de **Liste d'autorisation des terminaux USB**.
3. Sur la page de **liste d'autorisation des terminaux USB** qui apparaît, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de gestion de la base de données des terminaux USB qui apparaît, cliquez sur **Ajouter à la base de données**.
5. Dans la boîte de dialogue **Ajouter un terminal USB** qui apparaît, cliquez sur l'ordinateur auquel le terminal USB est connecté.
   Seuls les ordinateurs en ligne s'affichent dans la liste des ordinateurs.
   La liste des terminaux USB s'affiche uniquement pour les ordinateurs sur lesquels l'agent Prévention des pertes de données est installé.
   Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.
   Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.
6. Cochez les cases correspondant aux terminaux USB que vous voulez ajouter à la base de données, puis cliquez sur **Ajouter à la base de données**.
   Les terminaux USB sélectionnés sont ajoutés à la base de données.
7. Fermez ou enregistrez le plan de protection.

Pour ajouter des terminaux USB à la base de données depuis le panneau de détails de l'ordinateur

Remarque
Cette procédure s'applique uniquement aux terminaux qui sont en ligne et sur lesquels l'agent Prévention des pertes de données est installé. Vous ne pouvez pas consulter la liste des terminaux USB d'un ordinateur hors ligne ou sur lequel l'agent Prévention des pertes de données n'est pas installé.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez un ordinateur auquel le terminal USB souhaité a déjà été connecté et, dans le menu de droite, cliquez sur **Inventaire**.
   Le panneau de détails de l'ordinateur s'ouvre.
3. Dans le panneau de détails de l'ordinateur, cliquez sur l'onglet **Terminaux USB**.
   La liste des terminaux USB connus sur l'ordinateur sélectionné s'affiche.

© Acronis International GmbH, 2003-2026

Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.

Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.

4. Cochez les cases correspondant aux terminaux USB que vous voulez ajouter à la base de données, puis cliquez sur **Ajouter à la base de données**.

Pour ajouter des terminaux USB à la base de données depuis des alertes de service

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Trouvez une alerte de contrôle de terminal qui vous informe de l'accès refusé au terminal USB.
3. Dans la vue d'alerte simple, cliquez sur **Autoriser ce terminal USB**.
   Cela exclut le terminal USB du contrôle d'accès et l'ajoute à la base de données pour référence ultérieure.

Pour ajouter des terminaux USB en important une liste de terminaux dans la base de données

Vous pouvez importer un fichier JSON contenant une liste de terminaux USB à ajouter à la base de données. Consultez "Importer une liste de terminaux USB dans la base de données" (p. 470).

Pour supprimer des terminaux USB de la base de données

1. Ouvrir le plan de protection d'un terminal pour le modifier :
   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

   Remarque
   Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Liste d'autorisation des terminaux USB**.
3. Sur la page de gestion de la liste d'autorisation qui apparaît, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de sélection de terminaux USB depuis la base de données, cliquez sur les points de suspension (...) situés à la fin de l'élément de liste représentant le terminal, cliquez sur **Supprimer**, puis confirmez la suppression.
   Les terminaux USB sont supprimés de la base de données.
5. Fermez ou enregistrez le plan de protection.

Afficher les alertes de contrôle des terminaux

Le module de contrôle des terminaux peut être configuré pour émettre des alertes qui vous informent des tentatives refusées d'utilisation de certains types de terminaux par l'utilisateur (voir

© Acronis International GmbH, 2003-2026

Activer ou désactiver les notifications du système d'exploitation et les alertes de service). Procédez comme suit pour afficher ces alertes.

Pour afficher les alertes de contrôle des terminaux

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**.
2. Recherchez des alertes ayant le statut suivant : « L'accès au périphérique est bloqué ».

Consultez Alertes de contrôle des terminaux pour en savoir plus.

Paramètres d'accès

Sur la page des **paramètres d'accès**, vous pouvez autoriser ou refuser l'accès à certains types de terminaux, ainsi qu'activer ou désactiver les notifications du système d'exploitation et les alertes de contrôle des terminaux.

Remarque
Les paramètres d'accès configurés dans Contrôle des terminaux peuvent être remplacés lorsque Contrôle des terminaux et Data Loss Prevention sont utilisés conjointement pour protéger une ressource. Voir "Activation de Data Loss Prevention dans les plans de protection" (p. 1593).

Les paramètres d'accès vous permettent de limiter l'accès des utilisateurs aux ports et types de terminaux suivants :

- **Amovible** (contrôle d'accès par type de terminal) : terminaux possédant une interface permettant de se connecter à un ordinateur (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc.) et reconnus par le système d'exploitation comme étant des périphériques de stockage amovibles (par exemple, clés USB, lecteurs de carte, lecteurs magnéto-optiques, etc.). Le contrôle des terminaux classifie tous les disques durs connectés via USB, FireWire et PCMCIA en tant que terminaux amovibles. Il classifie également certains disques durs (généralement SATA et SCSI) en tant que terminaux amovibles s'ils prennent en charge la fonction de branchement à chaud et que le système d'exploitation en cours d'exécution n'est pas installé sur eux.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux terminaux amovibles, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout terminal amovible sur un ordinateur protégé. Les droits d'accès n'affectent pas les terminaux chiffrés avec BitLocker ou FileVault (uniquement avec le système de fichiers HFS+).

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Amovible chiffré** (contrôle d'accès par type de terminal) : terminaux amovibles chiffrés avec le chiffrement de lecteur BitLocker (sur Windows) ou FileVault (sur macOS).

  Sur macOS, seuls les lecteurs amovibles chiffrés lecteur utilisant le système de fichiers HFS+ (également nommé HFS Plus ou Mac OS Extended, ou encore HFS Extended) sont pris en charge. Les lecteurs amovibles chiffrés utilisant le système de fichiers APFS sont traités comme des lecteurs amovibles.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux terminaux amovibles chiffrés, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis

© Acronis International GmbH, 2003-2026

tout terminal amovible chiffré sur un ordinateur protégé. Les droits d'accès affectent uniquement les terminaux chiffrés avec BitLocker ou FileVault (uniquement avec le système de fichiers HFS+).

Ce type de terminaux est pris en charge à la fois sur Windows et macOS.

- **Imprimantes** (contrôle d'accès par type de terminal) : imprimantes physiques avec une interface de connexion à un ordinateur, quelle qu'elle soit (USB, LPT, Bluetooth, etc.), ainsi que toutes les imprimantes auxquelles un ordinateur sur le réseau peut accéder.

  Vous pouvez autoriser ou refuser l'accès aux imprimantes afin de contrôler l'impression de documents sur n'importe quelle imprimante sur un ordinateur protégé.

  Remarque
  Lorsque vous définissez le paramètre d'accès aux imprimantes sur **Refuser**, les applications et processus qui accèdent aux imprimantes doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **Presse-papiers** (contrôle d'accès par type de terminal) : presse-papiers Windows.

  Vous pouvez autoriser l'accès ou refuser l'accès au presse-papiers pour contrôler les opérations de copier-coller via le presse-papiers Windows sur un ordinateur protégé.

  Remarque
  Lorsque vous définissez le paramètre d'accès au presse-papiers sur **Refuser**, les applications et processus qui accèdent au presse-papiers doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **Capture d'écran** (contrôle d'accès par type de terminal) : permet la capture d'écran de l'écran complet, de la fenêtre active ou d'une partie sélectionnée de l'écran.

  Vous pouvez autoriser ou refuser l'accès aux captures d'écran afin de contrôler la capture d'écran sur un ordinateur protégé.

  Remarque
  Lorsque vous définissez le paramètre d'accès aux captures d'écran sur **Refuser**, les applications et processus qui accèdent à la capture d'écran doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **Terminaux mobiles** (contrôle d'accès par type de terminal) : terminaux (ex. : smartphones Android, etc.) qui communiquent avec un ordinateur via le protocole MTP (Media Transfer Protocol), avec n'importe quelle interface utilisée pour se connecter à un ordinateur (USB, IP, Bluetooth).

© Acronis International GmbH, 2003-2026

Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux terminaux mobiles, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout terminal mobile sur un ordinateur protégé.

Remarque
Lorsque vous définissez le paramètre d'accès aux terminaux mobiles sur **Lecture seule** ou **Refuser**, les applications et processus qui accèdent aux terminaux mobiles doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

Ce type de terminaux est pris en charge sur Windows uniquement.

- **Bluetooth** (contrôle d'accès par type de terminal) : terminaux Bluetooth internes ou externes disposant d'une interface de connexion à un ordinateur, quelle qu'elle soit (USB, PCMCIA, etc.). Ce paramètre contrôle l'utilisation des terminaux de ce type, plutôt que l'échange de données à l'aide de tels terminaux.

  Vous pouvez autoriser ou refuser l'accès au Bluetooth afin de contrôler le Bluetooth sur un ordinateur protégé.

  Remarque
  Sur macOS, les droits d'accès pour le Bluetooth n'affectent pas les terminaux Bluetooth HID. L'accès de ces terminaux est toujours autorisé pour éviter que les terminaux HID sans fil (souris et claviers) ne soient désactivés sur le matériel iMac et Mac Pro.

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Lecteurs optiques** (contrôle d'accès par type de terminal) : lecteurs CD/DVD/BD internes ou externes (y compris graveurs) disposant d'une interface de connexion à un ordinateur, quelle qu'elle soit (IDE, SATA, USB, FireWire, PCMCIA, etc.).

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux lecteurs optiques, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout lecteur optique sur un ordinateur protégé.

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Disquettes** (contrôle d'accès par type de terminal) : lecteurs de disquettes internes ou externes disposant d'une interface de connexion à un ordinateur, quelle qu'elle soit (IDE, USB, PCMCIA, etc.). Certains modèles de lecteurs de disquettes sont reconnus par le système d'exploitation comme des lecteurs amovibles. Dans ce cas, le module de contrôle des terminaux identifie également ces lecteurs comme étant des terminaux amovibles.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux lecteurs de disquettes, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout lecteur de disquettes sur un ordinateur protégé.

  Ce type de terminaux est pris en charge sur Windows uniquement.
- **USB** (contrôle d'accès par interface de terminal) : tout terminal connecté à un port USB, à l'exception des concentrateurs.

© Acronis International GmbH, 2003-2026

Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux ports USB, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout port USB sur un ordinateur protégé.

Ce type de terminaux est pris en charge à la fois sur Windows et macOS.

- **FireWire** (contrôle d'accès par interface de terminal) : tout terminal connecté à un port FireWire (IEEE 1394), à l'exception des concentrateurs.

  Vous pouvez autoriser l'accès complet ou l'accès en lecture seule aux ports FireWire, ou en refuser l'accès pour contrôler les opérations de copie de données vers et depuis tout port FireWire sur un ordinateur protégé.

  Ce type de terminaux est pris en charge à la fois sur Windows et macOS.
- **Terminaux redirigés** (contrôle d'accès par interface de terminal) : lecteurs mappés (disques durs, lecteurs amovibles et lecteurs optiques), terminaux USB et presse-papiers redirigés vers des sessions d'application virtuelle ou de bureau virtuel.

  Le module de contrôle des terminaux reconnaît les terminaux redirigés via les protocoles à distance Microsoft RDP, Citrix ICA, VMware PCoIP et HTML5/WebSockets dans les environnements de virtualisation Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer et VMware Horizon hébergés sur des ordinateurs Windows protégés. Il peut également contrôler les opérations de copies de données entre le presse-papiers Windows du système d'exploitation invité exécuté sur VMware Workstation, VMware Player, Oracle VM VirtualBox ou Windows Virtual PC, et le presse-papiers du système d'exploitation hôte exécuté sur l'ordinateur Windows protégé.

  Ce type de terminaux est pris en charge sur Windows uniquement.

  Vous pouvez configurer l'accès aux terminaux redirigés comme suit :

  - **Lecteurs mappés** : autorisez l'accès complet ou l'accès en lecture seule, ou refusez l'accès afin de contrôler les opérations de copie de données vers et depuis tout disque dur, lecteur amovible ou lecteur optique redirigé vers la session hébergée sur un ordinateur protégé.
  - **Presse-papiers entrant** : autorisez ou refusez l'accès pour contrôler les opérations de copie de données via le presse-papiers vers la session hébergée sur un ordinateur protégé.

    Remarque
    Lorsque vous définissez le paramètre d'accès au presse-papiers entrant sur **Refuser**, les applications et processus qui accèdent au presse-papiers doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

  - **Presse-papiers sortant** : autorisez ou refusez l'accès pour contrôler les opérations de copie de données via le presse-papiers depuis la session hébergée sur un ordinateur protégé.

    Remarque
    Lorsque vous définissez le paramètre d'accès au presse-papiers sortant sur **Refuser**, les applications et processus qui accèdent au presse-papiers doivent être redémarrés pour appliquer les paramètres d'accès nouvellement configurés. Pour vous assurer que les paramètres d'accès sont correctement appliqués, redémarrez les ressources protégées.

© Acronis International GmbH, 2003-2026

- **Ports USB** : autorisez ou refusez l'accès pour contrôler les opérations de copie des données vers et depuis les terminaux connectés à n'importe quel port USB redirigé vers la session hébergée sur un ordinateur protégé.

Les paramètres de contrôle des terminaux affectent tous les utilisateurs de la même manière. Par exemple, si vous refusez l'accès à des terminaux amovibles, vous empêchez tout utilisateur de copier des données depuis et à partir de ces terminaux sur un ordinateur protégé. Il est possible d'autoriser l'accès à des terminaux USB particuliers en les excluant du contrôle d'accès (voir Liste d'autorisation des types de terminaux et Liste d'autorisation des terminaux USB).

Lorsque l'accès à un terminal est contrôlé à la fois par son type et par son interface, le refus de l'accès au niveau interface a priorité. Par exemple, si l'accès aux ports USB est refusé (interface de terminal), l'accès aux terminaux mobiles connectés à un port USB est refusé, que l'accès aux terminaux mobiles soit autorisé ou non (type de terminal). Pour autoriser l'accès à un tel terminal, vous devez autoriser à la fois son interface et son type.

Remarque
Si le plan de protection utilisé sur macOS inclut des paramètres pour les types de terminaux qui sont uniquement pris en charge par Windows, alors ces paramètres sont ignorés pour macOS.

Important
Lorsqu'un terminal amovible, un terminal amovible chiffré, une imprimante ou un terminal Bluetooth est connecté à un port USB, l'autorisation de l'accès à ce terminal outrepasse le refus d'accès défini au niveau de l'interface USB. Si vous autorisez un tel type de terminal, l'accès à ce terminal est autorisé, que l'accès au port USB soit refusé ou non.

Notifications du système d'exploitation et alertes de service

Vous pouvez configurer le contrôle des terminaux afin qu'il affiche des notifications du système d'exploitation aux utilisateurs finaux s'ils essaient d'utiliser un type de terminal ou de port bloqué sur des ordinateurs protégés. Lorsque la case **Affichez des notifications du système d'exploitation aux utilisateurs finaux s'ils essaient d'utiliser un type de terminal ou de port bloqué** est cochée dans les paramètres d'accès, l'agent affiche un message contextuel dans la zone de notifications de l'ordinateur protégé si l'un des événements suivants se produit :

- Tentative refusée d'utilisation d'un terminal sur un port USB ou FireWire. Cette notification apparaît chaque fois qu'un utilisateur branche un terminal USB ou FireWire refusé au niveau de l'interface (par exemple, lors du refus d'un accès au port USB) ou au niveau du type (par exemple, lors du refus de l'utilisation de terminaux amovibles).La notification informe l'utilisateur qu'il n'est pas autorisé à accéder au terminal/lecteur spécifié.
- Une tentative refusée de copie d'un objet de données (comme un fichier) depuis un certain terminal. Cette notification apparaît lors du refus d'un accès en lecture aux terminaux suivants : lecteurs de disquettes, lecteurs optiques, terminaux amovibles, terminaux amovibles chiffrés, terminaux mobiles, lecteurs mappés redirigés, et données entrantes de presse-papiers redirigées. La notification informe l'utilisateur qu'il n'est pas autorisé à récupérer l'objet de

© Acronis International GmbH, 2003-2026

données spécifié depuis le terminal spécifié.

La notification de lecture refusée s'affiche également lors du refus d'un accès en lecture/écriture au Bluetooth, à un port FireWire, à un port USB ou à un port USB redirigé.

- Une tentative refusée de copie d'un objet de données (comme un fichier) vers un certain terminal. Cette notification apparaît lors du refus d'un accès en écriture aux terminaux suivants : lecteur de disquettes, lecteurs optiques, terminaux amovibles, terminaux amovibles chiffrés, terminaux mobiles, presse-papiers local, captures d'écran, imprimantes, lecteurs mappés redirigés, et données sortantes de presse-papiers redirigées. La notification informe l'utilisateur qu'il n'est pas autorisé à envoyer l'objet de données spécifié vers le terminal spécifié.

Les tentatives de l'utilisateur d'accéder à des types de terminaux bloqués sur des ordinateurs protégés peut entraîner des alertes qui sont consignées dans la console Cyber Protect. Il est possible d'activer des alertes pour chaque type de terminal (à l'exception des captures d'écran) ou de port séparément en cochant la case **Afficher une alerte** dans les paramètres d'accès. Par exemple, si l'accès aux terminaux amovibles est restreint à un accès en lecture seule et que la case **Afficher une alerte** est cochée pour ce type de terminal, une alerte est consignée chaque fois qu'un utilisateur essaie de copier des données vers un terminal amovible sur un ordinateur protégé. Consultez Alertes de contrôle des terminaux pour en savoir plus.

Voir aussi les étapes pour activer ou désactiver les notifications du système d'exploitation et les alertes de service.

Liste d'autorisation des types de terminaux

Sur la page **Liste d'autorisation des types de terminaux**, vous pouvez choisir les sous-classes de terminaux à exclure du contrôle d'accès des terminaux. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès dans le module de contrôle des terminaux.

Le module de contrôle des terminaux offre la possibilité d'autoriser l'accès à des terminaux de certaines sous-classes au sein d'un type de terminal refusé. Cette option vous permet de refuser tous les terminaux d'un certain type, à l'exception de certaines sous-classes de terminaux de ce type. Cela peut être utile lorsque, par exemple, vous devez refuser l'accès à tous les ports USB, tout en autorisant l'utilisation d'un clavier et d'une souris USB.

Lors de la configuration du module de contrôle des terminaux, vous pouvez spécifier les sous-classes de terminaux à exclure du contrôle d'accès des terminaux. Lorsqu'un terminal appartient à une sous-classe exclue, l'accès à ce terminal est autorisé, que ce type de terminal ou de port soit refusé ou non. De manière sélective, vous pouvez exclure les sous-classes de terminaux suivantes du contrôle d'accès des terminaux :

- **USB HID (souris, clavier, etc.)** : lorsque cette option est sélectionnée, permet l'accès aux terminaux d'interface (souris, clavier, etc.) connectés à un port USB, même si l'accès aux ports USB est refusé. Par défaut, cette option est sélectionnée pour que le refus d'accès au port USB ne désactive pas le clavier ni la souris.
  Pris en charge à la fois sur Windows et macOS.

© Acronis International GmbH, 2003-2026

- **Cartes réseau USB et FireWire** : lorsque cette option est sélectionnée, permet l'accès aux cartes réseau connectées à un port USB ou FireWire (IEEE 1394), même si l'accès aux ports USB et/ou FireWire est refusé.
  Pris en charge à la fois sur Windows et macOS.
- **Scanners et périphériques d'images fixes USB** : lorsque cette option est sélectionnée, permet l'accès aux scanners et aux périphériques d'images fixes connectés à un port USB, même si l'accès aux ports USB est refusé.
  Pris en charge uniquement sur Windows.
- **Périphériques audio USB** : lorsque cette option est sélectionnée, permet l'accès aux périphériques audio, comme les casques et les microphones, connectés à un port USB, même si l'accès aux ports USB est refusé.
  Pris en charge uniquement sur Windows.
- **Appareils photo USB** : lorsque cette option est sélectionnée, permet l'accès aux webcams connectées à un port USB, même si l'accès aux ports USB est refusé.
  Pris en charge uniquement sur Windows.
- **Bluetooth HID (souris, clavier, etc.)** : lorsque cette option est sélectionnée, permet l'accès aux terminaux d'interface (souris, clavier, etc.) connectés via Bluetooth, même si l'accès au Bluetooth est refusé.
  Pris en charge uniquement sur Windows.
- **Fonction copier-coller du presse-papiers dans l'application** : lorsque cette option est sélectionnée, permet le copier-coller de données via le presse-papiers au sein de la même application, même si l'accès au presse-papiers est refusé.
  Pris en charge uniquement sur Windows.

Remarque
Les paramètres pour les sous-classes de terminaux non pris en charge sont ignorés si ces paramètres sont configurés dans le plan de protection appliqué.

Lorsque vous devez placer des terminaux sur la liste d'autorisation, considérez ce qui suit :

- Avec la liste d'autorisation de types de terminaux, vous ne pouvez autoriser qu'une sous-classe entière de terminal. Vous ne pouvez pas autoriser un modèle de terminal spécifique, tout en refusant tous les autres de la même sous-classe. Par exemple, en excluant les caméras USB du contrôle d'accès des terminaux, vous autorisez toutes les caméras USB, quels que soient leur modèle et leur fabricant. Pour découvrir comment autoriser des terminaux/modèles spécifiques, consultez Liste d'autorisation des périphériques USB.
- Les types de terminaux peuvent uniquement être sélectionnés à partir d'une liste fermée de sous-classes de terminaux. Si le terminal à autoriser appartient à une autre sous-classe, il ne peut pas être autorisé à l'aide de la liste d'autorisation des types de terminaux. Par exemple, une sous-classe « Lecteur de cartes USB » ne peut pas être ajoutée à la liste d'autorisation. Pour autoriser un lecteur de cartes USB lorsque l'accès aux ports USB est refusé, suivez les instructions dans la Liste d'autorisation des périphériques USB.

© Acronis International GmbH, 2003-2026

- La liste d'autorisation des types de terminaux fonctionne uniquement pour les terminaux qui utilisent des pilotes Windows standard. Le module de contrôle des terminaux ne reconnaîtra peut-être pas la sous-classe de certains terminaux USB disposant de pilotes propriétaires. Vous ne pouvez donc pas autoriser l'accès à de tels terminaux USB à l'aide de la liste d'autorisation des types de terminaux. Dans ce cas, vous pourriez autoriser l'accès par terminal/modèle (consultez Liste d'autorisation des périphériques USB).

Liste d'autorisation des périphériques USB

La liste d'autorisation est conçue pour autoriser l'utilisation de certains terminaux USB, quels que soient les autres paramètres de contrôle des terminaux. Vous pouvez ajouter des terminaux ou des modèles de terminaux donnés à la liste d'autorisation afin de désactiver le contrôle d'accès pour ces terminaux. Par exemple, si vous ajoutez un terminal mobile avec un ID unique à la liste d'autorisation, vous autorisez l'utilisation de ce terminal particulier, même si n'importe quel autre terminal USB est refusé.

Sur la page **Liste d'autorisation des terminaux USB**, vous pouvez spécifier des terminaux ou des modèles de terminaux USB à exclure du contrôle d'accès des terminaux. Par conséquent, l'accès à ces terminaux est autorisé, quels que soient les paramètres d'accès dans le module de contrôle des terminaux.

Il existe deux façons d'identifier les terminaux dans la liste d'autorisation :

- Modèle de terminal : identifie collectivement tous les terminaux d'un certain modèle. Chaque modèle de terminal est identifié par identifiant de fournisseur (VID) et identifiant de produit (PID), par exemple USB\VID_0FCE&PID_E19E.

  Cette combinaison VID/PID n'identifie pas un terminal spécifique, mais un modèle de terminal complet. En ajoutant un modèle de terminal à la liste d'autorisation, vous autorisez l'accès à n'importe quel terminal de ce modèle. De cette manière, vous pouvez par exemple autoriser l'utilisation d'un modèle particulier d'imprimante USB.
- Terminal unique : identifie un certain terminal. Chaque modèle de terminal est identifié par identifiant de fournisseur (VID), identifiant de produit (PID) et numéro de série, par exemple USB\VID_0FCE&PID_E19E\D55E7FCA.

  Tous les terminaux USB ne possèdent pas de numéro de série. Vous pouvez ajouter un terminal à la liste d'autorisation en tant que terminal unique à condition qu'un numéro de série ait été attribué à ce terminal lors de la production. Par exemple, une clé USB qui dispose d'un numéro de série unique.

Pour ajouter un terminal à la liste d'autorisation, vous devez d'abord l'ajouter à la base de données des terminaux USB. Vous pouvez ensuite ajouter des terminaux à la liste d'autorisation en les sélectionnant depuis cette base de données.

La liste d'autorisation est gérée sur une page de configuration séparée appelée **Liste d'autorisation des terminaux USB**. Chaque élément de la liste représente un terminal ou un modèle de terminal et dispose des champs suivants :

© Acronis International GmbH, 2003-2026

- **Description** : le système d'exploitation attribue une certaine description lors de la connexion du terminal USB. Vous pouvez modifier la description du terminal dans la base de données des terminaux USB (voir la page de gestion de la base de données USB).
- **Type de terminal :** affiche « Unique » si l'élément de liste est un terminal unique, ou « Modèle » s'il s'agit d'un modèle de terminal.
- **Lecture seule :** lorsque cette option est sélectionnée, n'autorise que la réception de données depuis le terminal. Si le terminal ne prend pas en charge l'accès en lecture, l'accès au terminal est bloqué. Désélectionnez cette case pour autoriser l'accès complet au terminal.
- **Réinitialiser** : lorsque l'option est sélectionnée, force le terminal à simuler une déconnexion/connexion lorsqu'un nouvel utilisateur se connecte. Certains terminaux USB nécessitent une réinitialisation pour fonctionner. Par conséquent, nous vous recommandons de cocher cette case pour ces terminaux (souris, clavier, etc.). Nous vous recommandons également de désélectionner cette case pour les périphériques de stockage de données (clés USB, lecteurs optiques, disques durs externes, etc.).
  Le module de contrôle des terminaux ne sera peut-être pas en mesure de réinitialiser certains terminaux USB disposant de pilotes propriétaires. Si vous ne parvenez pas à accéder à un tel périphérique, vous devez retirer le périphérique USB du port USB, puis le réinsérer.

Remarque
Le champ **Réinitialiser** est masqué par défaut. Pour l'afficher dans le tableau, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis cochez la case **Réinitialiser**.

Remarque
Les champs **En lecture seule** et **Réinitialiser** ne sont pas pris en charge sur macOS. Si ces champs sont configurés dans le plan de protection appliqué, ils seront ignorés.

Vous pouvez ajouter ou supprimer des terminaux/modèles de la liste d'autorisation comme suit :

- Cliquez sur **Ajouter depuis la base de données** au-dessus de la liste, puis sélectionnez le ou les terminaux souhaités parmi ceux enregistrés dans la base de données des terminaux USB. Le terminal sélectionné est ajouté à la liste, où vous pouvez configurer ses paramètres et confirmer les modifications.
- Cliquez sur **Autoriser ce terminal USB** dans une alerte informant que l'accès au terminal USB est refusé (consultez Alertes de contrôle des terminaux). Le terminal est alors ajouté à la liste d'autorisation et à la base de données des terminaux USB.
- Cliquez sur l'icône de suppression à la fin d'un élément de liste. Le terminal/modèle en question est supprimé de la liste d'autorisation.

Base de données des périphériques USB

Le module de contrôle des terminaux tient à jour une base de données des terminaux USB depuis laquelle vous pouvez ajouter des terminaux à la liste d'exclusions (voir Liste d'autorisation des terminaux USB). Un terminal USB peut être enregistré dans la base de données de l'une des manières suivantes :

© Acronis International GmbH, 2003-2026

- Ajoutez un terminal à la page qui apparaît lors de l'ajout d'un terminal à la liste d'exclusion (voir Page de gestion de la base de données des terminaux USB).
- Ajoutez un terminal depuis l'onglet Terminaux USB du volet Inventaire d'un ordinateur dans la console Cyber Protect (voir Liste des terminaux USB sur un ordinateur).
- Autorisez un terminal à partir d'une alerte refusant l'accès à ce dernier (voir Alertes de contrôle des terminaux).

Voir aussi les étapes pour ajouter ou supprimer des terminaux USB de la base de données.

Page de gestion de la base de données des terminaux USB

Lors de la configuration de la liste d'autorisation pour les terminaux USB, vous avez la possibilité d'ajouter un terminal depuis la base de données. Si vous choisissez cette option, une page de gestion apparaît avec une liste de terminaux. Sur cette page, vous pouvez voir la liste de tous les terminaux enregistrés dans la base de données. Vous pouvez sélectionner les terminaux à ajouter à la liste d'autorisation et effectuer les opérations suivantes :

Enregistrer un terminal dans la base de données

1. Cliquez sur **Ajouter à la base de données** en haut de la page.
2. Dans la boîte de dialogue **Ajouter un terminal USB** qui apparaît, cliquez sur l'ordinateur auquel le terminal USB est connecté.
   Seuls les ordinateurs en ligne s'affichent dans la liste des ordinateurs.
   La liste des terminaux USB s'affiche uniquement pour les ordinateurs sur lesquels l'agent Prévention des pertes de données est installé.
   Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.
   Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.
3. Cochez la case correspondant au terminal USB que vous voulez enregistrer, puis cliquez sur **Ajouter à la base de données**.

Modifier la description d'un terminal

1. Sur la page **Base de données des terminaux USB**, cliquez sur les points de suspension (...) situés à la fin de l'élément de liste représentant le terminal, puis cliquez sur **Modifier**.
2. Modifiez la description dans la boîte de dialogue qui apparaît.

Supprimer un terminal de la base de données

1. Cliquez sur les points de suspension (...) situés à la fin de l'élément de liste représentant le terminal.
2. Cliquez sur **Supprimer**, puis confirmez la suppression.

Pour chaque terminal, la liste sur la page fournit les informations suivantes :

© Acronis International GmbH, 2003-2026

- **Description** : un identifiant lisible du terminal. Vous pouvez modifier la description comme vous le souhaitez.
- **Type de terminal :** affiche « Unique » si l'élément de liste est un terminal unique, ou « Modèle » s'il s'agit d'un modèle de terminal. Un terminal unique doit disposer d'un numéro de série, ainsi que d'un identifiant de fournisseur (VID) et d'un identifiant de produit, alors qu'un modèle de terminal est identifié par une combinaison de VID et PID.
- **Identifiant du fournisseur**, **ID de produit**, **Numéro de série** : ensemble, ces valeurs constituent l'identifiant du périphérique, sous la forme USB\VID_<vendor ID>&PID_<product ID>\<serial number>.
- **Compte** : indique le tenant à qui appartient ce terminal. Il s'agit du tenant qui contient le compte utilisateur qui a été utilisé pour enregistrer le terminal dans la base de données.

Remarque
Cette colonne est masquée par défaut. Pour l'afficher dans le tableau, cliquez sur l'icône en forme d'engrenage en haut à droite du tableau, puis sélectionnez **Compte**.

La colonne la plus à gauche permet de sélectionner les terminaux à ajouter à la liste d'autorisation : Cochez la case correspondant à chaque terminal à ajouter, puis cliquez sur le bouton **Ajouter à la liste d'autorisation**. Pour sélectionner ou désélectionner toutes les cases, cliquez sur la case à cocher située dans l'en-tête de colonne.

Vous pouvez effectuer une recherche dans la liste des terminaux ou y appliquer des filtres :

- Cliquez sur **Rechercher** en haut de la page, puis entrez une chaîne à rechercher. La liste affiche les terminaux dont la description correspond à la chaîne que vous avez saisie.
- Cliquez sur **Filtrer**, puis configurez et appliquez un filtre dans la boîte de dialogue qui apparaît. La liste est limitée aux terminaux correspondant au type, à l'identifiant de fournisseur, à l'identifiant de produit et au compte que vous avez sélectionnés lors de la configuration du filtre. Pour annuler le filtre et afficher tous les terminaux, cliquez sur **Réinitialiser au défaut**.

Exporter la liste des terminaux USB présents dans la base de données

Vous pouvez exporter la liste des terminaux USB ajoutés à la base de données.

1. Ouvrez le plan de protection d'un terminal pour le modifier.
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Liste d'autorisation des périphériques USB**.
3. Sur la page de liste d'autorisation des terminaux USB, cliquez sur **Ajouter depuis la base de données**.
4. Sur la page de gestion de la base de données des terminaux USB qui apparaît, cliquez sur **Exporter**.
   La boîte de dialogue Parcourir par défaut s'ouvre.
5. Sélectionnez l'emplacement dans lequel vous souhaitez sauvegarder le fichier, entrez un nouveau nom si besoin, puis cliquez sur **Enregistrer**.

© Acronis International GmbH, 2003-2026

La liste des terminaux USB est exportée sous la forme d'un fichier JSON.

Vous pouvez modifier le fichier JSON obtenu afin d'y ajouter ou d'y retirer des terminaux, ou modifier en masse les descriptions des terminaux.

Importer une liste de terminaux USB dans la base de données

Au lieu d'ajouter des terminaux USB depuis l'interface utilisateur de la console Cyber Protect, vous pouvez importer une liste de terminaux USB. La liste est un fichier au format JSON.

Remarque
Vous pouvez importer des fichiers JSON à une base de données qui ne contient pas les terminaux décrits dans le fichier. Pour importer un fichier modifié vers la base de données depuis laquelle il a été exporté, vous devez d'abord effacer la base de données, car vous ne pouvez pas importer d'entrées dupliquées. Si vous exportez la liste des terminaux USB, la modifiez et essayez de l'importer dans la même base de données sans effacer cette dernière, l'importation échouera.

1. Ouvrez le plan de protection d'un terminal pour le modifier.
2. Cliquez sur l'icône de flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Liste d'autorisation des périphériques USB**.
3. Sur la page de liste d'autorisation des terminaux USB, cliquez sur **Ajouter depuis la base de données**.
4. Utilisez le glisser-déplacer (ou la navigation) pour le fichier que vous souhaitez importer.

La console Cyber Protect vérifie si la liste contient des entrées dupliquées qui existent déjà dans la base de données et les ignore. Les terminaux USB qui ne figurent pas dans la base de données sont ajoutés à la fin de celle-ci.

Liste des terminaux USB sur un ordinateur

Le volet Inventaire d'un ordinateur dans la console Cyber Protect inclut l'onglet **Terminaux USB**. Si l'ordinateur est en ligne et que l'agent Prévention des pertes de données est installé dessus, l'onglet **Terminaux USB** affiche une liste de tous les terminaux USB qui ont déjà été connectés à cet ordinateur.

Les terminaux USB sont répertoriés sous la forme d'une arborescence. Le premier niveau de l'arborescence représente un modèle de terminal. Le deuxième niveau représente un terminal spécifique de ce modèle.

Pour chaque terminal, la liste fournit les informations suivantes :

- **Description** : le système d'exploitation attribue une description lors de la connexion du terminal USB. Cette description peut servir d'identifiant visible pour le terminal.
  Une icône bleue à côté de la description du terminal indique que le terminal est actuellement connecté à l'ordinateur. Si le terminal n'est pas connecté à l'ordinateur, l'icône est grisée.

© Acronis International GmbH, 2003-2026

- **Identifiant du périphérique** : l'identifiant que le système d'exploitation a attribué au terminal. L'identifiant possède le format suivant : USB\VID_<vendor ID>&PID_<product ID>\<serial number>, où <serial number> est facultatif. Exemples : USB\VID_0FCE&PID_ADDE\D55E7FCA (terminal avec numéro de série) ; USB\VID_0FCE&PID_ADDE (terminal sans numéro de série).

Pour ajouter des terminaux à la base de données des terminaux USB, cochez la case des terminaux souhaités, puis cliquez sur le bouton **Ajouter à la base de données**.

Exclusion de processus du contrôle d'accès

L'accès au presse-papiers Windows, aux captures d'écran, aux imprimantes et aux terminaux mobiles est contrôlé par le biais de hooks injectés dans des processus. Si des processus ne disposent pas d'un hook, l'accès à ces terminaux n'est pas contrôlé.

Remarque
L'exclusion de processus du contrôle d'accès n'est pas prise en charge sur macOS. Si une liste de processus exclus est configurée dans le plan de protection appliqué, elle sera ignorée.

Sur la page **Exclusions**, vous pouvez spécifier une liste de processus qui ne disposeront pas d'un hook. Cela signifie que les contrôles d'accès au presse-papiers (local et redirigé), aux captures d'écran, à une imprimante et aux terminaux mobiles ne seront pas appliqués à ces processus.

Par exemple, vous avez appliqué un plan de protection qui refuse l'accès aux imprimantes, puis vous lancez l'application Microsoft Word. Une tentative d'impression depuis cette application sera bloquée. Toutefois, si vous ajoutez le processus Microsoft Word à la liste d'exclusions, l'application ne disposera pas d'un hook. En conséquence, l'impression depuis Microsoft Word ne sera pas bloquée, contrairement à l'impression depuis d'autres applications.

Pour ajouter des processus aux exclusions

1. Ouvrir le plan de protection d'un terminal pour le modifier :
   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

   Remarque
   Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Exclusions**.
3. Sur la page **Exclusions**, à la ligne **Processus et dossiers**, cliquez sur **+Ajouter**.
4. Ajoutez les processus que vous souhaitez exclure du contrôle d'accès.
   Par exemple, `C:\Folder\subfolder\process.exe`.
   Vous pouvez utiliser les caractères génériques suivants :

© Acronis International GmbH, 2003-2026

- * remplace n'importe quel nombre de caractères.
- ? remplace un caractère.

Par exemple :

```
C:\Folder\*
*\Folder\SubFolder?\*
*\process.exe
```

5. Cliquez sur la coche, puis sur **Terminé**.
6. Dans le plan de protection, cliquez sur **Enregistrer**.
7. Redémarrez les processus que vous avez exclus pour vous assurer que les hooks ont bien été supprimés.

Les processus exclus auront accès au presse-papiers, aux captures d'écran, aux imprimantes et aux terminaux mobiles, quels que soient les paramètres d'accès pour ces terminaux.

Pour supprimer un processus de la liste d'exclusions

Ouvrir le plan de protection d'un terminal pour le modifier :

Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

Remarque
Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

1. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Exclusions**.
2. Sur la page **Exclusions**, cliquez sur l'icône de corbeille à côté du processus que vous souhaitez supprimer de la liste d'exclusions.
3. Cliquez sur **Terminé**.
4. Dans le plan de protection, cliquez sur **Enregistrer**.
5. Redémarrez le processus pour vous assurer que les hooks ont été correctement injectés.

Les paramètres d'accès issus du plan de protection seront appliqués aux processus que vous avez supprimés de la liste d'exclusions.

Pour modifier un processus dans la liste d'exclusions

1. Ouvrir le plan de protection d'un terminal pour le modifier :
   Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.

© Acronis International GmbH, 2003-2026

Remarque
Le contrôle des terminaux doit être activé dans le plan, afin que vous puissiez accéder aux paramètres de contrôle des terminaux.

2. Cliquez sur la flèche située à côté de l'interrupteur **Contrôle des terminaux** pour développer les paramètres, puis cliquez sur la ligne **Exclusions**.
3. Sur la page **Exclusions**, cliquez sur l'icône **Modifier** à côté du processus que vous souhaitez modifier.
4. Appliquez les modifications souhaitées, puis cliquez sur la coche pour les confirmer.
5. Cliquez sur **Terminé**.
6. Dans le plan de protection, cliquez sur **Enregistrer**.
7. Redémarrez les processus affectés afin de vous assurer que vos modifications ont été correctement appliquées.

Alertes de contrôle des terminaux

Le module de contrôle des terminaux tient un journal d'événements qui suit les utilisateurs qui tentent d'accéder à des types de terminaux, des ports ou des interfaces contrôlés. Certains événements peuvent entraîner des alertes qui sont consignées dans la console Cyber Protect. Par exemple, le module de contrôle des terminaux peut être configuré pour empêcher l'utilisation de terminaux amovibles, avec une alerte consignée chaque fois qu'un utilisateur tente de copier des données depuis ou vers un tel terminal.

Lors de la configuration du module de contrôles des terminaux, vous pouvez activer des alertes pour la plupart des éléments répertoriés sous le Type (à l'exception des captures d'écran) ou les Ports des terminaux. Si les alertes sont activées, une alerte est générée chaque fois qu'un utilisateur tente d'effectuer une opération qui n'est pas autorisée. Par exemple, si l'accès aux terminaux amovibles est restreint à un accès en lecture seule et que l'option **Afficher une alerte** est sélectionnée pour ce type de terminal, une alerte est générée chaque fois qu'un utilisateur essaie de copier des données vers un terminal amovible sur un ordinateur protégé.

Pour afficher les alertes dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**. Au sein de chaque alerte du module de contrôle des terminaux, la console fournit les informations suivantes sur l'événement respectif :

- **Type** : avertissement.
- **État** : affiche « L'accès au périphérique est bloqué ».
- **Message** : affiche « L'accès à '<type de terminal ou port>' sur '<nom de l'ordinateur>' est bloqué ». Par exemple, « L'accès à 'Amovible' sur 'pc-comptable' est bloqué ».
- **Date et heure** : date et heure auxquelles l'événement s'est produit.
- **Terminal** : nom de l'ordinateur sur lequel l'événement s'est produit.
- **Nom du plan** : nom du plan de protection à l'origine de l'événement.

© Acronis International GmbH, 2003-2026

- **Source** : terminal ou port impliqué dans l'événement. Par exemple, si la tentative d'accès d'un utilisateur à un terminal amovible a été refusée, ce champ indique Terminal amovible.
- **Action** : opération à l'origine de l'événement. Par exemple, si la tentative de copie de données sur un terminal d'un utilisateur a été refusée, ce champ indique Lecture. Pour plus d'informations, voir Valeurs du champ Action.
- **Nom** : nom de l'objet cible de l'événement, par exemple, fichier que l'utilisateur a essayé de copier ou terminal que l'utilisateur a essayé d'utiliser. Ne s'affiche pas si l'objet cible n'a pas pu être identifié.
- **Informations** : informations supplémentaires à propos du terminal cible de l'événement, comme l'identifiant de périphérique pour les périphériques USB. Ne s'affiche pas si aucune information supplémentaire sur le terminal cible n'est disponible.
- **Utilisateur** : nom de l'utilisateur à l'origine de l'événement.
- **Processus** : chemin d'accès complet au fichier exécutable de l'application à l'origine de l'événement. Dans certains cas, le nom du processus peut s'afficher à la place du chemin d'accès. Ne s'affiche pas si aucune information de processus n'est disponible.

Si une alerte s'applique à un terminal USB (y compris les terminaux amovibles et les terminaux amovibles chiffrés), l'administrateur peut, directement depuis l'alerte, ajouter le terminal à la liste d'autorisation, ce qui empêche le module de contrôle des terminaux de restreindre l'accès à ce terminal en particulier. Cliquer sur **Autoriser ce périphérique USB** l'ajoute à la liste d'autorisation des terminaux USB dans la configuration du module de contrôle des terminaux et l'ajoute également à la base de données des terminaux USB pour référence ultérieure.

Voir aussi les étapes pour afficher les alertes de contrôle des terminaux.

Valeurs du champ Action

Le champ **Action** d'alerte peut contenir les valeurs suivantes :

- **Lecture** : obtenir des données du terminal ou du port.
- **Écriture** : envoyer des données au terminal ou au port.
- **Formater** : accès direct (formatage, vérification du disque, etc.) au terminal. Dans le cas d'un port, l'opération s'applique au terminal connecté à ce port.
- **Éjecter** : supprimer le terminal du système ou éjecter le support du terminal. Dans le cas d'un port, l'opération s'applique au terminal connecté à ce port.
- **Imprimer** : envoyer un document à l'imprimante.
- **Copier le son** : copier-coller des données audio via le presse-papiers local.
- **Copier le fichier** : copier-coller un fichier via le presse-papiers local.
- **Copier l'image** : copier-coller une image via le presse-papiers local.
- **Copier le texte** : copier-coller du texte via le presse-papiers local.
- **Copier le contenu non identifié** : copier-coller d'autres données via le presse-papiers local.

© Acronis International GmbH, 2003-2026

- **Copier les données RTF (image)** : copier-coller une image via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (fichier)** : copier-coller un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (texte, image)** : copier-coller du texte accompagné d'une image via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (texte, fichier)** : copier-coller du texte accompagné d'un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (image, fichier)** : copier-coller une image accompagnée d'un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Copier les données RTF (texte, image, fichier)** : copier-coller du texte accompagné d'une image et d'un fichier via le presse-papiers local, au format texte enrichi (RTF).
- **Supprimer** : supprimer des données d'un terminal (par exemple, un terminal amovible, un terminal mobile, etc.).
- **Accès du terminal** : accéder à certains terminaux ou ports (par exemple, un terminal Bluetooth, un port USB, etc.).
- **Son entrant** : copier-coller des données audio, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Fichier entrant** : copier-coller un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Image entrante** : copier-coller une image, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Texte entrant** : copier-coller du texte, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Contenu non identifié entrant** : copier-coller d'autres données, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé.
- **Données RTF entrantes (image)** : copier-coller une image, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF entrantes (fichier)** : copier-coller un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF)
- **Données RTF entrantes (texte, image)** : copier-coller du texte accompagné d'une image, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF entrantes (texte, fichier)** : copier-coller du texte accompagné d'un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF entrantes (image, fichier)** : copier-coller une image accompagnée d'un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).

© Acronis International GmbH, 2003-2026

- **Données RTF entrantes (texte, image, fichier)** : copier-coller du texte, accompagné d'une image et d'un fichier, de l'ordinateur client vers la session hébergée, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Insérer** : Connecter un terminal USB ou un terminal FireWire.
- **Son sortant** : copier-coller des données audio, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Fichier sortant** : copier-coller un fichier, de la session hébergée vers l''ordinateur client, via le presse-papiers redirigé.
- **Image sortante** : copier-coller une image, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Texte sortant** : copier-coller du texte, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Contenu non identifié sortant** : copier-coller d'autres données, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé.
- **Données RTF sortantes (image)** : copier-coller une image, de la session hébergée vers l'ordinateur entier client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (fichier)** : copier-coller un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (texte, image)** : copier-coller du texte accompagné d'une image, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (texte, fichier)** : copier-coller du texte accompagné d'un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (image, fichier)** : copier-coller une image accompagnée d'un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Données RTF sortantes (texte, image, fichier)** : copier-coller du texte, accompagné d'une image et d'un fichier, de la session hébergée vers l'ordinateur client, via le presse-papiers redirigé, au format texte enrichi (RTF).
- **Renommer** : renommer les fichiers sur un terminal (par exemple, sur des périphériques amovibles, terminaux mobiles ou autres).

Effacement des données d'une ressource gérée

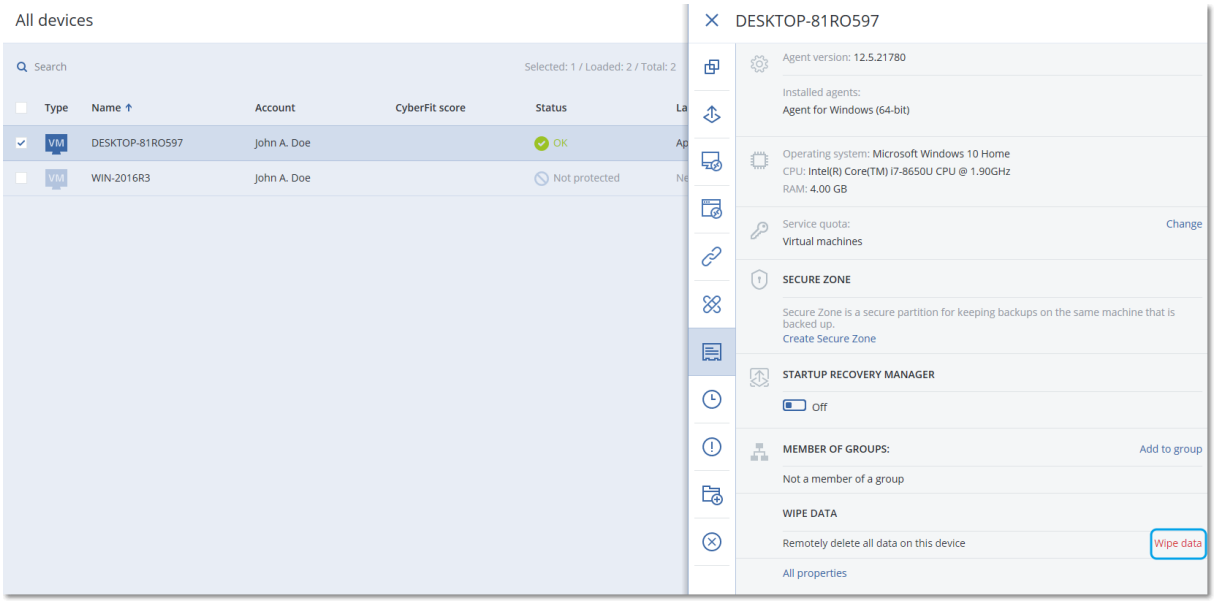
Remarque
L'effacement à distance est disponible dans le pack Advanced Security.

L'effacement à distance permet à un administrateur Cyber Protection et au propriétaire d'une machine de supprimer les données sur une machine gérée – par exemple, si elle est perdue ou volée. Ainsi, tout accès non autorisé à des informations sensibles sera empêché.

© Acronis International GmbH, 2003-2026

L'effacement à distance n'est disponible que pour les ordinateurs exécutant les versions de Windows 10 et ultérieures. Par défaut, la fonction `doWipeProtected` est utilisée. Si elle n'est pas disponible, la fonction `doWipe` est utilisée. Pour plus d'informations sur ces fonctions, consultez la documentation Microsoft.

Afin de recevoir la commande d'effacement, la machine doit être allumée et connectée à Internet.



Pour effacer les données d'une machine

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez la machine dont vous souhaitez effacer les données.

   Remarque
   Vous ne pouvez effacer les données que d'une machine à la fois.

3. Cliquez sur **Détails**, puis sur **Effacer les données**.
   Si la machine que vous avez sélectionnée est hors ligne l'option **Effacer les données** est inaccessible.
4. Confirmez votre choix.
5. Saisissez les identifiants de l'administrateur local de la machine, puis cliquez sur **Effacer les données**.

   Remarque
   Vous pouvez consulter les détails du processus d'effacement et la personne l'ayant initié dans **Surveillance** > **Activités**.

© Acronis International GmbH, 2003-2026

Affichage des ressources gérées par les intégrations RMM

Remarque
Cette fonctionnalité n'est disponible que si le service PSA est activé.

Lorsque vous intégrez une plate-forme RMM dans le cadre du service PSA, vous pouvez afficher et surveiller les informations provenant des terminaux gérés par la plate-forme RMM. Ces informations sont disponibles dans la console Cyber Protect, en accédant à **Terminaux**.

Pour afficher les ressources gérées par les intégrations RMM

1. Accédez à **Terminaux** > **Tous les terminaux**.
2. Triez la colonne **Intégration RMM** pour localiser l'intégration souhaitée.
3. Sélectionnez la ressource pertinente.
4. Dans le panneau **Actions**, sélectionnez **Détails**.
5. Le panneau affiche l'une des trois options en fonction de la ressource configurée :
   - Si les services Acronis sont définis pour la ressource sans intégration RMM : Si la ressource est configurée pour ne fonctionner qu'avec les services Acronis, aucune information sur l'intégration RMM ne s'affiche.
   - Si les services Acronis et une intégration RMM sont configurés pour la ressource : Les services Acronis et les détails concernant l'intégration RMM figurent dans deux onglets : **Vue d'ensemble** et **Intégration RMM**. Cliquez sur **Intégration RMM** pour afficher les détails de l'intégration, y compris le nom, le type (fourni par la plate-forme RMM), la description et l'emplacement de la ressource. Par ailleurs, tous les modules complémentaires d'agent RMM installés et activés sont également affichés.
   - Si la ressource est configurée avec une intégration RMM uniquement : Les détails de l'intégration RMM sont affichés, y compris le nom, le type (fourni par la plate-forme RMM), la description et l'emplacement de la ressource. Par ailleurs, tous les modules complémentaires d'agent RMM installés et activés sont également affichés.

Remarque
Notez que, lorsque la ressource est configurée avec l'intégration RMM (soit avec les services Acronis, soit uniquement avec une intégration RMM), vous pouvez effectuer les opérations suivantes :

- Établissement d'une connexion à distance (disponible pour les intégrations Datto RMM, N-able N-central et N-able RMM).
- Examen des modules complémentaires installés sur le terminal RMM tiers (disponible uniquement pour N-able RMM).
- Accès direct aux informations détaillées sur le terminal RMM tiers (disponible pour Datto RMM, N-able N-central, NinjaOne).

© Acronis International GmbH, 2003-2026

Ressources CyberApp

Les ressources CyberApp sont créées par des éditeurs de logiciels indépendants et apparaissent dans la console Cyber Protect une fois que vous avez activé une intégration CyberApp. Les conditions suivantes doivent être satisfaites :

- Le point d'extension **Ressources et actions** doit être activé dans l'application CyberApp.
- Un **type de ressource** au moins doit être défini dans l'application CyberApp.
- Le service de connecteur hébergé par l'éditeur de logiciels indépendant doit s'assurer que les ressources CyberApp sont ajoutées et mises à jour dans la plate-forme Acronis.

Pour plus d'informations sur le portail dédié aux fournisseurs et sur la création d'applications CyberApp, consultez le Guide de l'utilisateur du portail dédié aux fournisseurs.

Ressources agrégées

Une ressource physique peut avoir un agent Cyber Protect, et un ou plusieurs agents CyberApp installés simultanément. Dans ce cas, la même ressource aura plusieurs représentations dans l'écran **Tous les terminaux**. Un enregistrement distinct s'affiche pour la ressource Acronis et pour chaque ressource CyberApp. Si la fusion automatique des ressources est activée et configurée dans le portail dédié aux fournisseurs ou dans la console Cyber Protect, le système compare les adresses d'hôte et les adresses MAC des ressources Acronis et CyberApp, et fusionne toutes les représentations en une même ressource agrégée. Vous pouvez fusionner et annuler la fusion des ressources manuellement, dans la console Cyber Protect.

Utilisation de ressources CyberApp

Outre les actions standard intégrées dans la console Cyber Protect, vous pouvez effectuer les opérations qui deviennent disponibles une fois que les ressources CyberApp apparaissent dans la console telles que la fusion manuelle de ressources dans une ressource agrégée. Par ailleurs, vous pouvez également réaliser les opérations personnalisées configurées dans l'application CyberApp.

Fusionner

Prérequis

- Les ressources de différentes sources sont disponibles pour le tenant.

Vous pouvez fusionner manuellement une ressource Acronis avec une ou plusieurs ressources CyberApp dans une seule ressource agrégée.

Pour fusionner manuellement des ressources dans une ressource agrégée

© Acronis International GmbH, 2003-2026

1. Dans l'écran **Tous les terminaux**, cliquez sur les ressources que vous souhaitez fusionner.

   Remarque
   L'action de fusion s'affiche si vous sélectionnez des ressources de sources distinctes, par exemple une ressource Acronis et une ressource CyberApp.

2. Cliquez sur **Fusionner des ressources**.

Exécuter des actions personnalisées

Prérequis

- Une intégration CyberApp pour laquelle l'option **Actions sur les ressources** définie est activée pour le tenant.

Les actions personnalisées sont des actions configurées dans l'application CyberApp qui deviennent disponibles pour la ressource CyberApp correspondante lorsque vous activez l'intégration CyberApp pour le tenant.

Pour exécuter des actions personnalisées

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource.
2. Cliquez sur **Actions d'application intégrées**.
3. Cliquez sur l'action.

Utilisation de ressources agrégées

Outre les actions standard intégrées dans la console Cyber Protect, vous pouvez effectuer les opérations suivantes avec des ressources agrégées : affichage des détails et annulation de la fusion de ressources sources. Par ailleurs, vous pouvez également réaliser les opérations personnalisées configurées dans les applications CyberApp.

Afficher les détails

Prérequis

- Une ressource agrégée au moins est disponible pour le tenant.

Pour afficher les détails d'une ressource agrégée

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource agrégée.
2. Cliquez sur **Détails**.
   Les informations concernant la ressource agrégée sont disponibles dans différents onglets. Chaque onglet affiche les informations détaillées de chaque représentation de ressource.

Annuler la fusion

© Acronis International GmbH, 2003-2026

Prérequis

- Une ressource agrégée au moins est disponible pour le tenant.

Lorsque vous annulez la fusion d'une ressource agrégée, elle ne s'affiche plus dans la liste des terminaux. Vous voyez en revanche une entrée distincte pour chaque ressource source qui a été fusionnée dans la ressource agrégée.

Pour annuler la fusion d'une ressource agrégée

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource agrégée dont vous souhaitez annuler la fusion.
2. Cliquez sur **Annuler la fusion de ressources sources**.
3. Dans la fenêtre de confirmation, cliquez sur **Annuler la fusion**.

Exécuter des actions personnalisées

Prérequis

- Au moins une intégration CyberApp pour laquelle l'option **Actions sur les ressources** définie est activée pour le tenant.

Les actions personnalisées sont des actions configurées dans les applications CyberApp qui deviennent disponibles pour la ressource CyberApp correspondante lorsque vous activez l'intégration CyberApp pour le tenant.

Pour exécuter des actions personnalisées

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource.
2. Cliquez sur **Actions d'application intégrées**.
3. Selon les actions personnalisées disponibles, effectuez l'une des opérations suivantes.
   - Si la ressource agrégée comprend une ressource CyberApp, cliquez sur l'action.
   - Si la ressource agrégée comprend plusieurs ressources CyberApp, cliquez sur le nom de l'application CyberApp, puis sur l'action.

Association de ressources à des utilisateurs spécifiques

Remarque
Cette fonctionnalité n'est disponible que si le service PSA est activé.

En associant une ressource à un utilisateur spécifique, vous pouvez l'associer automatiquement à de nouveaux tickets du service d'assistance créé par l'utilisateur ou qui lui sont affectés.

Pour associer une ressource à un utilisateur

© Acronis International GmbH, 2003-2026

1. Accédez à **Terminaux** > **Tous les terminaux**, puis sélectionnez la ressource pertinente.
2. Dans le panneau **Actions**, sélectionnez **Associer à un utilisateur**.
3. Sélectionnez l'utilisateur souhaité.

   Vous pouvez également modifier l'utilisateur sélectionné pour les ressources associées existantes si nécessaire.
4. Cliquez sur **Terminé**.

   L'utilisateur sélectionné s'affiche désormais dans la colonne **Utilisateur lié**.

Pour dissocier une ressource d'un utilisateur

1. Accédez à **Terminaux** > **Tous les terminaux**, puis sélectionnez la ressource pertinente.
2. Dans le panneau **Actions**, sélectionnez **Associer à un utilisateur**.
3. Cliquez sur **Dissocier l'utilisateur**.
4. Cliquez sur **Terminé**.

Consultation du dernier utilisateur connecté

Si vous activez l'option **Afficher le dernier utilisateur connecté** dans le plan de gestion à distance appliqué à une ressource, le système enregistrera dans le journal les informations sur les utilisateurs qui se connectent au terminal. Vous pouvez consulter ces informations dans le tableau de bord ou dans les détails de la ressource.

Pour plus d'informations sur le paramètre **Afficher la dernière connexion**, voir Plans de gestion à distance.

Pour voir l'utilisateur qui s'est connecté en dernier à un terminal

1. Cliquez sur **Terminaux**.

   L'écran **Tous les terminaux** s'ouvre. Dans la colonne **Dernière connexion**, vous pouvez voir le nom de l'utilisateur qui s'est connecté en dernier sur chaque terminal. Dans la colonne **Heure de la dernière connexion**, vérifiez l'heure à laquelle l'utilisateur s'est connecté en dernier sur chaque terminal.
2. Cliquez sur un terminal dont vous souhaitez consulter les détails.
3. Cliquez sur l'icône **Détails**.
4. Dans la section **Derniers utilisateurs connectés**, vérifiez le nom de l'utilisateur qui s'est connecté en dernier au terminal ainsi que la date et l'heure de la dernière connexion.

Remarque
Le système répertorie jusqu'à 5 utilisateurs différents qui se sont connectés en dernier au terminal.

© Acronis International GmbH, 2003-2026

Score #CyberFit pour les machines

Le Score #CyberFit vous fournit un mécanisme d'évaluation et de notation de la sécurité qui évalue l'état de la sécurité de votre machine. Il identifie les failles de sécurité de l'environnement informatique et les vecteurs d'attaques ouvertes vers les terminaux, et recommande des actions d'amélioration sous la forme d'un rapport. Cette fonctionnalité est disponible dans toutes les éditions de Cyber Protect.

La fonctionnalité Score #CyberFit est prise en charge sur :

- Windows 7 (première version) et versions ultérieures
- Windows Server 2008 R2 et versions ultérieures

Fonctionnement

L'agent de protection installé sur une machine procède à une évaluation de la sécurité et calcule le Score #CyberFit de la machine. Le Score #CyberFit d'une machine est recalculé régulièrement de façon automatique.

Mécanisme de notation #CyberFit

Le Score #CyberFit d'une machine est calculé sur la base des indicateurs suivants :

- Protection antimalware 0-275
- Protection des sauvegardes 0-175
- Pare-feu 0-175
- Réseau privé virtuel (VPN) 0-75
- Chiffrement du disque intégral 0-125
- Sécurité du réseau 0-25

Le Score #CyberFit maximum d'une machine est de 850.

Indicateur	Qu'est-ce qui est évalué ?	Recommandations aux utilisateurs	Score
Antimalware	L'agent vérifie si un logiciel antimalware est installé ou non sur une machine.	Résultats : • Votre protection antimalware est activée (+275 points) • Vous n'avez pas de protection antimalware ; votre système pourrait courir un risque (0 point) Recommandations fournies par le Score #CyberFit : Vous devriez avoir une solution antimalware	275 : un logiciel antimalware est installé sur une machine 0 : aucun logiciel antimalware n'est installé

© Acronis International GmbH, 2003-2026

		installée et activée sur votre machine, afin qu'elle reste protégée contre les risques en matière de sécurité. Nous vous invitons à consulter des sites tels que AV-Test ou AV-Comparatives pour obtenir une liste des solutions antimalware recommandées.	sur une machine
Sauvegarde	L'agent vérifie si une solution de sauvegarde est installée sur un ordinateur.	Résultats : • Vous avez une solution de sauvegarde qui protège vos données (+175 points) • Aucune solution de sauvegarde n'a été trouvée ; vos données pourraient courir un risque (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons de sauvegarder vos données régulièrement afin d'éviter la perte de données ou les attaques par ransomware. Vous trouverez ci-dessous des solutions de sauvegarde à envisager : • Acronis Cyber Protect/Cyber Backup/True Image • Sauvegarde de serveur Windows (Windows Server 2008 R2 et versions ultérieures)	175 : une solution de sauvegarde est installée sur une machine 0 : aucune solution de sauvegarde n'est installée sur une machine
Pare-feu	L'agent vérifie si un pare-feu est disponible et activé dans votre environnement. L'agent effectue les actions suivantes : 1. Vérifie le pare-feu Windows et la protection du réseau pour savoir si un pare-feu public est activé. 2. Vérifie le pare-feu Windows et la protection du	Résultats : • Vous avez un pare-feu activé pour les réseaux publics et privés, ou une solution de pare-feu tierce a été trouvée (+175 points) • Vous avez un pare-feu activé uniquement pour les réseaux publics (+100 points) • Vous avez un pare-feu activé uniquement pour les réseaux privés (+75 points) • Vous n'avez pas de pare-feu activé ; vos connexions réseau ne sont pas sécurisées (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons d'activer un pare-feu pour vos réseaux publics et privés afin d'améliorer votre protection contre les attaques malveillantes envers votre système. Vous trouverez ci-dessous des guides détaillés concernant la configuration de	100 : un pare-feu public Windows est activé 75 : un pare-feu privé Windows est activé 175 : des pare-feu publics et privés Windows sont activés OU une solution de pare-feu tierce est activée

© Acronis International GmbH, 2003-2026

	réseau pour savoir si un pare-feu privé est activé. 3. Vérifie la solution/l'agent de pare-feu tiers pour savoir si des pare-feu Windows publics ou privés sont désactivés.	votre pare-feu Windows, en fonction de vos besoins de sécurité et de l'architecture de votre réseau : Guides pour les utilisateurs finaux / employés : Comment configurer le Pare-feu Windows Defender sur votre PC Comment configurer le Pare-feu Windows sur votre PC Guides pour les administrateurs et ingénieurs système : Comment déployer le Pare-feu Windows Defender avec la sécurité avancée Comment créer des règles avancées dans le Pare-feu Windows	0 : aucun pare-feu Windows ni solution de pare-feu tierce n'est activé
Réseau privé virtuel (VPN)	L'agent vérifie si une solution VPN est installée sur une machine et si le VPN est activé et en cours d'exécution.	Résultats : • Vous avez une solution VPN, et pouvez recevoir et envoyer des données en toute sécurité sur les réseaux publics et partagés (+75 points) • Aucune solution VPN n'a été trouvée ; votre connexion aux réseaux publics et partagés n'est pas sécurisée (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons d'utiliser un VPN pour accéder à votre réseau d'entreprise et à vos données confidentielles. Il est essentiel d'utiliser un VPN pour que vos communications restent sécurisées et privées, en particulier si vous utilisez la connexion Internet gratuite d'un café, d'une bibliothèque, d'un aéroport ou autre. Vous trouverez ci-dessous des solutions de VPN à envisager : • VPN Acronis Business • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81	75 : un VPN est activé et en cours d'exécution 0 : aucun VPN n'est activé

© Acronis International GmbH, 2003-2026

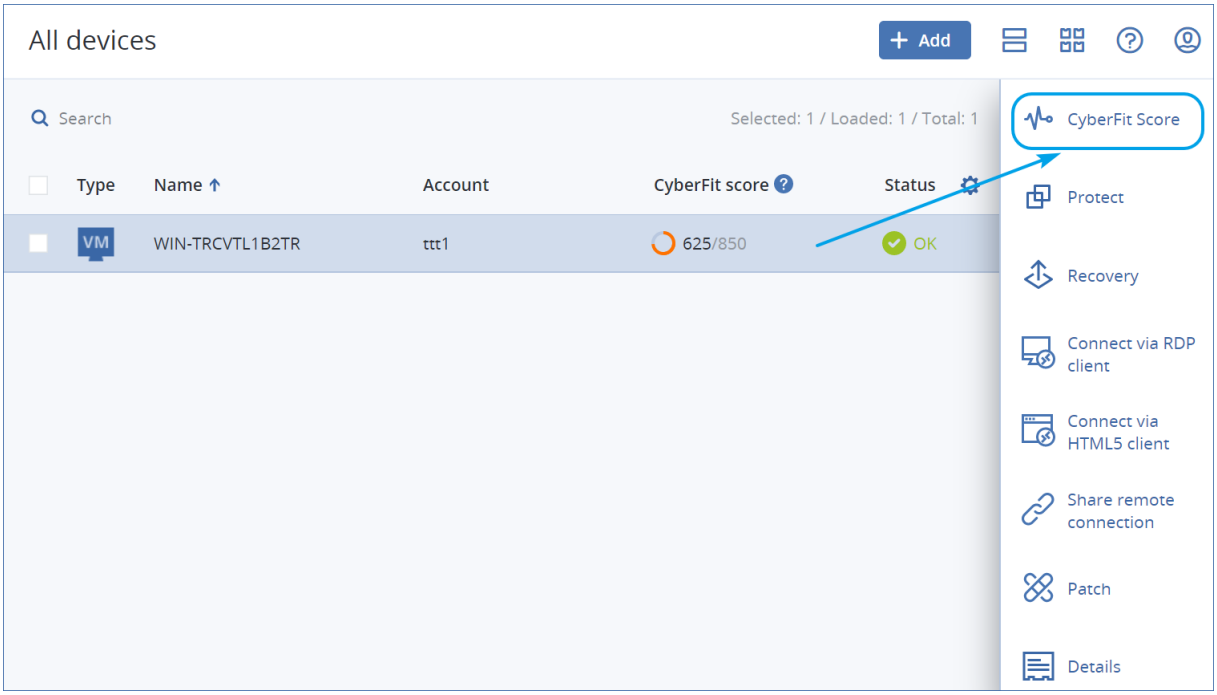
		• VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
Chiffrement de disque	L'agent vérifie si le chiffrement du disque est activé sur une machine. L'agent vérifie si Windows BitLocker est activé.	Résultats : • Votre chiffrement complet de disque est activé ; votre machine est protégée contre l'altération physique (+125 points) • Seuls certains disques durs sont chiffrés ; votre machine pourrait courir un risque d'altération physique (+75 points) • Aucun chiffrement de disque n'a été trouvé ; votre machine court un risque d'altération physique (0 point) Recommandations fournies par le Score #CyberFit : Nous vous recommandons d'activer Windows BitLocker afin d'améliorer la protection de vos données et fichiers. Guide : Comment activer un terminal de chiffrement dans Windows	125 : tous les disques sont chiffrés 75 : au moins un de vos disques est chiffré, mais il existe également des disques non chiffrés 0 : aucun disque n'est chiffré
Sécurité du réseau (trafic NTLM sortant vers des serveurs distants)	L'agent vérifie si le trafic NTLM sortant d'une machine est restreint vers des serveurs distants.	Résultats : • Le trafic NTLM sortant vers des serveurs distants est refusé ; vos identifiants sont protégés (+25 points) • Le trafic NTLM sortant vers des serveurs distants n'est pas refusé ; vos identifiants pourraient être exposés (0 point) Recommandations fournies par le Score #CyberFit : Pour une meilleure protection, nous vous recommandons de refuser tout le trafic NTLM sortant vers des serveurs distants. Vous pouvez trouver des informations sur la façon dont modifier les paramètres NTLM et ajouter des exceptions en cliquant sur le lien ci-dessous. Guide : Restreindre le trafic NTLM sortant vers des serveurs distants	25 : le trafic NTLM sortant est défini sur ToutRefuser 0 : le trafic NTLM sortant est défini sur une autre valeur

© Acronis International GmbH, 2003-2026

Sur la base des points cumulés attribués à chaque indicateur, le Score #CyberFit total d'une machine peut correspondre à l'une des notations suivantes, qui reflète le niveau de protection du terminal :

- 0 - 579 : Mauvais
- 580 - 669 : Passable
- 670 - 739 : Bon
- 740 - 799 : Très bon
- 800 - 850 : Excellent

Vous pouvez consulter le Score #CyberFit de vos machines dans la console Cyber Protect : accédez à **Terminaux** > **Tous les terminaux**. Dans la liste des terminaux, vous pouvez voir la colonne **Score #CyberFit**. Vous pouvez également exécuter l'analyse du Score #CyberFit d'une machine pour vérifier sa posture en matière de sécurité.



Vous pouvez également obtenir des informations concernant le Score #CyberFit sur les pages de widget et de rapport correspondantes.

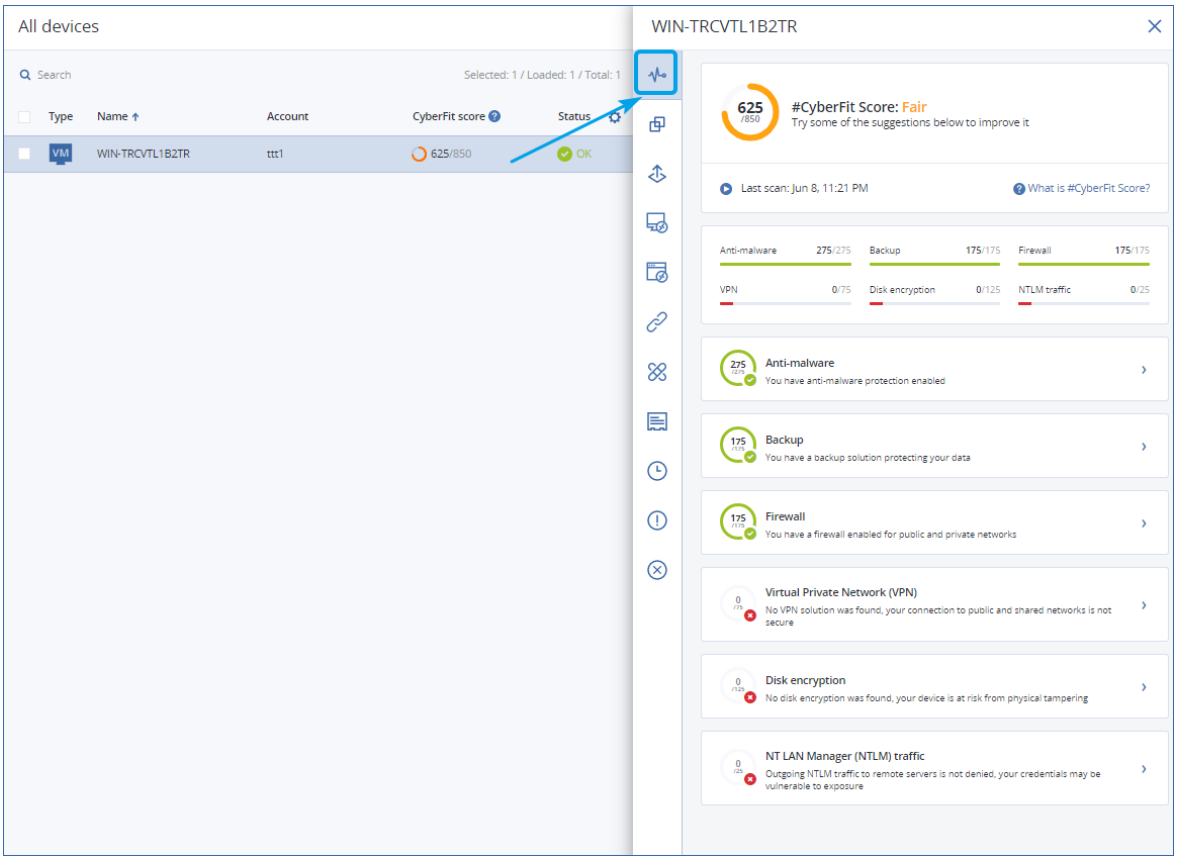
Lancer une analyse du Score #CyberFit

Pour lancer une analyse du Score #CyberFit

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez la machine, puis cliquez sur **Score #CyberFit**.
3. Si la machine n'a jamais été analysée, cliquez sur **Exécuter une première analyse**.

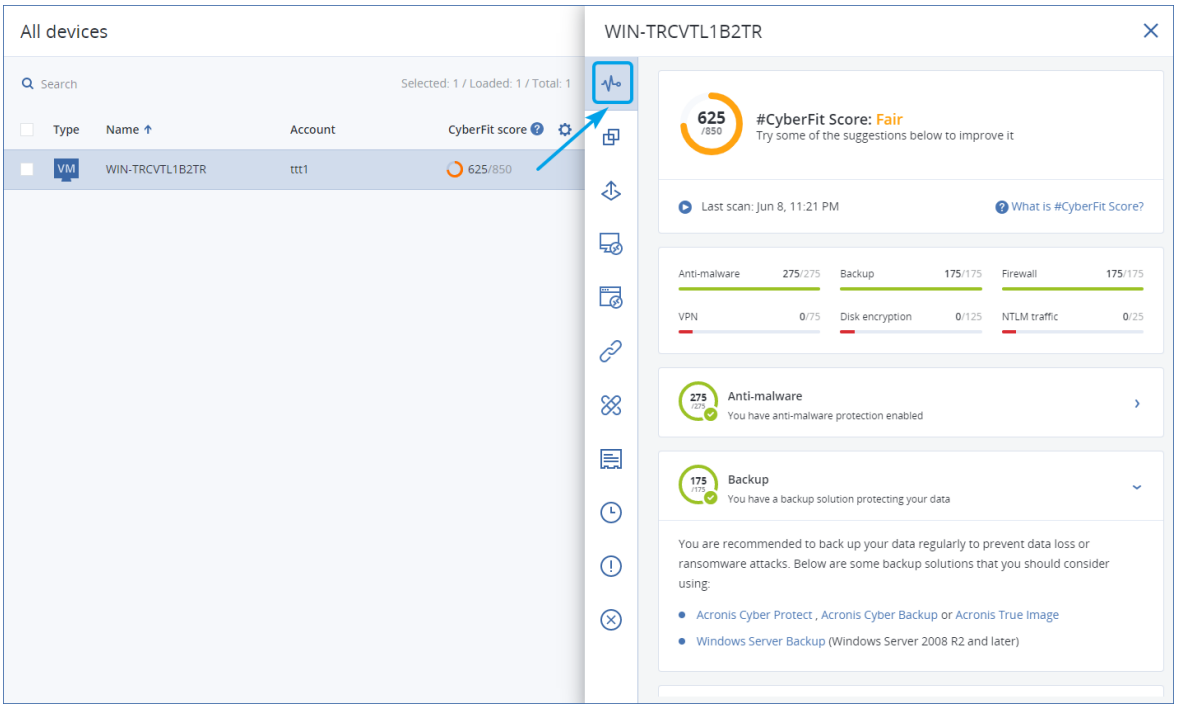
© Acronis International GmbH, 2003-2026

4. Une fois l'analyse terminée, vous verrez le Score #CyberFit total de la machine, ainsi que les scores de chacun des six indicateurs évalués : Antimalware, Sauvegarde, Pare-feu, Réseau privé virtuel (VPN), Chiffrement de disque et Trafic sortant NT LAN Manager (NTLM).



5. Pour vérifier comment améliorer le score de chaque indicateur pour lequel les configurations de sécurité pourraient être améliorées, développez la section correspondante et lisez les recommandations.

© Acronis International GmbH, 2003-2026



6. Après mis les recommandations en place, vous pouvez toujours recalculer le Score #CyberFit de la machine en cliquant sur le bouton flèche juste en dessous du Score #CyberFit total.

Création de cyber-scripts

Avec la création de cyberscripts, vous pouvez automatiser des opérations de routine sur les ordinateurs Windows et macOS de votre environnement : installation de logiciels, modification de configuration, démarrage ou arrêt de services, et création de comptes. Vous pouvez ainsi réduire le risque d'erreur et le temps passé sur de telles opérations lorsque vous les effectuez manuellement.

La création de cyberscripts est disponible pour les administrateurs et utilisateurs au niveau du client, ainsi que pour les administrateurs partenaires (fournisseurs de services). Pour plus d'informations sur les différents niveaux d'administration, voir "Niveaux d'administration dans la console Cyber Protect" (p. 387).

Les scripts que vous pouvez utiliser doivent être approuvés au préalable. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent approuver et tester de nouveaux scripts. Pour plus d'informations sur la modification du statut des scripts, voir "Modification de l'état du script" (p. 501).

En fonction de votre rôle, vous pouvez effectuer des opérations différentes sur les scripts et les plans de script. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

Prérequis

- La fonctionnalité Cyber Scripting nécessite la licence RMM (modèle de licence basé sur le service) ou la licence Sécurité et RMM (modèle de licence basé sur la solution).

© Acronis International GmbH, 2003-2026

- Pour utiliser toutes les fonctions de création de cyber-scripts, comme la modification ou l'exécution de scripts, la création de plans de création de scripts, etc., vous devez activer l'authentification à deux facteurs pour votre compte.

Limites

- Les langages de script suivants sont pris en charge :
  - PowerShell
  - Bash
- Les opérations de création de scripts ne peuvent être exécutées que sur les ordinateurs cibles sur lesquels un agent de protection est installé.

Plates-formes prises en charge

Cyber Scripting est disponible pour les ressources Windows et macOS.

Le tableau suivant résume les versions prises en charge.

Système d'exploitation	Version
Windows	Windows 7 SP1 et versions ultérieures - toutes les éditions
	Windows 8/8.1 – toutes les éditions (x86, x64), sauf les éditions Windows RT
	Windows 10 - éditions Home, Pro, Education, Enterprise, IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 et versions ultérieures - éditions Standard, Enterprise, Datacenter, Foundation et Web
	Windows Server 2012/2012 R2 – toutes les éditions
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

© Acronis International GmbH, 2003-2026

Rôles d'utilisateur et droits de création de cyber-scripts

Les actions disponibles avec les scripts et les plans de création de scripts dépendent de l'état du script et de votre rôle d'utilisateur.

Les administrateurs peuvent gérer des objets, tels que des plans ou des ressources, dans leurs propres tenants et dans leurs tenants enfants, avec les limitations suivantes :

- Les tenants clients peuvent restreindre l'accès des administrateurs partenaires.
- Les unités peuvent toujours être accessibles par les administrateurs clients et les administrateurs partenaires qui gèrent le tenant client parent.

Les administrateurs ne peuvent pas voir ou accéder aux objets à un niveau supérieur à leur propre tenant.

Les administrateurs de niveau inférieur n'ont qu'un accès en lecture seule aux plans de création de scripts appliqués à leurs ressources par un administrateur de niveau supérieur.

Les rôles suivants octroient des droits en matière de création de cyber-scripts :

- **Administrateur d'entreprise**
  Ce rôle octroie des droits d'administrateur complets dans tous les services. Concernant la création de cyber-scripts, il octroie les mêmes droits que le rôle Cyberadministrateur.
- **Cyberadministrateur**
  Ce rôle octroie des autorisations complètes, y compris l'approbation des scripts qui peuvent être utilisés dans le tenant, et la capacité à exécuter des scripts avec l'état **Test**.
- **Administrateur**
  Ce rôle octroie des autorisations partielles, avec la capacité d'exécuter des scripts approuvés, ainsi que de créer et d'exécuter des plans de création de scripts qui utilisent des scripts approuvés.
- **Administrateur en lecture seule**
  Ce rôle octroie des autorisations limitées, avec la capacité de visualiser les scripts et les plans de protection utilisés dans le tenant.
- **Utilisateur**
  Ce rôle octroie des autorisations partielles, avec la capacité d'exécuter des scripts approuvés, ainsi que de créer et d'exécuter des plans de création de scripts qui utilisent des scripts approuvés, mais uniquement sur le propre ordinateur de l'utilisateur.

Le tableau suivant résume toutes les actions disponibles, en fonction de l'état du script et du rôle de l'utilisateur.

Rôle	Objet	État du script		
		Brouillon	Test	Approuvé

© Acronis International GmbH, 2003-2026

Cyberadministrateur **Administrateur d'entreprise**	Plan de création de script	Modifier (supprimer un brouillon de script d'un plan) Supprimer Retirer Désactiver Arrêter	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter
	Script	Créer Modifier Modifier l'état Cloner Supprimer Annuler l'exécution	Créer Modifier Modifier l'état Exécuter Cloner Supprimer Annuler l'exécution	Créer Modifier Modifier l'état Exécuter Cloner Supprimer Annuler l'exécution
Administrateur **Utilisateur** (pour ses propres ressources)	Plan de création de script	Affichage Modifier Retirer Désactiver Arrêter	Affichage Annuler l'exécution	Créer Modifier Appliquer Activer Exécuter Supprimer Retirer Désactiver Arrêter
	Script	Créer Modifier Cloner Supprimer Annuler l'exécution	Affichage Cloner Annuler l'exécution	Exécuter Cloner Annuler l'exécution

© Acronis International GmbH, 2003-2026

Administrateur en lecture seule	Plan de création de script	Affichage	Affichage	Affichage
	Script	Affichage	Affichage	Affichage

Scripts

Un script est un ensemble d'instructions interprétées lors de l'exécution et exécutées sur une machine cible. Les scripts offrent une solution pratique pour l'automatisation de tâches répétitives ou complexes.

Avec la création de cyberscripts, vous pouvez exécuter un script prédéfini ou créer un script personnalisé. Tous les scripts à votre disposition se trouvent dans **Gestion** > **Référentiel de scripts**. Les scripts prédéfinis se trouvent dans la section **Bibliothèque**. Les scripts que vous avez créés ou clonés sur votre tenant se trouvent dans la section **Mes scripts**.

Vous pouvez utiliser un script en l'incluant dans un plan de création de scripts ou en lançant une opération **Exécution rapide du script**.

Remarque
Vous ne pouvez utiliser que des scripts approuvés, créés ou clonés dans votre tenant. Si un script a été supprimé du référentiel de scripts ou est en état de **brouillon**, il ne s'exécutera pas. Vous pouvez vérifier les détails d'une opération de script ou l'annuler dans **Surveillance** > **Activités**.

Le tableau suivant fournit plus d'informations sur les actions possibles avec un script en fonction de son statut.

Statut	Actions possibles
Brouillon	Les nouveaux scripts que vous créez et ceux que vous clonez dans votre référentiel ont le statut de **brouillon**. Vous n'êtes pas autorisé à exécuter ces scripts ni à les inclure dans des plans de script.
Test	Les administrateurs ayant le rôle de **cyberadministrateur** peuvent exécuter ces scripts et les inclure dans les plans de script.
Approuvé	Vous pouvez exécuter ces scripts et les inclure dans des plans de script.

Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent modifier le statut d'un script ou supprimer un script approuvé. Pour plus d'informations, voir "Modification de l'état du script" (p. 501).

Création d'un script

Vous pouvez créer un script en écrivant le code manuellement.

Créer un script

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion** > **Référentiel de scripts**.
2. Dans **Mes scripts**, cliquez sur **Créer un script à l'aide de l'intelligence artificielle**.
3. Dans le volet principal, écrivez le corps du script.

Important
Lorsque vous créez un script, incluez des vérifications de code de sortie pour chaque opération. Dans le cas contraire, l'échec d'une opération pourrait être ignoré et l'état d'activité de création de script dans **Surveillance** > **Activités** pourrait indiquer **Succès** alors que cela n'est pas le cas.

4. Spécifiez les paramètres de script.

Paramètre	Description
Nom du script	Nom du script. Le champ est rempli automatiquement, mais vous pouvez en modifier la valeur.
Description	Description du script. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] Le champ sera rempli automatiquement lors de la génération du script. Vous pouvez modifier la description fournie par l'intelligence artificielle.
Langue	Langage du script. Les valeurs disponibles sont les suivantes : • **PowerShell**. Il s'agit de la valeur par défaut. • **Bash** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré avant la génération du script.
Système d'exploitation	Système d'exploitation installé sur la ressource cible sur laquelle le script sera exécuté. Les valeurs disponibles sont les suivantes : • **Windows**. Il s'agit de la valeur par défaut. • **macOS** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré avant la génération du script.
Statut	État du script. • **Brouillon**. Il s'agit de la valeur par défaut. Les nouveaux scripts que vous créez et ceux que vous clonez dans votre référentiel sont à l'état de **Brouillon**. Vous n'êtes pas autorisé à exécuter des scripts **Brouillons** ni à les inclure dans des plans de script. • **Test**. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent changer le statut d'un script en **Test**, exécuter des scripts avec ce statut **Test** et des plans de script avec ces scripts. • **Approuvé**. Vous pouvez exécuter des scripts **approuvés** et les inclure dans des plans de script. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent modifier le statut d'un script ou supprimer un script approuvé. Pour plus d'informations, voir "Modification de l'état du script" (p. 501).

© Acronis International GmbH, 2003-2026

Paramètre	Description
Mots-clés	Les mots-clés ne sont pas sensibles à la casse et peuvent compter jusqu'à 32 caractères. Vous ne pouvez utiliser ni parenthèses, ni crochets, ni virgules, ni espaces. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] La balise **générée par l'intelligence artificielle** est ajoutée automatiquement lors de la génération du script. Vous pouvez la supprimer manuellement ou en ajouter d'autres.

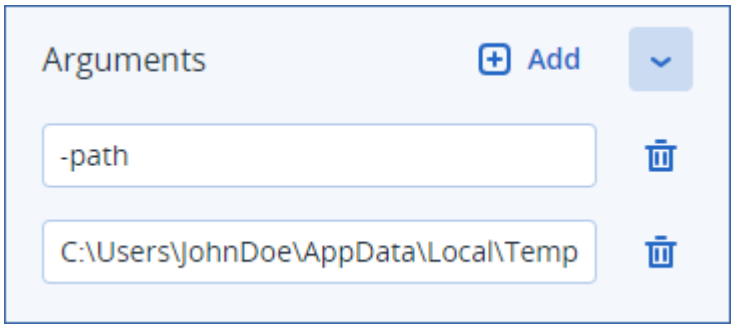
5. [Uniquement pour les scripts qui nécessitent des identifiants] Spécifiez les identifiants.

   Vous pouvez utiliser un identifiant unique (par exemple, un jeton) ou une paire d'identifiants (par exemple, un nom d'utilisateur et un mot de passe).
6. [Uniquement pour les scripts qui nécessitent des arguments] Spécifiez les arguments et leurs valeurs, comme suit :
   a. Cliquez sur **Ajouter**.
   b. Dans le champ **Ajouter des arguments**, indiquez l'argument.
   c. Cliquez sur **Ajouter**.
   d. Dans le deuxième champ qui apparaît, indiquez la valeur de l'argument.

   Remarque
   Vous ne pouvez spécifier que les arguments que vous avez déjà définis dans le corps du script.

   Par exemple :

   e. Répétez les étapes ci-dessus si vous avez besoin d'ajouter plusieurs arguments.

© Acronis International GmbH, 2003-2026

7. Cliquez sur **Enregistrer**.

Le script est enregistré dans votre référentiel avec le statut **Brouillon**.

Vous ne pouvez utiliser le script que lorsqu'un administrateur ayant le rôle de **cyberadministrateur** a changé son statut en **Approuvé**. Pour plus d'informations, voir "Modification de l'état du script" (p. 501).

Pour utiliser un script dans un autre tenant que vous gérez, vous devez cloner ce script dans ce tenant. Pour plus d'informations, voir "Clonage d'un script" (p. 499).

Création d'un script à l'aide de l'intelligence artificielle

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

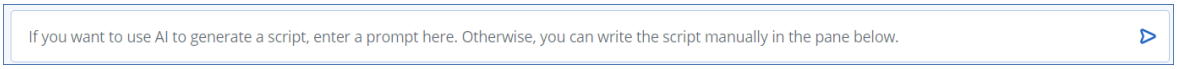
Vous pouvez utiliser l'intelligence artificielle pour transformer les invites en scripts puissants, ce qui vous permet d'économiser du temps et des efforts. Vous pouvez utiliser cette fonctionnalité des manières suivantes :

- Saisissez une invite pour demander à l'intelligence artificielle de créer un script de toutes pièces.
- Saisissez une invite pour demander à l'intelligence artificielle d'examiner et de compléter un code que vous avez saisi dans le corps du script. Vous pouvez utiliser cette fonction lorsque vous avez des difficultés avec des codes plus complexes.

Cette fonctionnalité utilise le modèle GPT-4 d'OpenAI. Vous pouvez l'utiliser pour créer pour votre organisation jusqu'à 100 scripts par mois calendaire, gratuitement.

Pour créer un script en utilisant l'intelligence artificielle

1. Dans la console Cyber Protect, accédez à **Gestion** > **Référentiel de scripts**.
2. Dans **Mes scripts**, cliquez sur **Créer un script à l'aide de l'intelligence artificielle**.
3. Dans l'invite, entrez une description de l'opération que le script doit effectuer. Veillez à ce que la description que vous saisissez soit aussi claire et détaillée que possible.

   Par exemple :

   ```
   I need a script that deletes Temporary files for all users (including user profiles +
   Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. Dans l'invite, cliquez sur le bouton fléché.
5. Dans la fenêtre de confirmation, sélectionnez la langue et le système d'exploitation, puis cliquez sur **Générer**.

   Le script généré par l'intelligence artificielle s'affiche dans le volet principal. Le nom et la description du script sont automatiquement générés par l'intelligence artificielle afin qu'ils

© Acronis International GmbH, 2003-2026

correspondent au script. La balise **Généré par l'intelligence artificielle** est automatiquement attribuée au script.

6. Examinez le script généré par l'intelligence artificielle et, si nécessaire, modifiez-le manuellement.
7. Si nécessaire, modifiez les paramètres du script.

Paramètre	Description
Nom du script	Nom du script. Le champ est rempli automatiquement, mais vous pouvez en modifier la valeur.
Description	Description du script. Ce paramètre est facultatif. [Pour les scripts générés par l'intelligence artificielle] Le champ sera rempli automatiquement lors de la génération du script. Vous pouvez modifier la description fournie par l'intelligence artificielle.
Langue	Langage du script. Les valeurs disponibles sont les suivantes : • **PowerShell**. Il s'agit de la valeur par défaut. • **Bash** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré avant la génération du script.
Système d'exploitation	Système d'exploitation installé sur la ressource cible sur laquelle le script sera exécuté. Les valeurs disponibles sont les suivantes : • **Windows**. Il s'agit de la valeur par défaut. • **macOS** [Pour les scripts générés par l'intelligence artificielle] Ce paramètre est configuré avant la génération du script.
Statut	État du script. • **Brouillon**. Il s'agit de la valeur par défaut. Les nouveaux scripts que vous créez et ceux que vous clonez dans votre référentiel sont à l'état de **Brouillon**. Vous n'êtes pas autorisé à exécuter des scripts **Brouillons** ni à les inclure dans des plans de script. • **Test**. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent changer le statut d'un script en **Test**, exécuter des scripts avec ce statut **Test** et des plans de script avec ces scripts. • **Approuvé**. Vous pouvez exécuter des scripts **approuvés** et les inclure dans des plans de script. Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent modifier le statut d'un script ou supprimer un script approuvé. Pour plus d'informations, voir "Modification de l'état du script" (p. 501).
Mots-clés	Les mots-clés ne sont pas sensibles à la casse et peuvent compter jusqu'à 32 caractères. Vous ne pouvez utiliser ni parenthèses, ni crochets, ni virgules, ni espaces. Ce paramètre est facultatif.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	[Pour les scripts générés par l'intelligence artificielle] La balise **générée par l'intelligence artificielle** est ajoutée automatiquement lors de la génération du script. Vous pouvez la supprimer manuellement ou en ajouter d'autres.

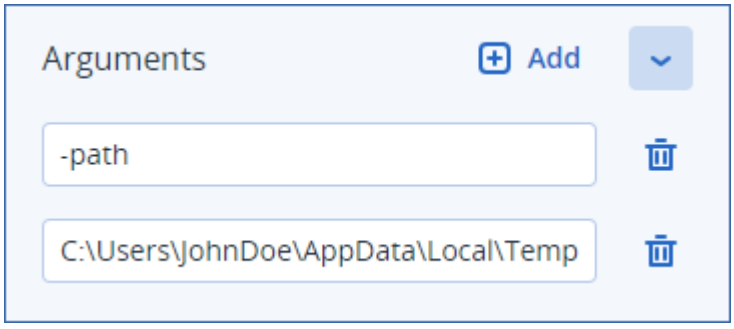
8. [Facultatif] [Uniquement pour les scripts qui nécessitent des identifiants] Spécifiez les identifiants.

   Vous pouvez utiliser un identifiant unique (par exemple, un jeton) ou une paire d'identifiants (par exemple, un nom d'utilisateur et un mot de passe).
9. [Uniquement pour les scripts qui nécessitent des arguments] Spécifiez les arguments et leurs valeurs, comme suit :
   a. Cliquez sur **Ajouter**.
   b. Dans le champ **Ajouter des arguments**, indiquez l'argument.
   c. Cliquez sur **Ajouter**.
   d. Dans le deuxième champ qui apparaît, indiquez la valeur de l'argument.

   Remarque
   Vous ne pouvez spécifier que les arguments que vous avez déjà définis dans le corps du script.

   Par exemple :

   e. Répétez les étapes ci-dessus si vous avez besoin d'ajouter plusieurs arguments.
10. Cliquez sur **Enregistrer**.

    Le script est enregistré dans votre référentiel avec le statut **Brouillon**.

© Acronis International GmbH, 2003-2026

Vous ne pouvez utiliser le script que lorsqu'un administrateur ayant le rôle de **cyberadministrateur** a changé son statut en **Approuvé**. Pour plus d'informations, voir "Modification de l'état du script" (p. 501).

Pour utiliser un script dans un autre tenant que vous gérez, vous devez cloner ce script dans ce tenant. Pour plus d'informations, voir "Clonage d'un script" (p. 499).

Clonage d'un script

Le clonage d'un script est nécessaire dans les cas suivants :

- Avant d'utiliser un script de la **bibliothèque**. Dans ce cas, vous devez d'abord cloner le script dans la section **Mes scripts**.
- Quand vous souhaitez cloner des scripts que vous avez créé dans un tenant parent dans ses tenants ou unités enfant.

Cloner un script

1. Dans **Référentiel de scripts**, trouvez le script que vous souhaitez cloner.
2. Effectuez l'une des actions suivantes :
   - [Si vous clonez un script depuis **Mes scripts**] Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Cloner**.
   - [Si vous clonez un script depuis **Bibliothèque**] Cliquez sur **Cloner** à côté du nom du script que vous avez sélectionné.
3. Dans la fenêtre contextuelle **Cloner le script**, sélectionnez l'un des états de script suivants dans la liste déroulante **État** :
   - **Brouillon** (par défaut) : ce statut ne vous permet pas d'exécuter le script immédiatement.
   - **Test** : ce statut vous permet d'exécuter le script.
   - **Approuvé** : ce statut vous permet d'exécuter le script.
4. [Si vous gérez plusieurs tenants ou unités] Sélectionnez l'emplacement où vous souhaitez cloner le script.

   Dans la boîte de dialogue **Cloner le script**, vous ne voyez que les tenants que vous pouvez gérer et qui ont la licence RMM (modèle de licence basé sur le service) ou la licence Sécurité et RMM (modèle de licence basé sur la solution).

Le script est alors cloné dans la section **Mes scripts** du tenant ou de l'unité que vous avez sélectionné. Si vous gérez un seul tenant ne comportant aucune unité, le script est automatiquement copié dans votre section **Mes scripts**.

Important
Les identifiants qu'un script utilise ne sont pas copiés lorsque vous clonez un script vers un tenant autre que le tenant d'origine.

© Acronis International GmbH, 2003-2026

Modification ou suppression d'un script

Remarque
En fonction de votre rôle, vous pouvez effectuer des opérations différentes sur les scripts et les plans de script. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

Modifier un script

1. Dans **Référentiel de scripts**, accédez à **Mes scripts**, puis trouvez le script que vous souhaitez modifier.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Modifier**.
3. Modifiez le script, puis cliquez sur **Enregistrer**.
4. [Si vous modifiez un script utilisé par un plan de création de scripts] Confirmez votre choix en cliquant sur **Enregistrer le script**.

   Remarque
   La dernière version du script sera utilisée lors de la prochaine exécution du plan de création de scripts.

Versions du script

Une nouvelle version du script est créée si vous modifiez l'un des attributs de script suivants :

- corps du script
- nom du script
- description
- langage de script
- informations d'identification
- arguments

Si vous modifiez d'autres attributs, vos modifications seront ajoutées à la version du script actuelle. Pour en savoir plus sur les versions et sur la manière de les comparer, reportez-vous à "Comparaison de versions de script" (p. 501).

Remarque
L'état du script est mis à jour uniquement lorsque vous modifiez la valeur du champ **État**. Seuls les administrateurs disposant du rôle Cyberadministrateur peuvent modifier l'état d'un script.

Supprimer un script

1. Dans **Référentiel de scripts**, accédez à **Mes scripts**, puis trouvez le script que vous souhaitez supprimer.

© Acronis International GmbH, 2003-2026

2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Supprimer**.
3. Cliquez sur **Supprimer**.
4. [Si vous souhaitez modifier un script utilisé par un plan de création de scripts] Confirmez votre choix en cliquant sur **Enregistrer le script**.

Remarque
Les plans de création de scripts qui utilisent le script supprimé ne s'exécuteront plus.

Modification de l'état du script

Un nouveau script créé et se trouvant dans l'état **Brouillon** ne peut pas être utilisé tant que son statut n'est pas passé à **Approuvé**. Selon le cas d'utilisation, un script peut rester dans l'état **Test** pendant un certain temps avant d'être approuvé.

Remarque
En fonction de votre rôle, vous pouvez effectuer des opérations différentes sur les scripts et les plans de script. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

Prérequis

- Votre utilisateur est un administrateur auquel a été attribué le rôle de **cyberadministrateur**.
- Un script avec l'état correspondant est disponible.

Modifier l'état du script

1. Dans le **référentiel de scripts**, accédez à **Mes scripts**.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Modifier**.
3. Dans la liste déroulante **Statut**, sélectionnez le statut.
4. Cliquez sur **Enregistrer**.
5. [Si vous modifiez le statut d'un script approuvé] Pour confirmer la modification, cliquez sur **Enregistrer le script**.

Remarque
Si l'état du script a été modifié et défini sur **Brouillon**, les plans de création de scripts qui l'utilisent ne s'exécuteront plus.

Seuls les administrateurs ayant le rôle de **cyberadministrateur** peuvent exécuter des scripts dans l'état de **test** et des plans de script avec de tels scripts.

Comparaison de versions de script

Vous pouvez comparer deux versions d'un script et rétablir une version précédente de ce dernier. Vous pouvez également vérifier qui a créé une version spécifique et quand cela a été fait.

© Acronis International GmbH, 2003-2026

Comparer des versions de script

1. Dans **Référentiel de scripts**, accédez à **Mes scripts**, puis trouvez le script dont vous souhaitez comparer les versions.
2. Cliquez sur les points de suspension (...) situés à côté du nom du script, puis cliquez sur **Historique des versions**.
3. Sélectionnez deux versions à comparer, puis cliquez sur **Comparer les versions**.
   Toute modification apportée au corps de texte du script, à ses arguments ou aux identifiants est mise en évidence.

Pour rétablir une version précédente

1. Dans la fenêtre **Comparer les versions de script**, cliquez sur **Rétablir à cette version**.
2. Dans la fenêtre contextuelle **Revenir à une version antérieure**, sélectionnez l'état du script dans la liste déroulante **État**.

La version sélectionnée est restaurée et enregistrée en tant que version la plus récente dans l'historique des versions.

Pour restaurer un script, vous pouvez également sélectionner une version dans la fenêtre **Historique des versions**, puis cliquer sur le bouton **Restaurer**.

Important
Vous ne pouvez exécuter que des scripts dont le statut est **Test** ou **Approuvé**. Pour plus d'informations, voir "Modification de l'état du script" (p. 501).

Télécharger le résultat d'une opération de création de scripts

Vous pouvez télécharger le résultat d'une opération de création de scripts sous forme de fichier .zip. Elle contient deux fichiers texte : `stdout` et `stderr`. Dans `stdout`, vous pouvez afficher les résultats d'une opération de création de scripts réussie. Le fichier `stderr` contient des informations sur les erreurs qui se sont produites lors de l'opération de création de scripts.

Télécharger le fichier de résultat

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Activités**.
2. Cliquez sur l'activité de création de cyber-scripts dont vous souhaitez télécharger le résultat.
3. À l'écran **Détails de l'activité**, cliquez sur **Télécharger le résultat**.

Référentiel de scripts

Le référentiel de scripts se trouve dans l'onglet **Gestion**. Dans le référentiel, vous pouvez rechercher des scripts à l'aide de leur nom ou de leur description. Vous pouvez aussi utiliser les filtres, ou trier les scripts en fonction de leur nom ou de leur état.

© Acronis International GmbH, 2003-2026

Pour gérer un script, cliquez sur les points de suspension (...) situés à côté de son nom, puis sélectionnez l'action souhaitée. Vous pouvez aussi cliquer sur le script, puis vous servir des boutons présents sur l'écran qui apparaît.

Le référentiel de scripts doit contenir les sections suivantes :

- **Mes scripts**
  Vous y trouverez les scripts que vous pouvez utiliser directement dans votre environnement. Il s'agit des scripts que vous avez créés à partir de zéro et des scripts que vous avez clonés ici.
  Vous pouvez filtrer les scripts de cette section en fonction des critères suivants :
  - Mots-clés
  - Statut
  - Langue
  - Système d'exploitation
  - Propriétaire du script
- **Bibliothèque**
  La bibliothèque contient des scripts prédéfinis que vous pouvez utiliser dans votre environnement après les avoir clonés dans la section **Mes scripts**. Vous pouvez uniquement inspecter et cloner ces scripts.
  Vous pouvez filtrer les scripts de cette section en fonction des critères suivants :
  - Mots-clés
  - Langue
  - Système d'exploitation

  Pour plus d'informations, voir Scripts approuvés par le fournisseur (70595).

Plans de création de scripts

Un plan de création de scripts vous permet d'exécuter un script sur plusieurs ressources, de planifier l'exécution d'un script et de configurer des paramètres supplémentaires.

Les plans de création de scripts que vous avez créés et ceux appliqués à vos ressources sont disponibles dans **Gestion** > **Plans de création de scripts**. Ici, vous pouvez consulter le propriétaire ou l'état du plan, ainsi que son emplacement d'exécution.

Une barre sur laquelle vous pouvez cliquer affiche les états à code couleur suivants pour les plans de création de scripts :

- En cours d'exécution (bleu)
- Vérification de la compatibilité (gris foncé)
- Désactivé (gris clair)
- OK (verte)
- Alerte critique (rouge)

© Acronis International GmbH, 2003-2026

- Erreur (orange)
- Avertissement (jaune)

En cliquant sur la barre d'état, vous pouvez afficher l'état d'un plan et sur combien de ressources il s'applique. Il est également possible de cliquer sur chaque état.

Dans l'onglet **Plans de création de scripts**, vous pouvez gérer les plans en effectuant les actions suivantes :

- Exécuter
- Arrêter
- Modifier
- Renommer
- Désactiver
- Activer
- Cloner
- Exporter. La configuration du plan sera exportée au format JSON vers la machine locale.
- Supprimer

La visibilité d'un plan de création de scripts et des actions disponibles avec lui dépend du propriétaire du plan et de votre rôle d'utilisateur. Par exemple, les administrateurs d'entreprise ne peuvent voir que les plans de création de scripts appartenant au partenaire et appliqués à leurs ressources. Ils ne peuvent effectuer aucune action sur ces plans.

Pour plus d'informations sur les personnes autorisées à créer et à gérer des plans de création de scripts, reportez-vous à "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

Gérer un plan de création de scripts

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Trouvez le plan que vous souhaitez gérer, puis cliquez sur les points de suspension (...) correspondants.
3. Sélectionnez l'action souhaitée, puis suivez les instructions à l'écran.

Création d'un plan de création de scripts

Vous pouvez créer un plan de création de scripts de l'une des manières suivantes :

- Dans l'onglet **Terminaux**
  Sélectionnez des ressources, puis créez un plan de création de scripts pour elles.
- Dans l'onglet **Gestion** > **Plans de création de scripts**
  Créez un plan de création de scripts, puis sélectionnez les ressources auxquelles l'appliquer.

Créer un plan de création de scripts dans l'onglet Terminaux

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Sélectionnez les ressources ou les groupes de terminaux auxquels vous souhaitez appliquer un plan de création de scripts, puis cliquez respectivement sur **Protection** ou **Protéger un groupe**.
3. [Si des plans sont déjà appliqués] Cliquez sur **Ajouter un plan**.
4. Cliquez sur **Création d'un plan** > **Plan de création de scripts**.
   Un modèle pour le plan de création de scripts s'ouvre.
5. [Facultatif] Pour modifier le nom du plan de création de scripts, cliquez sur l'icône en forme de crayon.
6. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.

   Remarque
   Vous ne pouvez utiliser que vos scripts approuvés dans **Référentiel de scripts** >**Mes scripts**. Seul un administrateur ayant le rôle de **cyberadministrateur** peut utiliser des scripts à l'état de **Test**. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

7. Configurez la planification et les conditions de démarrage pour le plan de création de scripts.
8. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
9. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de création de cyber-scripts échouera.
   Les valeurs minimale et maximale que vous pouvez spécifier sont respectivement une et 1 440 minutes.
10. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
    Pour plus d'informations sur cette politique, voir la documentation de Microsoft.
11. Cliquez sur **Créer**.

Créer un plan de création de scripts dans l'onglet Plans de création de scripts

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur **Création d'un plan**.
   Un modèle pour le plan de création de scripts s'ouvre.
3. [Facultatif] Pour sélectionner les ressources ou les groupes de terminaux auxquels appliquer le nouveau plan, cliquez sur **Ajouter des ressources**.
   a. Cliquez sur **Machines avec des agents** pour développer la liste, puis sélectionnez les ressources ou les groupes de terminaux de votre choix.
   b. Cliquez sur **Ajouter**.

© Acronis International GmbH, 2003-2026

Pour en savoir plus sur la façon de créer des groupes de terminaux au niveau du partenaire, voir "Création d'un groupe statique de terminaux au niveau du partenaire" (p. 390) et "Création d'un groupe dynamique de terminaux au niveau du partenaire" (p. 390).

Remarque
Vous pouvez aussi sélectionner des ressources ou des groupes de terminaux après avoir créé le plan.

4. [Facultatif] Pour modifier le nom du plan de création de scripts, cliquez sur l'icône en forme de crayon.
5. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.

Remarque
Vous ne pouvez utiliser que vos scripts approuvés dans **Référentiel de scripts** >**Mes scripts**. Seul un administrateur ayant le rôle de **cyberadministrateur** peut utiliser des scripts à l'état de **Test**. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

6. Configurez la planification et les conditions de démarrage pour le plan de création de scripts.
7. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
8. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de création de cyber-scripts échouera.
   Les valeurs minimale et maximale que vous pouvez spécifier sont respectivement une et 1 440 minutes.
9. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
   Pour plus d'informations sur cette politique, voir la documentation de Microsoft.
10. Cliquez sur **Créer**.

Planification et conditions de démarrage

Planification

Vous pouvez configurer un plan de création de scripts pour qu'il soit exécuté une seule fois ou de façon répétée, et pour qu'il démarre en fonction d'une planification ou qu'il soit déclenché par un certain événement.

Les options suivantes sont disponibles :

© Acronis International GmbH, 2003-2026

- Ex. une fois

  Pour cette option, vous devez configurer la date et l'heure d'exécution du plan.
- Planifier selon l'horaire

  Avec cette option, vous pouvez configurer des plans de création de scripts qui s'exécutent toutes les heures, tous les jours ou tous les mois.

  Pour que la planification ne soit effective que temporairement, cochez la case **Exécuter sur une plage de dates**, puis configurez la période pendant laquelle le plan planifié sera exécuté.
- Lorsque l'utilisateur se connecte au système

  Vous pouvez choisir si un utilisateur spécifique ou n'importe quel utilisateur qui se connecte déclenche le plan de création de scripts.
- Lorsqu'un utilisateur se déconnecte du système

  Vous pouvez choisir si un utilisateur spécifique ou n'importe quel utilisateur qui se déconnecte déclenche le plan de création de scripts.
- Au démarrage du système
- Lorsque le système est arrêté

  Remarque
  Cette option de planification ne fonctionne qu'avec les scripts qui s'exécutent dans le compte système.
- Lorsque le système est en ligne

Conditions de démarrage

Les conditions de démarrage ajoutent plus de flexibilité à vos plans planifiés. Si vous configurez plusieurs conditions, toutes devront être remplies simultanément pour que le plan puisse démarrer.

Les conditions de démarrage ne sont pas effectives si vous exécutez le plan manuellement à l'aide de l'option **Exécuter maintenant**.

Condition	Description
Exécuter uniquement si la ressource est en ligne	Cette condition est remplie lorsque la ressource cible est connectée à Internet.
L'utilisateur est inactif	Cette condition est remplie lorsqu'un écran de veille s'exécute sur l'ordinateur ou si l'ordinateur est verrouillé.
Utilisateur déconnecté	Si vous sélectionnez cette condition, vous pouvez reporter un plan planifié jusqu'à ce que l'utilisateur de la ressource cible se déconnecte.
Compris dans un intervalle de temps	Si vous sélectionnez cette condition, vous devez définir l'intervalle de temps pendant lequel le plan peut s'exécuter.

© Acronis International GmbH, 2003-2026

Condition	Description
Économiser de la batterie	Si vous sélectionnez cette condition, vous pouvez vous assurer que le plan ne sera pas interrompu en raison d'une batterie faible. Les options suivantes sont disponibles : • **Ne pas démarrer lors d'une alimentation sur batterie** Le plan démarrera uniquement si l'ordinateur est connecté à une source d'alimentation. • **Démarrer pendant l'alimentation sur batterie si le niveau de batterie est supérieur à** Le plan démarrera si l'ordinateur est connecté à une source d'alimentation ou si le niveau de batterie est supérieur à la valeur spécifiée.
Ne pas démarrer pendant une connexion mesurée	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si la ressource cible accède à Internet via une connexion mesurée.
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si la ressource cible est connectée à l'un des réseaux sans fil spécifiés. Pour utiliser cette condition, vous devez indiquer le SSID du réseau interdit. La restriction s'applique à tous les réseaux qui contiennent le nom spécifié comme sous-chaîne dans leur nom, quelle que soit la casse. Par exemple, si vous spécifiez `téléphone` comme nom de réseau, le plan ne démarrera pas lorsque le terminal sera connecté à l'un des réseaux suivants : `Téléphone de Jean`, `téléphone_wifi` ou `mon_wifi_TÉLÉPHONE`.
Vérifier l'adresse IP du terminal	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si l'une des adresses IP de la ressource cible se trouve au sein ou en dehors de la plage d'adresses IP spécifiée. Les options suivantes sont disponibles : • **Démarrer si en dehors de la plage d'adresses IP** • **Démarrer si dans la plage d'adresses IP** Prend en charge uniquement les adresses IPv4.
Si les conditions de démarrage ne sont pas remplies, exécuter quand même la tâche	Utilisez cette option pour définir l'intervalle de temps après lequel le plan sera exécuté, quelles que soient les autres conditions. Le plan démarrera dès que les autres conditions seront remplies ou dès que la période spécifiée sera écoulée. Cette option n'est pas disponible si vous avez sélectionné l'option **Exécuter une fois** pour la planification.

Gestion des ressources cibles pour un plan

Vous pouvez sélectionner les ressources ou les groupes de terminaux auxquels vous souhaitez appliquer un plan de création de scripts au moment de la création du plan, ou ultérieurement.

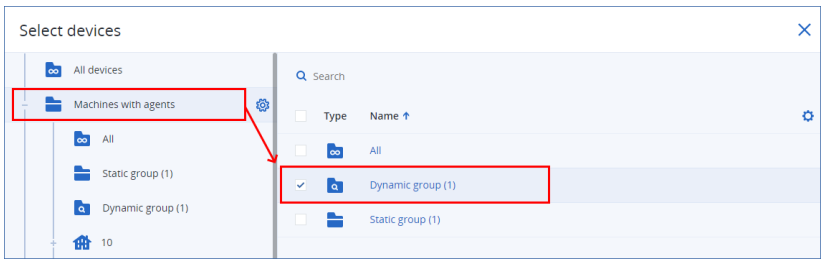
© Acronis International GmbH, 2003-2026

Les administrateurs partenaires peuvent appliquer le même plan à des ressources de différents clients, et peuvent créer des groupes de terminaux contenant des ressources de différents clients. Pour savoir comment créer un groupe de terminaux au niveau du partenaire, voir "Création d'un groupe statique de terminaux au niveau du partenaire" (p. 390) et "Création d'un groupe dynamique de terminaux au niveau du partenaire" (p. 390).

Ajouter des ressources initiales à un plan

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur le nom du plan pour lequel vous souhaitez spécifier des ressources cibles.
3. Cliquez sur **Ajouter des ressources**.
4. Sélectionnez les ressources ou les groupes de terminaux souhaités, puis cliquez sur **Ajouter**.

Remarque
Pour sélectionner un groupe de terminaux, cliquez sur son niveau parent, puis, dans le volet principal, cochez la case à côté de son nom.



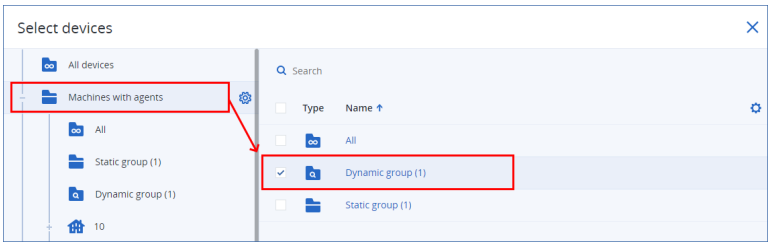
5. Pour enregistrer le plan modifié, cliquez sur **Enregistrer**.

Gérer les ressources existantes pour un plan

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur le nom du plan dont vous souhaitez modifier les ressources cibles.
3. Cliquez sur **Gérer les ressources**.
   L'écran **Terminaux** répertorie les ressources auxquelles le plan de création de scripts est actuellement appliqué. Si vous gérez plusieurs tenants, les ressources sont classées par tenant.
   - Pour ajouter de nouvelles ressources ou de nouveaux groupes de terminaux, cliquez sur **Ajouter**.
     a. Sélectionnez les ressources ou les groupes de terminaux souhaités. Vous pouvez ajouter des ressources à partir de tous les tenants que vous gérez.

© Acronis International GmbH, 2003-2026

Remarque
Pour sélectionner un groupe de terminaux, cliquez sur son niveau parent, puis, dans le volet principal, cochez la case à côté de son nom.



b. Cliquez sur **Ajouter**.

- Pour supprimer des ressources ou des groupes de terminaux, sélectionnez-les, puis cliquez sur **Supprimer**.

4. Cliquez sur **Terminé**.
5. Pour enregistrer le plan modifié, cliquez sur **Enregistrer**.

Importation de plans de création de scripts

Vous pouvez importer des plans de création de scripts qui ont été exportés dans un fichier JSON. Vous pouvez ainsi gagner du temps et garantir la cohérence des paramètres entre les tenants.

Prérequis

Un fichier JSON avec la configuration du plan est disponible sur l'ordinateur à partir duquel vous êtes connecté à la console.

Pour importer un plan de création de script

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de création de scripts**.
2. Cliquez sur **Importer**.
3. Dans la fenêtre qui s'ouvre, parcourez jusqu'au fichier JSON.
4. Cliquez sur le fichier, puis cliquez sur **Ouvrir**.
   Le plan de création script apparaît à l'écran. Vous pouvez maintenant l'appliquer aux ressources.

Exécution rapide du script

Vous pouvez exécuter un script immédiatement, sans l'inclure dans un plan de script. Vous ne pouvez pas utiliser cette opération sur plus de 150 ressources, sur des ressources hors ligne ou dans des groupes de terminaux.

La ressource cible doit se voir affecter un quota de service qui prend en charge la fonctionnalité Exécution rapide du script, et la licence RMM (modèle de licence basé sur le service) ou la licence Sécurité et RMM (modèle de licence basé sur la solution) doit être activée pour son tenant. Un quota de service approprié sera automatiquement affecté s'il est disponible dans le tenant.

© Acronis International GmbH, 2003-2026

Remarque
Vous ne pouvez utiliser que vos scripts approuvés dans **Référentiel de scripts** >**Mes scripts**. Seul un administrateur ayant le rôle de **cyberadministrateur** peut utiliser des scripts à l'état de **Test**. Pour plus d'informations sur les rôles, voir "Rôles d'utilisateur et droits de création de cyber-scripts" (p. 491).

Vous pouvez lancer une exécution rapide de l'une des manières suivantes :

- Depuis l'onglet **Terminaux**
  Sélectionnez une ou plusieurs ressources, puis sélectionnez les scripts à exécuter sur cette ou ces dernières.
- Depuis l'onglet **Gestion** > **Référentiel de création de scripts**
  Sélectionnez un script, puis sélectionnez une ou plusieurs ressources cibles.

Exécuter un script depuis l'onglet Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez la ressource sur laquelle vous souhaitez exécuter le script, puis cliquez sur **Protection**.
3. Cliquez sur **Exécution rapide du script**.
4. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.
5. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
6. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de cyber-script échouera.
   Vous pouvez utiliser des valeurs comprises entre 1 et 1 440 minutes.
7. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
   Pour plus d'informations sur cette politique, voir la documentation de Microsoft.
8. Cliquez sur **Exécuter maintenant**.

Exécuter un script depuis l'onglet Référentiel de création de scripts

1. Dans la console Cyber Protect, accédez à **Gestion** > **Référentiel de création de scripts**.
2. Sélectionnez le script que vous souhaitez exécuter, puis cliquez sur **Exécution rapide du script**.
3. Cliquez sur **Ajouter des ressources** pour sélectionner les ressources cibles, puis cliquez sur **Ajouter**.
4. Cliquez sur **Choisir le script**, sélectionnez le script que vous souhaitez utiliser, puis cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

5. Choisissez le compte dans le cadre duquel le script s'exécutera sur la ressource cible. Les options suivantes sont disponibles :
   - Compte système (sous macOS, il s'agit du compte racine)
   - Compte actuellement connecté
6. Spécifiez la durée pendant laquelle le script peut s'exécuter sur la ressource cible.
   Si l'exécution du script ne peut se terminer dans le délai défini, l'opération de cyber-script échouera.
   Vous pouvez utiliser des valeurs comprises entre 1 et 1 440 minutes.
7. [Uniquement pour les scripts PowerShell] Configurez la règle d'exécution PowerShell.
   Pour plus d'informations sur cette politique, voir la documentation de Microsoft.
8. Cliquez sur **Exécuter maintenant**.

© Acronis International GmbH, 2003-2026

Gestion de la sauvegarde et de la restauration des ressources et fichiers

Le module de sauvegarde permet la sauvegarde et la restauration de machines physiques et virtuelles, de fichiers et de bases de données vers un système de stockage local ou dans le Cloud.

Systèmes d'exploitation et environnements pris en charge pour la sauvegarde et la restauration

Les informations ci-dessous s'appliquent à la sauvegarde et à la restauration. Pour plus de détails sur les fonctionnalités de protection prises en charge par le système d'exploitation, voir "Fonctionnalités de protection prises en charge par système d'exploitation" (p. 27).

Agent pour Windows

Le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

Cet agent inclut un composant pour la protection antivirus et antimalware et le filtrage d'URL qui prend en charge un ensemble de systèmes d'exploitation différents. Voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Remarque
La liste des systèmes d'exploitation pris en charge ci-dessous s'applique à la sauvegarde et à la restauration.

- Windows 10 versions 1809 et ultérieures : éditions Famille, Professionnel, Éducation, Entreprise, IoT Entreprise et LTSC (anciennement LTSB)
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server
- Windows Server 2025 – toutes les options d'installation, sauf Nano Server

© Acronis International GmbH, 2003-2026

Important
Avant de mettre à niveau le système d'exploitation d'une ressource protégée sur laquelle un agent de protection ou le serveur de gestion est installé, notez les points suivants :

- Dans le cas d'une mise à niveau majeure (par exemple, de Windows 7 à Windows 10), vous devez réinstaller l'agent ou le serveur de gestion après la mise à niveau pour garantir leur bon fonctionnement.
- Dans le cas d'une mise à jour mineure au sein d'une version majeure (par exemple, de Windows 10 version 20H2 à Windows 10 version 21H1), il n'est pas nécessaire de réinstaller l'agent après la mise à jour du système d'exploitation.

Agent pour Windows (hérité)

Cet agent inclut un composant pour la protection antivirus et antimalware et le filtrage d'URL qui prend en charge un ensemble de systèmes d'exploitation différents. Voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Remarque
La liste des systèmes d'exploitation pris en charge ci-dessous s'applique à la sauvegarde et à la restauration.

- Windows XP Professionnel SP1 (x64), SP2 (x64), SP3 (x86)

  Remarque
  Sur les systèmes Windows XP, l'Agent pour Windows prend uniquement en charge les lecteurs au format NTFS.

- Windows Server 2003 SP1/2003 R2 et versions ultérieures – éditions Standard et Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* – éditions Standard, Enterprise, Datacenter, Foundation et Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 - toutes les éditions

© Acronis International GmbH, 2003-2026

Remarque

Pour utiliser Cyber Protection avec Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft avant d'installer l'agent de protection :

- Mises à jour de sécurité étendues (ESU) pour Windows 7
- KB4474419
- KB4490628

Pour plus d'informations sur les mises à jour requises, voir cet article de la base de connaissances.

- Windows Server 2008 R2* – éditions Standard, Enterprise, Datacenter, Foundation et Web
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – toutes les éditions
- Windows 8/8.1 – toutes les éditions (x86, x64), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 versions 1803 et antérieures : éditions Famille, Professionnel, Éducation, Entreprise, IoT Entreprise et LTSC (anciennement LTSB)
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server

Remarque

* Pour utiliser Cyber Protection avec cette version de Windows, vous devez installer la mise à jour du support de signature de code SHA2 de Microsoft (article KB4474419) avant d'installer l'agent de protection.

Pour plus d'informations sur les problèmes liés à la mise à jour de la prise en charge de la signature de code SHA2, reportez-vous à cet article de la base de connaissances.

Important

Avant de mettre à niveau le système d'exploitation d'une ressource protégée sur laquelle un agent de protection ou le serveur de gestion est installé, notez les points suivants :

- Dans le cas d'une mise à niveau majeure (par exemple, de Windows 7 à Windows 10), vous devez réinstaller l'agent ou le serveur de gestion après la mise à niveau pour garantir leur bon fonctionnement.
- Dans le cas d'une mise à jour mineure au sein d'une version majeure (par exemple, de Windows 10 version 20H2 à Windows 10 version 21H1), il n'est pas nécessaire de réinstaller l'agent après la mise à jour du système d'exploitation.

© Acronis International GmbH, 2003-2026

Agent pour SQL, agent pour Active Directory, agent pour Exchange (pour la sauvegarde de bases de données et la sauvegarde reconnaissant les applications)

Ces agents sont fournis avec l'agent pour Windows et l'agent pour Windows (hérité). Avec l'agent pour Windows, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

Chacun de ces agents est pris en charge sur les mêmes versions de Windows que l'agent pour Windows et l'agent pour Windows (hérité), et peut être installé sur un ordinateur exécutant une version prise en charge de l'application concernée, à l'exception suivante :

- Windows Server 2025 n'est pas pris en charge.

Agent pour empêcher les pertes de données

Cet agent est fourni avec l'agent pour Windows et l'agent pour Windows (hérité). Avec l'agent pour Windows, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

Contrôle des terminaux

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 – Windows Server 2022
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)

Remarque
Agent for Data Loss Prevention pour macOS ne prend en charge que les processeurs x64. Les processeurs Apple Silicon ARM ne sont pas supportés.

Prévention des pertes de données

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 – Windows Server 2022

© Acronis International GmbH, 2003-2026

Remarque
Agent for Data Loss Prevention peut être installé sur des systèmes macOS non pris en charge, car il fait partie intégrante d'Agent for Mac. Dans ce cas, la console Cyber Protect indiquera que Agent for Data Loss Prevention est installé sur l'ordinateur, mais les fonctionnalités de contrôle des terminaux et de prévention des pertes de données ne fonctionneront pas. La fonctionnalité de contrôle des terminaux ne fonctionnera que sur les systèmes macOS supporté par Agent for Data Loss Prevention.

Agent pour File Sync & Share

Cet agent est fourni dans le cadre de l'agent pour Windows et de l'agent pour Windows (hérité).

Agent pour File Sync & Share prend en charge un ensemble de systèmes d'exploitation différent de Agent pour Windows et Agent pour Windows (Legacy).

Pour vérifier les systèmes d'exploitation pris en charge par Agent pour File Sync & Share, voir la documentation de Cloud Cyber Files.

Agent pour Exchange (pour la sauvegarde de boîte aux lettres)

Cet agent est fourni avec l'agent pour Windows et l'agent pour Windows (hérité). Avec l'agent pour Windows, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

- Windows Server 2008 – éditions Standard, Enterprise, Datacenter, Foundation et Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 - toutes les éditions
- Windows Server 2008 R2 - éditions Standard, Enterprise, Datacenter, Foundation et Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – toutes les éditions
- Windows 8/8.1 – toutes les éditions (x86, x64), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – éditions Famille, Professionnel, Éducation et Entreprise
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

© Acronis International GmbH, 2003-2026

Agent pour Microsoft 365

Cet agent est fourni avec l'agent pour Windows et l'agent pour Windows (hérité). Avec l'agent pour Windows, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

- Windows Server 2008 – éditions Standard, Enterprise, Datacenter, Foundation et Web (x64 uniquement)
- Windows Small Business Server 2008
- Windows Server 2008 R2 - éditions Standard, Enterprise, Datacenter, Foundation et Web
- Windows Home Server 2011
- Windows Small Business Server 2011 – toutes les éditions
- Windows 8/8.1 – toutes les éditions (x64 uniquement), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2008/2008 R2/2012/2012R2/2016 (x64 uniquement)
- Windows 10 – éditions Famille, Professionnel, Éducation et Entreprise (x64 uniquement)
- Windows Server 2016 – toutes les options d'installation (x64 uniquement), sauf Nano Server
- Windows Server 2019 – toutes les options d'installation (x64 uniquement), sauf Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

Agent pour Oracle

Cet agent est fourni avec l'agent pour Windows, l'agent pour Windows (hérité) et l'agent pour Linux (64 bits). Avec l'agent pour Windows et l'agent pour Linux, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits.

- Windows Server 2008R2 – éditions Standard, Enterprise, Datacenter et Web (x86, x64)
- Windows Server 2012R2 – éditions Standard, Enterprise, Datacenter et Web (x86, x64)
- Linux – tout noyau ou distribution pris en charge par un agent pour Linux (répertorié ci-dessous)

Agent pour MySQL/MariaDB

Cet agent est fourni avec l'agent pour Linux (64 bits).

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

- Linux – tout noyau ou distribution pris en charge par un agent pour Linux (répertorié ci-dessous)

Agent pour Linux

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

© Acronis International GmbH, 2003-2026

Cet agent inclut un composant pour la protection antivirus et antimalware et le filtrage d'URL qui prend en charge un ensemble de systèmes d'exploitation différents. Voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Remarque
La liste des systèmes d'exploitation pris en charge ci-dessous s'applique à la sauvegarde et à la restauration.

Cyber Protect Cloud prend en charge les distributions Linux x86 et x86_64 qui utilisent les composants suivants :

- Version du noyau de 2.6.9 à 6.15
  Les versions de noyau prises en charge sont répertoriées en fonction des versions sur www.kernel.org. Certaines distributions, telles que Red Hat Enterprise Linux, rétroportent de nouvelles fonctionnalités sur d'anciennes versions du noyau. Ces noyaux propres à la distribution pourraient ne pas être pris en charge, même si leur version se trouve dans la plage prise en charge.
- La bibliothèque C GNU (glibc) 2.3.4 ou version ultérieure

Les distributions suivantes ont été testées spécifiquement. Cependant, même si votre distribution Linux ou votre version de noyau ne figure pas dans la liste ci-dessous, elle pourrait fonctionner correctement dans tous les scénarios requis en raison des spécificités des systèmes d'exploitation Linux. Si vous rencontrez des problèmes lors de l'utilisation de Cyber Protect Cloud avec votre combinaison de distribution et de version de noyau, contactez l'équipe d'assistance pour qu'elle effectue une enquête plus approfondie.

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*, 10*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04, 23.10, 24.04, 24.10, 25.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38, 39, 40, 41, 42

  Important
  Les configurations avec Btrfs ne sont pas prises en charge. Pour plus d'informations, voir "Systèmes de fichiers pris en charge" (p. 539).

- SUSE Linux Enterprise Server 10, 11, 12, 15

  Important
  Les configurations avec Btrfs ne sont pas prises en charge. Pour plus d'informations, voir "Systèmes de fichiers pris en charge" (p. 539).

© Acronis International GmbH, 2003-2026

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11, 12, 13
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*, 10*
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6* – noyau Unbreakable Enterprise et noyau compatible Red Hat

Remarque
Installation de l'agent de protection sur Oracle Linux 8.6 et versions ultérieures, sur lesquelles le Secure Boot est activé, nécessite la signature manuelle des modules du noyau. Pour plus d'informations sur la signature d'un module de noyau, voir cet article de la base de connaissances.

- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.4*, 9.5*, 9.6*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- Rocky Linux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- ALT Linux 7.0

* À partir de la version 8.4, prise en charge uniquement avec les noyaux 4.18 et ultérieurs.

Important
Avant de mettre à niveau le système d'exploitation d'une ressource protégée sur laquelle l'agent Cyber Protection ou un serveur de gestion est installé, notez ce qui suit.
- Dans le cas d'une mise à niveau de version majeure, vous devez réinstaller l'agent ou le serveur de gestion après la mise à niveau pour garantir son bon fonctionnement.
- Avant d'installer une nouvelle version de noyau, consultez la section "Agent pour Linux" (p. 518) pour vérifier que la version est prise en charge.

Agent pour Mac

Cet agent inclut un composant pour la protection antivirus et antimalware et le filtrage d'URL qui prend en charge un ensemble de systèmes d'exploitation différents. Voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Remarque
La liste des systèmes d'exploitation pris en charge ci-dessous s'applique à la sauvegarde et à la restauration.

Les architectures x64 et ARM (utilisées dans les processeurs Apple Silicon Apple M1, M2 et ultérieurs) sont toutes deux prises en charge.

© Acronis International GmbH, 2003-2026

Remarque
Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14
- macOS Sequoia 15
- macOS Tahoe 26

Remarque
L'agent prend également en charge toutes les versions mineures des systèmes d'exploitation énumérés ci-dessus. Par exemple, macOS Sonoma 14.5.

Important
À partir de la version C23.07, Cyber Protect Cloud ne prend pas en charge les systèmes d'exploitation suivants : OS X Yosemite 10.10, OS X El Capitan 10.11 et macOS Sierra 10.12.

Cyber Protect Monitor ne prend pas en charge les versions macOS 10.x et 11.x.

Nous vous recommandons vivement d'effectuer la mise à niveau de votre système d'exploitation vers une version prise en charge afin de garantir la compatibilité et de pouvoir utiliser toutes les fonctionnalités de Cyber Protect Cloud.

Agent pour VMware (appliance virtuelle)

Cet agent est fourni en tant qu'appliance virtuelle qui s'exécute sur un hôte ESXi.

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

En mode compatible FIPS, seul VMware ESXi 8.0 est pris en charge.

Agent pour VMware (Windows)

Cet agent est fourni avec l'agent pour Windows et l'agent pour Windows (hérité). Avec l'agent pour Windows, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

© Acronis International GmbH, 2003-2026

Cet agent est pris en charge sur les mêmes versions de Windows que l'agent pour Windows et l'agent pour Windows (hérité), avec les limitations suivantes :

- Les systèmes d'exploitation 32 bits ne sont pas pris en charge.
- Windows XP, Windows Server 2003/2003 R2 et Windows Small Business Server 2003/2003 R2 ne sont pas pris en charge.
- En mode compatible FIPS, seul VMware ESXi 8.0 est pris en charge.

Agent pour Hyper-V

Cet agent est fourni avec l'agent pour Windows et l'agent pour Windows (hérité). Avec l'agent pour Windows, le mode compatible FIPS est pris en charge sur les systèmes d'exploitation 64 bits. Voir "Mode compatible FIPS" (p. 59).

- Windows Server 2008 (x64 uniquement) avec rôle Hyper-V, y compris le mode d'installation de Server Core
- Windows Server 2008 R2 avec rôle Hyper-V, y compris le mode d'installation de Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 avec rôle Hyper-V, y compris le mode d'installation de Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (x64 uniquement) avec Hyper-V
- Windows 10 – éditions Familiale, Pro, Education et Enterprise avec Hyper-V
- Windows 11 – éditions Familiale, Pro, Education et Enterprise avec Hyper-V
- Rôle de Windows Server 2016 avec Hyper-V – toutes les options d'installation, sauf Nano Server
- Microsoft Hyper-V Server 2016
- Rôle de Windows Server 2019 avec Hyper-V – toutes les options d'installation, sauf Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server
- Windows Server 2025 – toutes les options d'installation, sauf Nano Server

Agent pour Virtuozzo

Cet agent est fourni avec l'agent pour Linux (64 bits).

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

© Acronis International GmbH, 2003-2026

Agent pour Virtuozzo Hybrid Infrastructure

Cet agent est fourni sous forme d'appliance virtuelle qui s'exécute sur un hôte Virtuozzo Hybrid Infrastructure.

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2, 6.3

Agent pour Scale Computing HC3

Cet agent est fourni sous forme d'appliance virtuelle qui s'exécute sur un hôte Scale Computing HC3.

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

Scale Computing HyperCore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4

Agent pour oVirt

Cet agent est fourni sous la forme d'une appliance virtuelle qui s'exécute sur un hôte hyperviseur KVM géré par oVirt.

Le mode compatible FIPS est pris en charge. Voir "Mode compatible FIPS" (p. 59).

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent pour Synology

Cet agent est fourni sous forme d'appliance virtuelle qui s'exécute sur un NAS Synology.

DiskStation Manager 6.2.x, 7.x

L'agent pour Synology ne prend en charge que les NAS dotés de processeurs x86_64. Les processeurs ARM ne sont pas pris en charge. Voir le centre de connaissances Synology.

Agent pour Azure

Cet agent est fourni sous forme d'appliance virtuelle qui s'exécute dans votre abonnement Microsoft Azure.

Agent pour Nutanix

Cet agent est fourni sous forme d'appliance virtuelle qui s'exécute dans un cluster Nutanix AHV.

Système d'exploitation Nutanix Acropolis (AOS) 6.5, 6.6, 6.7, 6.8, 6.10

© Acronis International GmbH, 2003-2026

Cyber Protect Monitor

- Avec l'agent pour Windows
  - Windows 10 version 1809 et ultérieure
  - Windows Server 2019 et versions ultérieures
- Avec l'agent pour Windows (hérité)
  - Windows 7 et versions ultérieures
  - Windows Server 2008 R2 et versions ultérieures
- Avec Agent pour Mac
  - Toutes les versions de macOS prises en charge par l'Agent pour Mac, à l'exception de macOS 10.x et macOS 11.x.

Versions de Microsoft SQL Server prises en charge

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Les éditions SQL Server Express des versions de serveur SQL susmentionnées sont également prises en charge.

Remarque
La sauvegarde de Microsoft SQL n'est prise en charge que pour les bases de données fonctionnant sur les systèmes de fichiers NFTS, REFS et FAT32. ExFat n'est pas pris en charge.

Versions Microsoft Exchange Server compatibles

- Microsoft Exchange Server Subscription Edition (SE)
- Microsoft Exchange Server 2019 – toutes les éditions.
- Microsoft Exchange Server 2016 – toutes les éditions.
- Microsoft Exchange Server 2013 – toutes les éditions, mise à jour cumulative 1 (CU1) et ultérieures.

© Acronis International GmbH, 2003-2026

- Microsoft Exchange Server 2010 – toutes les éditions, tous les service packs. La sauvegarde et restauration granulaire pour boîte aux lettres depuis les sauvegardes de base de données sont prises en charge par le Service Pack 1 (SP1).
- Microsoft Exchange Server 2007 – toutes les éditions, tous les service packs. La sauvegarde et restauration granulaire pour boîte aux lettres depuis les sauvegardes de base de données ne sont pas prises en charge.

Versions de Microsoft SharePoint prises en charge

Cyber Protection prend en charge les versions de Microsoft SharePoint suivantes :

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

* Pour pouvoir utiliser SharePoint Explorer avec ces versions, il est nécessaire d'avoir une batterie de restauration SharePoint à laquelle joindre les bases de données.

Les sauvegardes ou bases de données à partir desquelles vous extrayez des données doivent provenir de la même version de SharePoint que celle sur laquelle SharePoint Explorer est installé.

Versions Oracle Database prises en charge

- Oracle Database version 11g, toutes éditions
- Oracle Database version 12c, toutes éditions
- Oracle Database version 19c, toutes éditions
- Oracle Database version 21c, toutes éditions

Prise en charge des configurations à instance unique seulement.

Versions SAP HANA prises en charge

- HANA 2.0 SPS 03 installé sur RHEL 7.6 en cours d'exécution sur une machine physique ou une machine virtuelle VMware ESXi.
- HANA 2.0 SPS 03 installé dans SUSE 15 avec le système de fichiers XFS.

SAP HANA ne prend pas en charge la restauration de conteneurs de bases de données multi-tenants à l'aide d'instantanés de stockage. Par conséquent, cette solution prend en charge les conteneurs SAP HANA avec une base de données tenant uniquement.

© Acronis International GmbH, 2003-2026

Versions de MySQL prises en charge

- 5.5.x − Éditions Community Server, Enterprise, Standard et Classic
- 5.6.x − Éditions Community Server, Enterprise, Standard et Classic
- 5.7.x − Éditions Community Server, Enterprise, Standard et Classic
- 8.0.x − Éditions Community Server, Enterprise, Standard et Classic

Versions de MariaDB prises en charge

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

Plates-formes de virtualisation prises en charge

Le tableau suivant récapitule la prise en charge de diverses plates-formes de virtualisation.

Pour plus d'informations sur les différences entre les sauvegardes avec et sans agent, voir "Sauvegarde avec et sans agent" (p. 40).

Remarque
Si vous utilisez une plateforme ou une version de virtualisation qui n'est pas répertoriée ci-dessous, la méthode de **sauvegarde basée sur l'agent (sauvegarde à partir d'un système d'exploitation invité)** devrait toujours fonctionner correctement dans tous les scénarios requis. Si vous rencontrez des problèmes avec la sauvegarde basée sur l'agent, contactez l'équipe de support pour plus d'informations.

VMware (Broadcom)

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Versions VMware vSphere : 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **Éditions VMware vSphere :**	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Broadcom**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** >

© Acronis International GmbH, 2003-2026

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	**(VMware) ESXi** > **Agent pour l'installation dans Windows** ou **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Broadcom (VMware) ESXi** > **Appliance virtuelle (OVF)**	**Windows** ou **Linux**
VMware vSphere Hypervisor (ESXi gratuit)**	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Serveur VMware (serveur virtuel VMware) VMware Workstation VMware ACE VMware Player	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

* Dans le cas de ces éditions, le transport HotAdd pour disques virtuels est pris en charge sur vSphere 5.0 et versions ultérieures. Sur la version 4.1, il est possible que les sauvegardes soient plus lentes.

** La sauvegarde à un niveau hyperviseur n'est pas prise en charge pour vSphere Hypervisor parce que ce produit limite l'accès à l'interface de Ligne de Commande à distance (RCLI) au mode lecture seule. L'agent fonctionne pendant la période d'évaluation de l'hyperviseur vSphere tant qu'une clé de série n'est pas saisie. Une fois que vous avez saisi une clé de série, l'agent s'arrête de fonctionner.

Remarque
Cyber Protect Cloud prend officiellement en charge toute mise à jour d'une version majeure de vSphere prise en charge.

Par exemple, la prise en charge de vSphere 8.0 inclut la prise en charge de toute mise à jour de cette version, sauf indication contraire. Autrement dit, vSphere 8.0 Update 1 est également prise en charge, au même titre que la version initiale de vSphere 8.0.

La prise en charge d'une version spécifique de VMware vSphere signifie que vSAN de la version correspondante est également pris en charge. Par exemple, la prise en charge de vSphere 8.0 signifie que vSAN 8.0 est également pris en charge.

© Acronis International GmbH, 2003-2026

Limites

- **Machines tolérantes aux pannes**
  L'agent Pour VMware sauvegarde les machines tolérantes aux pannes uniquement si cette tolérance a été activée sur VMware vSphere 6.0 et versions ultérieures. Si vous avez effectué une mise à niveau à partir d'une ancienne version de vSphere, il vous suffit de désactiver puis d'activer la tolérance aux pannes sur chaque machine. Si vous utilisez une version antérieure de vSphere, installez un agent sur le système d'exploitation invité.
- **Disques et RDM indépendants**
  L'agent pour VMware ne sauvegarde pas les disques mappage de terminal brut (RDM) en mode de compatibilité physique ni les disques indépendants. L'agent ignore ces disques et ajoute des avertissements au journal. Vous pouvez éviter les avertissements en excluant des disques et RDM indépendants en mode de compatibilité physique à partir du plan de protection. Si vous voulez sauvegarder ces disques ou données, installez un agent sur le système d'exploitation invité.
- **Connexion iSCSI en tant qu'invité**
  L'agent pour VMware ne sauvegarde pas les volumes LUN connectés par un initiateur iSCSI qui fonctionne sous le système d'exploitation invité. Étant donné que l'hyperviseur ESXi n'a pas connaissance de ces volumes, ces derniers ne sont pas inclus dans les instantanés au niveau de l'hyperviseur et sont omis d'une sauvegarde sans avertissement. Si vous souhaitez sauvegarder ces volumes ou ces données sur ces volumes, installez un agent sur le système d'exploitation invité.
- **Machines virtuelles chiffrées** (introduites dans VMware vSphere 6.5)
  - Les machines virtuelles sont sauvegardées à l'état chiffré. Si le chiffrement est essentiel pour vous, activez le chiffrement des sauvegardes lors de la création d'un plan de protection.
  - Les machines virtuelles restaurées sont toujours chiffrées. Une fois la restauration terminée, vous pouvez activer le chiffrement manuellement.
  - Si vous sauvegardez des machines virtuelles chiffrées, nous vous recommandons de chiffrer également la machine virtuelle sur laquelle l'agent pour VMware est exécuté. Dans le cas contraire, les opérations des machines chiffrées risquent d'être plus lentes que prévu. Appliquez la **politique de chiffrement VM** à la machine de l'agent à l'aide du client vSphere Web.
  - Les machines virtuelles chiffrées sont sauvegardées via LAN, même si vous configurez le mode de transport SAN pour l'agent. L'agent revient au transport NBD, car VMware ne prend pas en charge le transport SAN pour la sauvegarde de disques virtuels chiffrés.
- **Secure Boot**
  - Machines virtuelles VMware : (introduites dans VMware vSphere 6.5) **Secure Boot** est désactivé dès qu'une machine virtuelle est restaurée en tant que nouvelle machine virtuelle. Une fois la restauration terminée, vous pouvez activer cette option manuellement. Cette restriction s'applique à VMware.
  - Machines virtuelles Hyper-V : pour toutes les machines virtuelles de génération 2, le démarrage sécurisé est désactivé après la restauration dans une autre machine virtuelle, nouvelle ou existante.

© Acronis International GmbH, 2003-2026

- La **sauvegarde de la configuration ESXi** n'est pas prise en charge pour VMware vSphere 7.0 et les versions ultérieures.
- **Les machines virtuelles dont l'UUID d'instance est vide n'apparaissent pas dans la console Cyber Protect.**

  Les machines virtuelles VMware dont la propriété vSphere `Instance UUID` (`vc.uuid`) est vide ne sont pas répertoriées dans la console Cyber Protect. Pour plus d'informations sur la résolution de ce problème, consultez cet article de la base de connaissances.
- **Paramètres réseau de l'agent de protection**

  La sauvegarde d'une machine virtuelle VMware peut échouer si l'agent de protection ne peut pas déduire en adresse IP le nom de l'hôte ESXi enregistré dans vCenter, même si le nom de l'hôte vCenter peut être déduit. L'erreur suivante s'affiche : « Vous n'avez pas de droits d'accès à ce fichier ».

  Pour résoudre le problème, modifiez les paramètres réseau de l'agent de protection en configurant le DNS ou en modifiant le fichier `/etc/hosts`. Pour vérifier la solution, exécutez la commande suivante sur l'ordinateur où se trouve l'agent de protection :

  ```
  ping <ESXi host name>
  ```
- **Opérations prises en charge pour les ordinateurs dotés de volumes logiques**

  La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Clouds publics

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Amazon EC2 Instances	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Microsoft Azure machines virtuelles	Pris en charge **Terminaux** > **Ajouter** > **Machines virtuelles Microsoft Azure**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Microsoft

Hyper-V machines virtuelles fonctionnant sur un cluster hyperconvergé avec Storage Spaces Direct (S2D) sont prises en charge. Storage Spaces Direct est également pris en charge en tant que

© Acronis International GmbH, 2003-2026

stockage de sauvegarde.

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Windows Server 2008 (x64) avec Hyper-V Windows Server 2008 R2 avec Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 avec Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) avec Hyper-V Windows 10 avec Hyper-V Windows 11 avec Hyper-V Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server Windows Server 2025 avec Hyper-V – toutes les options d'installation, excepté Nano Server	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Microsoft Hyper-V**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** >

© Acronis International GmbH, 2003-2026

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
		Windows ou **Linux**
Microsoft Virtual Server 2005	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Remarque
Les machines virtuelles Hyper-V en cours d'exécution sur un cluster hyperconvergent avec espaces de stockage directs (S2D) sont prises en charge. Les Espaces de Stockage Directs sont également pris en charge en tant que stockage des sauvegardes.

Limites

- **Disques pass-through**
  L'agent pour Hyper-V ne sauvegarde pas les disques pass-through. Pendant la sauvegarde, l'agent ignore ces disques et ajoute des avertissements au journal. Vous pouvez éviter les avertissements en excluant des disques pass-through du plan de protection. Si vous voulez sauvegarder ces disques ou données, installez un agent sur le système d'exploitation invité.
- **Mise en cluster invité Hyper-V**
  Agent pour Hyper-V ne prend pas en charge la sauvegarde des machines virtuelles Hyper-V qui constituent des nœuds d'un cluster de basculement Windows Server. Un instantané VSS au niveau hôte peut même temporairement déconnecter le disque quorum externe du cluster. Si vous voulez sauvegarder ces machines, installez les agents dans les systèmes d'exploitation invités.
- **Connexion iSCSI en tant qu'invité**
  L'agent pour Hyper-V ne sauvegarde pas les volumes LUN connectés par un initiateur iSCSI qui fonctionne sous le système d'exploitation invité. Étant donné que l'hyperviseur Hyper-V n'a pas connaissance de ces volumes, ces derniers ne sont pas inclus dans les instantanés au niveau de l'hyperviseur et sont omis d'une sauvegarde sans avertissement. Si vous souhaitez sauvegarder ces volumes ou ces données sur ces volumes, installez un agent sur le système d'exploitation invité.
- **Dépendance à l'égard du sous-système Microsoft WMI**
  Les sauvegardes sans agent des machines virtuelles Hyper-V dépendent du sous-système Microsoft WMI, et en particulier de la classe `Msvm_VirtualSystemManagementService`. Si les requêtes WMI échouent, les sauvegardes échoueront également. Pour plus d'informations sur la classe `Msvm_VirtualSystemManagementService`, voir la documentation Microsoft.
- **Machines virtuelles avec disques PMEM**

© Acronis International GmbH, 2003-2026

La sauvegarde des machines virtuelles Hyper-V dotées de disques à mémoire persistante (PMEM) n'est pas prise en charge.

- **Restauration interplate-forme**

  Si l'agent pour Hyper-V restaure une sauvegarde créée par un autre agent, en tant que nouvelle machine virtuelle Hyper-V, la machine résultante est de génération 1.
- **Secure Boot**

  Pour garantir le démarrage des machines virtuelles Hyper-V de génération 2 qui sont restaurées, Secure Boot est désactivé. Vous pouvez le réactiver manuellement dans l'outil de gestion Hyper-V. Pour plus d'informations sur Secure Boot et les machines virtuelles de génération 2, consultez la documentation Microsoft.
- **Sauvegardes de machines virtuelles Linux cohérentes en cas de plantage**

  Les sauvegardes de machines virtuelles Linux exécutées sur un hôte Hyper-V 2019 échouent sur des instantanés cohérents en cas de plantage, en raison d'une limitation de Microsoft (impossibilité de créer des points de contrôle de production pour les machines virtuelles Linux). Pour éviter les avertissements pendant une sauvegarde, désactivez l'option de sauvegarde VSS pour les machines virtuelles dans le plan de protection.
- **Exécution d'une machine virtuelle à partir d'une sauvegarde**

  L'exécution d'une machine virtuelle à partir d'une sauvegarde sur un hôte Hyper-V échoue si la sauvegarde est située sur le même volume que le chemin d'accès sélectionné pour les disques de VM montés. Pour résoudre ce problème, sélectionnez un volume différent pour le chemin d'accès aux disques de la machine virtuelle montée. L'espace sera utilisé uniquement pour les modifications générées dans la machine virtuelle montée et n'occupera pas la totalité de la taille du disque virtuel.
- **Opérations prises en charge pour les ordinateurs dotés de volumes logiques**

  La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Scale Computing

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Scale Computing HyperCore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Scale Computing HyperCore**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

© Acronis International GmbH, 2003-2026

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Proxmox VE

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Proxmox VE 7.x, 8, and 8.1	Non pris en charge	Pris en charge uniquement pour les invités entièrement virtualisés (HVM). Les invités paravirtualisés (PV) ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Proxmox VE 8.2, 8.3, 8.4, 9.0	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Proxmox VE**	Pris en charge uniquement pour les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Citrix Hypervisor/XenServer

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Citrix Hypervisor/XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2	Non pris en charge	Pris en charge uniquement pour les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Hôtes**

© Acronis International GmbH, 2003-2026

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
		de virtualisation > **Citrix Hypervisor/XenServer** > **Windows** ou **Linux**

Red Hat et Linux

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Red Hat Virtualization (gérée par oVirt) 4.2, 4.3, 4.4, 4.5	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM)	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **KVM** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.3 exécuté sur Red Hat Enterprise Linux 7.6, 7.7 ou CentOS 7.6, 7.7	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.4 exécuté sur Red Hat Enterprise Linux 8.x ou CentOS Stream 8.x	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.5 exécuté sur Red Hat Enterprise Linux 8.x ou CentOS Stream 8.x	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Red Hat Virtualization (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

© Acronis International GmbH, 2003-2026

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Parallels

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Parallels Workstation	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Parallels Server 4 Bare Metal	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Oracle

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Oracle Linux Virtualization Manager (basé sur oVirt)* 4.3	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **LWM Oracle (oVirt)**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Non pris en charge	Pris en charge uniquement pour les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge. **Terminaux** > **Ajouter** >

© Acronis International GmbH, 2003-2026

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
		Postes de travail ou **Serveurs** > **Windows** ou **Linux**
Oracle VM VirtualBox 4.x	Non pris en charge	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

*Oracle Linux Virtualization Manager est pris en charge par Agent pour oVirt.

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Nutanix

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde basée sur un agent (Sauvegarde depuis un SE invité)
Système d'exploitation Nutanix Acropolis (AOS) 6.5, 6.6, 6.7, 6.8, 6.10	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Nutanix AHV**	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Nutanix AHV** > **Windows** ou **Linux**

Virtuozzo Hybrid Server

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Pris en charge **Terminaux** > **Ajouter** > **Hôtes**	Pris en charge pour les machines virtuelles

© Acronis International GmbH, 2003-2026

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
	de virtualisation > **Virtuozzo**	uniquement. Les conteneurs ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Virtuozzo 7.0.13, 7.0.14	Pris en charge pour les conteneurs ploop uniquement. Les machines virtuelles ne sont pas prises en charge. **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo**	Pris en charge pour les machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**
Virtuozzo Hybrid Server 7.5	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo**	Pris en charge pour les machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge. **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

Limites

Opérations prises en charge pour les ordinateurs dotés de volumes logiques

La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Virtuozzo Hybrid Infrastructure

Plate-forme	Sauvegarde sans agent (Sauvegarde au niveau de l'hyperviseur)	Sauvegarde avec agent (Sauvegarde depuis un SE invité)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2, 6.3, 7.0	Pris en charge **Terminaux** > **Ajouter** > **Hôtes de virtualisation** > **Virtuozzo Hybrid Infrastructure**	Pris en charge **Terminaux** > **Ajouter** > **Postes de travail** ou **Serveurs** > **Windows** ou **Linux**

© Acronis International GmbH, 2003-2026

Limites

- **Sauvegarde des MV sans agent avec disques sur un stockage iSCSI externe**
  Vous ne pouvez pas sauvegarder des machines virtuelles à partir de Virtuozzo Hybrid Infrastructure si les disques d'une machine virtuelle sont placés sur des volumes iSCSI externes (associés au cluster VHI).
- **Opérations prises en charge pour les ordinateurs dotés de volumes logiques**
  La sauvegarde et la restauration des ressources avec volumes logiques, tels que LDM dans Windows (disques dynamiques) et LVM dans Linux, sont prises en charge avec certaines limitations. Pour plus d'informations sur ces limitations, voir "Opérations prises en charge pour les volumes logiques" (p. 543).

Compatibilité avec les stockages Data Domain Dell EMC

Vous pouvez utiliser les terminaux Data Domain Dell EMC comme stockage des sauvegardes.

Avec ce stockage, nous vous recommandons d'utiliser un modèle de sauvegarde qui crée des sauvegardes complètes régulièrement, par exemple **Toujours complète**. Pour en savoir plus sur les modèles de sauvegarde disponibles, voir "Modèles de sauvegarde" (p. 571).

Verrouillage de la rétention

Le verrouillage de la rétention (mode gouvernance) est pris en charge. Si ce verrouillage est activé dans le stockage Data Domain, vous devez ajouter la variable d'environnement `AR_RETENTION_LOCK_SUPPORT` à la machine avec l'agent de protection qui utilise ce stockage comme destination de sauvegarde. Pour plus d'informations, voir "Ajout de la variable AR_RETENTION_LOCK_SUPPORT" (p. 538).

Remarque
Les stockages Data Domain Dell EMC dont le verrou de rétention est activé ne sont pas pris en charge par l'agent pour Mac.

Si le verrouillage de la rétention est activé dans le stockage Data Domain, les sauvegardes dans le stockage ne seront pas supprimées par les règles de rétention dans le plan de protection. Aucune erreur n'est affichée. Les sauvegardes seront supprimées lorsque le verrouillage de rétention expirera et que les règles de rétention seront à nouveau appliquées.

Selon la configuration du plan de protection, les règles de rétention sont appliquées à une archive avant ou après une sauvegarde.

Ajout de la variable AR_RETENTION_LOCK_SUPPORT

Si le verrouillage de la rétention est activé sur le stockage Data Domain, vous devez ajouter la variable d'environnement `AR_RETENTION_LOCK_SUPPORT` à l'ordinateur avec l'agent de protection qui utilise ce stockage comme destination de sauvegarde.

Pour ajouter la variable d'environnement `AR_RETENTION_LOCK_SUPPORT`

 © Acronis International GmbH, 2003-2026

Sous Windows

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent de protection.
2. Dans le **Panneau de configuration**, accédez à **Système et sécurité** > **Système** > **Paramètres système avancés**.
3. Dans l'**onglet Avancé**, cliquez sur **Variables d'environnement**.
4. Dans le panneau **Variables système**, cliquez sur **Nouveau**.
5. Dans la fenêtre **Nouvelle variable système**, ajoutez la nouvelle variable comme suit :
   - Nom de la variable : `AR_RETENTION_LOCK_SUPPORT`
   - Valeur de la variable : `1`
6. Cliquez sur **OK**.
7. Dans la fenêtre **Variables d'environnement**, cliquez sur **OK**.
8. Redémarrez la machine.

Sous Linux

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec l'agent de protection.
2. Accédez au répertoire `/sbin`, puis ouvrez le fichier `acronis_mms` à modifier.
3. Ajoutez la ligne suivante au-dessus de la ligne `export LD_LIBRARY_PATH` :

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Enregistrez le fichier `acronis_mms`.
5. Redémarrez la machine.

Dans une appliance virtuelle

1. Connectez-vous en tant qu'administrateur à l'appliance virtuelle.
2. Accédez au répertoire `/bin`, puis ouvrez le fichier `autostart` à modifier.
3. Ajoutez la ligne suivante sous la ligne `export LD_LIBRARY_PATH` :

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Enregistrez le fichier `autostart`.
5. Redémarrez l'appliance virtuelle.

Systèmes de fichiers pris en charge

Un agent de protection peut sauvegarder tout système de fichiers accessible depuis le système d'exploitation sur lequel l'agent en question est installé. Par exemple, l'agent pour Windows peut sauvegarder et restaurer un système de fichiers ext4 si le pilote correspondant est installé sur Windows.

© Acronis International GmbH, 2003-2026

Le tableau ci-dessous répertorie les systèmes de fichiers qui peuvent être sauvegardés et restaurés (le support de démarrage prend uniquement en charge la restauration). Les limites s'appliquent aux agents comme au support de démarrage.

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
FAT16/32	Tous les agents*	+	+	Aucune limite
NTFS	Tous les agents	+	+	
ext2/ext3/ext4	Tous les agents	+	-	
HFS+	Agent pour Mac	-	+	
APFS	Agent pour Mac	-	+	• Prise en charge à partir de macOS High Sierra 10.13 • La configuration du disque doit être recréée manuellement en cas de restauration vers une machine non d'origine ou à froid.
JFS	Agent pour Linux	+	-	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle
ReiserFS3	Agent pour Linux	+	-	
ReiserFS4	Agent pour Linux	+	-	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle

© Acronis International GmbH, 2003-2026

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
				• Il n'est pas possible de redimensionner des volumes pendant une restauration
ReFS	Tous les agents	+	+	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration • Lors de la restauration d'un fichier à partir d'une sauvegarde ReFS, seul le contenu est restauré. Les listes de contrôle d'accès (ACL) et les autres flux ne sont pas restaurés. Les fichiers dispersés sont restaurés comme des fichiers normaux.
XFS	Tous les agents	+	+	• Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration • Le mode de sauvegarde incrémentielle rapide n'est pas supporté pour le système de fichiers XFS. Les

© Acronis International GmbH, 2003-2026

Système de fichiers	Pris en charge par			Limites
	Agents	Support de démarrage pour Windows et Linux	Support de démarrage pour Mac	
				sauvegardes incrémentielles et différentielles de volumes XFS dans le cloud peuvent être considérablement plus lentes que des sauvegardes ext4 comparables qui utilisent le mode incrémentiel rapide.
Linux swap	Agent pour Linux	+	-	Aucune limite
exFAT	Tous les agents	+ Un support de démarrage ne peut pas être utilisé pour la restauration si la sauvegarde *est stockée sur* exFAT	+	• Seule la sauvegarde de disque/volume est prise en charge • Les filtres de fichier (inclusions/exclusions) ne sont pas pris en charge par le support • Des fichiers individuels ne peuvent pas être restaurés à partir d'une sauvegarde

*Sur les systèmes Windows XP, l'Agent pour Windows prend uniquement en charge les lecteurs au format NTFS.

Le logiciel passe automatiquement en mode secteur par secteur lorsque la sauvegarde présente des systèmes de fichiers non reconnus ou non pris en charge (par exemple, Btrfs). Il est possible d'effectuer une sauvegarde secteur par secteur pour tout système de fichiers qui :

- est basé sur des blocs ;
- n'utilise qu'un seul disque ;
- dispose d'un schéma de partitionnement MBR/GPT standard.

Si le système de fichiers ne remplit pas ces conditions, la sauvegarde échoue.

© Acronis International GmbH, 2003-2026

Déduplication des données

Dans Windows Server 2012 et versions ultérieures, vous pouvez activer la fonctionnalité de déduplication des données pour un volume NTFS. La déduplication des données réduit l'espace utilisé sur le volume en stockant les fragments de fichiers dupliqués du volume une fois seulement.

Vous pouvez sauvegarder et restaurer au niveau disque et sans limites un volume sur lequel la déduplication des données est activée. La sauvegarde de niveau fichier est prise en charge, sauf lors de l'utilisation du fournisseur VSS Acronis. Pour récupérer des fichiers à partir d'une sauvegarde de disque, exécutez une machine virtuelle depuis votre sauvegarde ou montez la sauvegarde sur un ordinateur exécutant Windows Server 2012 ou version ultérieure, puis copiez les fichiers à partir du volume monté.

La fonctionnalité de déduplication des données de Windows Server n'est pas liée à la fonctionnalité de déduplication Acronis Backup.

Opérations prises en charge pour les volumes logiques

La sauvegarde et la restauration des ressources avec des volumes logiques tels que LDM sous Windows (disques dynamiques) et LVM sous Linux sont prises en charge, mais avec les limitations suivantes.

Sauvegarde

La sauvegarde avec agent est une sauvegarde créée par un agent de protection installé sur la ressource ou sur un support de démarrage.

La sauvegarde sans agent n'est disponible que pour les machines virtuelles. Elle est effectuée au niveau de l'hyperviseur par un agent qui peut sauvegarder et restaurer toutes les machines virtuelles de l'environnement. Aucun agent n'est installé sur les machines virtuelles protégées.

Pour plus d'informations sur les différences entre les sauvegardes avec et sans agent, voir "Sauvegarde avec et sans agent" (p. 40).

Sauvegarde basée sur un agent	Sauvegarde sans agent
• Les volumes logiques sont sauvegardés par volume. • Les filtres de fichiers (inclusions/exclusions) sont pris en charge.	• Lorsqu'un volume logique est détecté sur un disque, ce dernier est sauvegardé en mode secteur par secteur (RAW). La structure de partition du disque n'est pas analysée et aucune image de volume n'est stockée séparément. • Les différents volumes LDM ou LVM ne peuvent pas être sélectionnés comme sources de sauvegarde, ni par sélection directe, ni par la l'utilisation de règles de politique. L'option **Ordinateur complet** est disponible dans la section **Quoi sauvegarder** d'un plan de

© Acronis International GmbH, 2003-2026

Sauvegarde basée sur un agent	Sauvegarde sans agent
	protection. • Les filtres de fichiers (inclusions/exclusions) ne sont pas pris en charge. Les inclusions ou exclusions configurées seront ignorées.

Restauration

La restauration avec agent est effectuée par un agent installé sur la ressource ou sur un support de démarrage.

La restauration sans agent ne prend en charge que les machines virtuelles en tant que cibles. Elle est effectuée au niveau de l'hyperviseur par un agent qui peut sauvegarder et restaurer toutes les machines virtuelles de l'environnement. Il n'est pas nécessaire de créer manuellement une machine cible vers laquelle la sauvegarde est restaurée.

	À partir d'une sauvegarde avec agent	À partir d'une sauvegarde sans agent
Restauration avec agent	• Une restauration par volume est possible. • La restauration de fichiers et de dossiers est possible. • Vous pouvez restaurer un ordinateur Linux avec des volumes LWM à partir d'une sauvegarde avec agent dans le cloud public vers un nouvel ordinateur en utilisant la réplication de sauvegarde et un support de démarrage. Tout d'abord, répliquer la sauvegarde depuis l'emplacement du cloud public vers un partage de mise en réseau ou un disque local. Ensuite, utiliser un support de démarrage basé sur Linux (avec une représentation de volume de type Linux) pour recréer la structure LWM et restaurer l'ordinateur.	• La restauration par volume n'est pas disponible. • La restauration de fichiers et de dossiers est possible.
Restauration sans agent	• La migration de machines (P2V, V2P et V2V) n'est pas prise en charge. Pour restaurer des données à partir d'une sauvegarde avec agent, utilisez un support de démarrage. • L'opération **Exécuter en tant que VM** n'est pas prise en charge.	• La restauration par volume n'est pas disponible. • La restauration de l'ensemble de la machine est possible. • La restauration de fichiers et de dossiers est possible. • L'opération **Exécuter en tant que VM**

© Acronis International GmbH, 2003-2026

	À partir d'une sauvegarde avec agent	À partir d'une sauvegarde sans agent
	• La restauration de fichiers et de dossiers est possible.	est prise en charge. Pour que la machine virtuelle soit amorçable, vous devrez peut-être modifier l'ordre d'amorçage. Pour plus d'informations, consultez cet article de la base de connaissances. • La conversion dans les types de machines virtuelles suivants est prise en charge : ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

Compatibilité avec le logiciel de chiffrage

Les données de sauvegarde et de restauration chiffrées par le logiciel de chiffrement de *niveau de fichier* ne sont soumises à aucune limite.

Un logiciel de chiffrement de *niveau disque* chiffre à la volée. C'est la raison pour laquelle des données contenues dans la sauvegarde ne sont pas chiffrées. Un logiciel de chiffrement de niveau disque modifie généralement les zones système : secteurs de démarrage, tables de partition ou tables de système de fichiers. Ces facteurs ont une incidence sur la sauvegarde et la restauration de niveau disque, sur la possibilité du système restauré de démarrer et d'avoir accès à Secure Zone.

Vous pouvez sauvegarder les données chiffrées par les logiciels de chiffrement de niveau disque suivants :

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Pour assurer une restauration de niveau disque fiable, suivez les règles communes et les recommandations spécifiques au logiciel.

Règle commune d'installation

Nous vous recommandons vivement d'installer le logiciel de chiffrement avant d'installer les agents de protection.

Façon d'utiliser Secure Zone

Secure Zone ne doit pas être chiffrée avec un chiffrement de niveau disque. C'est la seule façon d'utiliser Secure Zone :

© Acronis International GmbH, 2003-2026

1. Installez le logiciel de chiffrement, puis installez l'agent.
2. Créez Secure Zone.
3. Excluez Secure Zone lorsque vous chiffrez le disque ou ses volumes.

Règle de sauvegarde commune

Vous pouvez créer une sauvegarde de niveau disque dans le système d'exploitation.

Procédures de restauration spécifiques au logiciel

Chiffrement de lecteur BitLocker Microsoft

Pour restaurer un système qui a été chiffrée par BitLocker :

1. Démarrer à partir du support de démarrage.
2. Restaurer le système. Les données restaurées seront non chiffrées.
3. Redémarrer le système restauré.
4. Activer BitLocker.

Si vous devez restaurer seulement une partition d'un disque contenant plusieurs partitions, faites-le sous le système d'exploitation. La restauration sous un support de démarrage peut rendre la partition restaurée non détectable pour Windows.

McAfee Endpoint Encryption et PGP Whole Disk Encryption

Vous pouvez restaurer une partition système chiffrée en utilisant uniquement le support de démarrage.

Si le démarrage du système restauré échoue, reconstruisez le secteur de démarrage principal tel que décrit dans l'article de base de connaissances suivant : https://support.microsoft.com/kb/2622803.

Compatibilité avec les disques durs Advanced Format (secteurs 4 K)

La sauvegarde et la restauration sont prises en charge sur les disques durs traditionnels avec une taille de secteur de 512 octets, et sur les disques au format avancé avec une taille de secteur de 4096 octets.

Lorsque vous restaurez des données d'un disque à un autre, les deux disques doivent avoir la même taille de secteur logique (c'est la taille qui est présentée au système d'exploitation). Les volumes sur le disque sont automatiquement alignés, si nécessaire. Ainsi, le début d'un cluster dans le système de fichiers correspond toujours au début d'un secteur physique sur le disque.

L'International Disk Drive Equipment and Materials Association (IDEMA) spécifie deux types de disques Advanced Format :

© Acronis International GmbH, 2003-2026

- Disques à émulation 512 octets (512e)

  Ces disques ont une taille de secteur logique de 512 octets.
- Disques natifs 4K (4Kn)

  Ces disques ont une taille de secteur logique de 4096 octets.

  Les disques 4Kn sont couramment utilisés comme lecteurs externes avec connexion USB. Le démarrage du système pourrait ne pas être pris en charge avec ces disques.

Pour plus d'informations sur le Advanced Format, voir https://idema.org/initiatives/advanced-format.

Pour vérifier la taille de secteur logique d'un disque

Windows

1. Assurez-vous que le disque contient un volume NTFS.
2. Exécutez la commande suivante en tant qu'administrateur, en spécifiant la lettre de lecteur du volume NTFS (par exemple, `D`) :

   ```
   fsutil fsinfo ntfsinfo D:
   ```
3. Vérifiez la valeur dans la ligne **Bytes Per Sector**.

   Par exemple :

   ```
   Bytes Per Sector: 512
   ```

Linux

1. Vérifiez le nom du périphérique du disque.

   Par exemple `/dev/sdb`.
2. Exécutez la commande suivante en tant qu'utilisateur root (superutilisateur), en spécifiant le nom du périphérique du disque :

   ```
   parted /dev/sdb print
   ```
3. Vérifiez la première valeur de la ligne **Sector size (logical/physical)**.

   Par exemple :

   ```
   Sector size (logical/physical): 512B/4096B
   ```

Sauvegarde

Un plan de protection avec module de sauvegarde activé est un ensemble de règles qui définissent la manière dont les données en question seront protégées sur une machine spécifique.

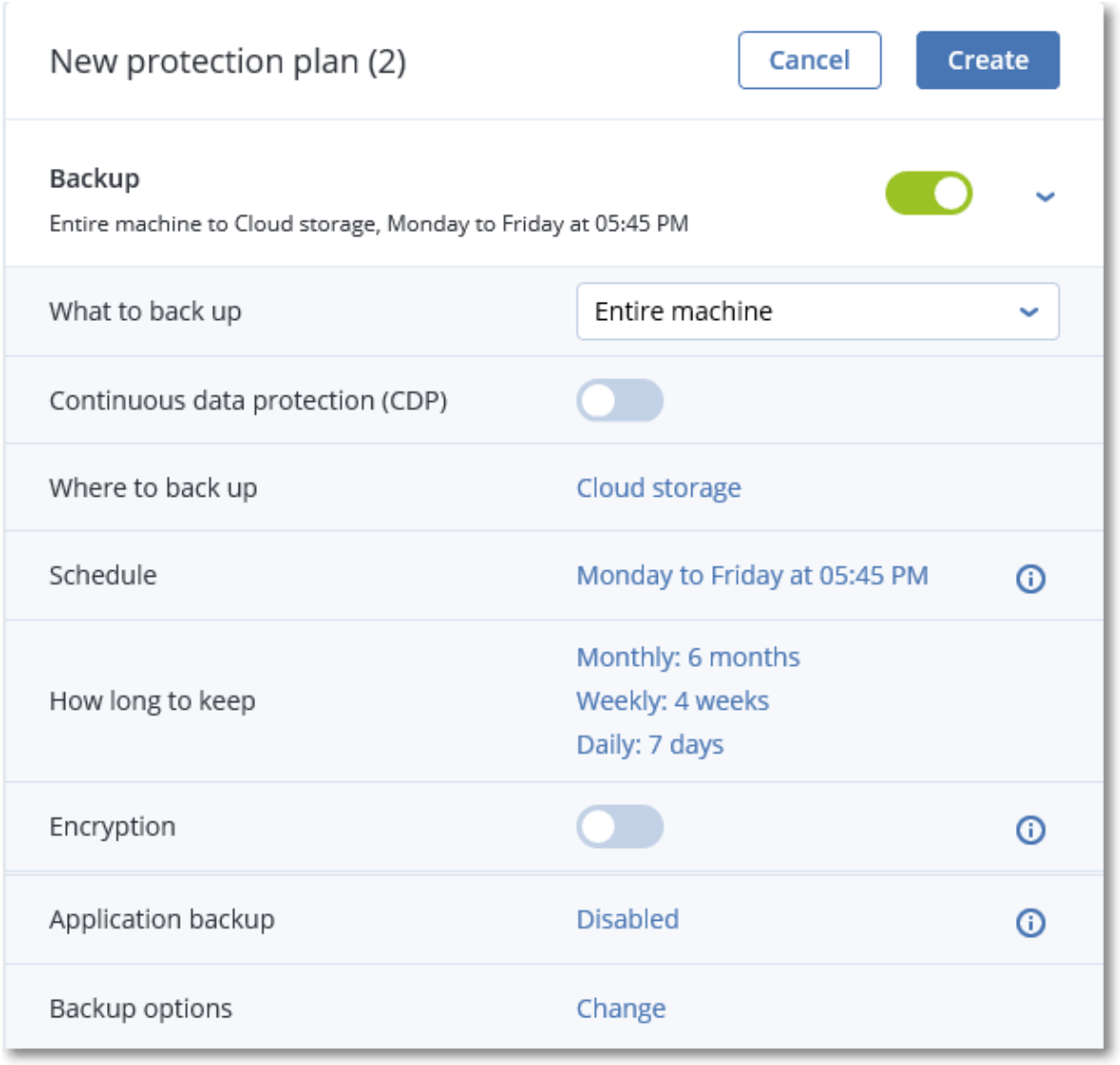
Un plan de protection peut être appliqué à plusieurs machines, soit au moment de sa création, soit plus tard.

Créer votre premier plan de protection avec module de sauvegarde activé

© Acronis International GmbH, 2003-2026

1. Sélectionnez les machines que vous voulez sauvegarder.
2. Cliquez sur **Protection**.

   Les plans de protection appliqués à l'ordinateur s'affichent. Si aucun plan n'est encore appliqué à la machine, vous verrez le plan de protection par défaut qui peut être appliqué. Vous pouvez modifier les paramètres le cas échéant et appliquer ce plan ou en créer un nouveau.
3. Pour créer un plan, cliquez sur **Création d'un plan**. Activez le module **Sauvegarde** et dévoilez les paramètres.

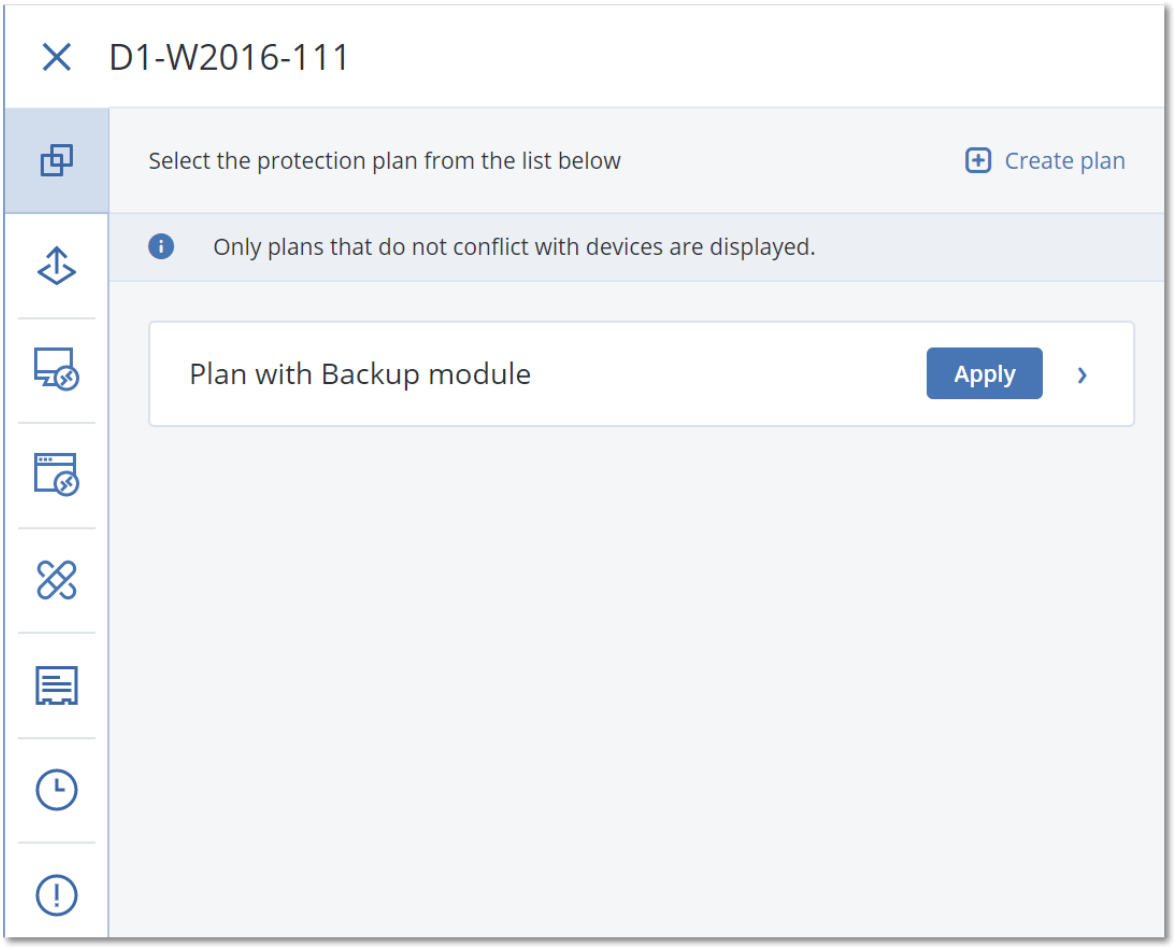


4. [Facultatif] Pour modifier le nom du plan de protection, cliquez sur le nom par défaut.
5. [Facultatif] Pour modifier les paramètres du module de sauvegarde, cliquez sur la section correspondante du volet du plan de protection.
6. [Facultatif] Pour modifier les options de sauvegarde, cliquez sur **Modifier** à côté d'**Options de sauvegarde**.
7. Cliquez sur **Créer**.

Appliquer un plan de protection existant

© Acronis International GmbH, 2003-2026

1. Sélectionnez les machines que vous voulez sauvegarder.
2. Cliquez sur **Protection**. Si un plan de protection courant est déjà appliqué aux machines sélectionnées, cliquez sur **Ajouter un plan**.
   Le logiciel affiche les plans de protection existants.



3. Sélectionnez un plan de protection à appliquer.
4. Cliquez sur **Appliquer**.

Aide-mémoire pour la sauvegarde

Le tableau suivant récapitule les paramètres de sauvegarde les plus courants.

QUOI SAUVEGARDER	ÉLÉMENTS A SAUVEGARDER Méthodes de sélection	OÙ SAUVEGARDER	PLANIFICATION Modèles de sauvegarde
Disques/volumes (machines	Sélection directe	Cloud	Toujours

© Acronis International GmbH, 2003-2026

QUOI SAUVEGARDER	ÉLÉMENTS A SAUVEGARDER Méthodes de sélection	OÙ SAUVEGARDER	PLANIFICATION Modèles de sauvegarde
physiques[1])	Règles de stratégie Filtres de fichiers	Dossier local Dossier réseau NFS* Secure Zone**	incrémentielle (fichier unique) Toujours complète Complète hebdomadaire, incrémentielle journalière Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS) Personnalisée (C-D-I)
Disques/volumes (machines virtuelles[2])	Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau NFS*	
Fichiers (machines physiques uniquement[3])	Sélection directe Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau NFS* Secure Zone**	Toujours incrémentielle (fichier unique) Toujours complète Complète hebdomadaire, incrémentielle journalière Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS) Personnalisée (C-D-I)
Configuration ESXi	Sélection directe	Dossier local Dossier réseau NFS*	

[1]Une machine sauvegardée par un agent installé sur le système d'exploitation.
[2]Une machine virtuelle sauvegardée au niveau de l'hyperviseur par un agent externe tel que l'agent pour VMware ou l'agent pour Hyper-V. Une machine virtuelle avec un agent interne est traitée comme une machine physique au niveau de la sauvegarde.
[3]Une machine sauvegardée par un agent installé sur le système d'exploitation.

© Acronis International GmbH, 2003-2026

QUOI SAUVEGARDER		ÉLÉMENTS A SAUVEGARDER Méthodes de sélection	OÙ SAUVEGARDER	PLANIFICATION Modèles de sauvegarde
Etat du système		Sélection directe	Cloud Dossier local Dossier réseau	Toujours complète Complète hebdomadaire, incrémentielle journalière Personnalisée (C-I) Toujours incrémentielle (fichier unique) - Uniquement pour les bases de données SQL
Bases de données SQL		Sélection directe		
Bases de données Exchange		Sélection directe		
Microsoft 365	Boîtes aux lettres (agent local pour Microsoft 365)	Sélection directe	Cloud Dossier local Dossier réseau	Toujours incrémentielle (fichier unique)
	Boîtes aux lettres (agent Cloud pour Microsoft 365)	Sélection directe	Cloud	Jusqu'à 6 sauvegardes par jour
	Dossiers publics	Sélection directe		
	Teams	Sélection directe		
	Fichiers OneDrive	Sélection directe Règles de stratégie		
	Données SharePoint Online	Sélection directe Règles de stratégie		
Google Workspace	Boîtes aux lettres Gmail	Sélection directe	Cloud	Jusqu'à 6 sauvegardes par jour
	Fichiers Google Drive	Sélection directe Règles de stratégie		
	Fichiers de Drive partagés	Sélection directe Règles de stratégie		

* La sauvegarde vers des partages NFS n'est pas disponible sous Windows.

© Acronis International GmbH, 2003-2026

** Il est impossible de créer Secure Zone sur un Mac.

Remarque
Les sauvegardes vers le cloud public nécessitent un quota de stockage de **Sauvegarde locale**.

Durée de conservation des sauvegardes

Vous pouvez conserver vos sauvegardes indéfiniment ou configurer une période de rétention selon les critères suivants :

- Par ancienneté des sauvegardes (règle unique/ensemble de sauvegardes)
- Par nombre de sauvegardes
- Par volume total de sauvegardes

Remarque
La règle de rétention **Par volume total de sauvegardes** n'est pas disponible avec le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** ni lors de la sauvegarde dans le stockage dans le cloud.

Voir Règles de rétention.

Sélection des données à sauvegarder

Sélection d'un ordinateur complet

La sauvegarde d'une machine dans son intégralité correspond à une sauvegarde de tous ses disques non amovibles. Pour plus d'informations sur la sauvegarde de disque, reportez-vous à "Sélection de disques ou de volumes" (p. 553).

Limites

- Les sauvegardes de disque ne sont pas prises en charge pour les volumes APFS chiffrés qui sont verrouillés. Ce type de volumes est ignoré lors des sauvegardes complètes de machine.
- Vous ne pouvez pas restaurer le contenu du dossier racine de OneDrive à partir d'une sauvegarde **Ordinateur complet** ou **Disque/volumes**, même si le dossier OneDrive est affiché lors de la navigation dans l'archive de sauvegarde dans une application de gestionnaire de fichiers telle que l'Explorateur de fichiers. Lors de la navigation dans l'archive dans la console Cyber Protect, le dossier OneDrive n'est pas affiché. Lors de la navigation dans l'archive dans la console Web Restore, le dossier OneDrive est affiché en tant que fichier, mais la restauration à partir de cette sauvegarde n'est pas possible.
  Pour pouvoir restaurer le contenu du dossier OneDrive, créez une sauvegarde **Fichiers/dossiers**. Les fichiers qui ne sont pas disponibles sur le terminal s'affichent dans l'archive, mais ne peuvent pas être restaurés.

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Sélection de disques ou de volumes

Une sauvegarde de niveau disque contient une copie d'un disque ou d'un volume sous forme compacte. Vous pouvez restaurer des disques, volumes, dossiers et fichiers depuis une sauvegarde de disque.

Vous pouvez sélectionner les disques ou les volumes à sauvegarder pour chaque ressource figurant dans le plan de protection (sélection directe) ou configurer des règles de stratégie pour plusieurs ressources. Par ailleurs, vous pouvez exclure certains fichiers d'une sauvegarde ou n'inclure que des fichiers spécifiques en configurant des filtres de fichier. Pour plus d'informations, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 620).

Pour sélectionner des disques ou des volumes

Sélection directe

La sélection directe n'est disponible que pour les machines physiques.

1. Dans **Quoi sauvegarder**, sélectionnez **Disques/volumes**.
2. Cliquez sur **Éléments à sauvegarder**.
3. Dans **Sélectionner les éléments à sauvegarder**, sélectionnez **Directement**.
4. Pour chacune des ressources comprises dans le plan de protection, cochez les cases à côté des disques ou des volumes à sauvegarder.
5. Cliquez sur **Terminé**.

Par règles de stratégie

1. Dans **Quoi sauvegarder**, sélectionnez **Disques/volumes**.
2. Cliquez sur **Éléments à sauvegarder**.
3. Dans **Sélectionner les éléments à sauvegarder**, choisissez **Utilisation des règles de stratégie**.
4. Sélectionnez n'importe quelle règle prédéfinie, créez les vôtres ou combinez les deux.
   Pour plus d'informations sur les règles de stratégie disponibles, voir "Règles de stratégie pour les disques et les volumes" (p. 555).
   Les règles de stratégie seront appliquées à l'ensemble des ressources incluses dans le plan de protection.
   Si aucune des règles spécifiées ne peut être appliquée à une ressource, la sauvegarde de cette ressource échoue.
5. Cliquez sur **Terminé**.

Limites

- Les sauvegardes de disque ne sont pas prises en charge pour les volumes APFS chiffrés qui sont verrouillés. Ce type de volumes est ignoré lors des sauvegardes complètes de machine.

© Acronis International GmbH, 2003-2026

- Vous ne pouvez pas restaurer le contenu du dossier racine de OneDrive à partir d'une sauvegarde **Ordinateur complet** ou **Disque/volumes**, même si le dossier OneDrive est affiché lors de la navigation dans l'archive de sauvegarde dans une application de gestionnaire de fichiers telle que l'Explorateur de fichiers. Lors de la navigation dans l'archive dans la console Cyber Protect, le dossier OneDrive n'est pas affiché. Lors de la navigation dans l'archive dans la console Web Restore, le dossier OneDrive est affiché en tant que fichier, mais la restauration à partir de cette sauvegarde n'est pas possible.

  Pour pouvoir restaurer le contenu du dossier OneDrive, créez une sauvegarde **Fichiers/dossiers**. Les fichiers qui ne sont pas disponibles sur le terminal s'affichent dans l'archive, mais ne peuvent pas être restaurés.
- Vous pouvez sauvegarder des disques connectés via le protocole iSCSI sur une machine physique. Toutefois, des limites s'appliquent si vous utilisez l'agent pour VMware ou l'agent pour Hyper-V pour sauvegarder les disques connectés à iSCSI. Pour plus d'informations, voir "Limites" (p. 528).

Que stocke une sauvegarde de disque ou de volume ?

Une sauvegarde de disque ou de volume stocke le **système de fichiers** d'un disque ou d'un volume en entier et inclut toutes les informations nécessaires pour le démarrage du système d'exploitation. Il est possible de restaurer des disques ou volumes entiers à partir de telles sauvegardes de même que des fichiers ou dossiers individuels.

Avec l'option **secteur-par-secteur (mode nu)**activée, une sauvegarde de disque stocke tous les secteurs du disque. L'option secteur-par-secteur peut être utilisée pour la sauvegarde de disques avec systèmes de fichiers non-reconnus ou non-supportés ainsi que d'autres formats de données propriétaires.

Windows

Une sauvegarde de volume stocke tous les fichiers et dossiers du volume sélectionné indépendemment de leurs attributs (y compris fichiers cachés et système), secteur de démarrage, tableau d'allocation de fichiers (FAT) s'il existe, fichier racine et la piste zéro du disque dur avec le secteur de démarrage principal (MBR).

Une sauvegarde de disque stocke tous les volumes du disque sélectionné (incluant les volumes cachés tels que les partitions de maintenance du fabricant) et la piste zéro avec la zone d'amorce maître.

Les éléments suivants ne sont *pas* inclus dans une sauvegarde de disque ou de volume (de même que dans une sauvegarde de niveau fichier) :

- Le fichier d'échange (pagefile.sys) et le fichier qui maintient le contenu de la RAM quand la machine se met en veille (hiberfil.sys). Après la restauration, les fichiers seront re-créés dans leur emplacement approprié avec une taille zéro.
- Si la sauvegarde est effectuée sous le système d'exploitation (par opposition au support de démarrage ou à la sauvegarde de machines virtuelles au niveau hyperviseur) :

© Acronis International GmbH, 2003-2026

- Stockage Windows shadow. Le chemin vers cet emplacement de stockage est déterminé par la valeur de registre **VSS Default Provider** qui peut être trouvée dans la clé de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Ceci signifie que dans les systèmes d'exploitation démarrant avec Windows Vista, les points de restauration Windows ne sont pas sauvegardés.
- Si l'option **VSS (service de cliché instantané des volumes)** de sauvegarde est activée, les fichiers et les dossiers qui ont été indiqués dans la clé de la base de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**.

Linux

Une sauvegarde de volume stocke tous les fichiers et répertoires du volume sélectionné indépendemment de leurs attributs, du secteur de démarrage, et le système de fichiers super bloc.

Une sauvegarde de disque stocke tous les volumes des disques ainsi que la piste zéro avec la zone d'amorce maître.

Mac

Un disque ou une sauvegarde de volume stocke tous les fichiers et répertoires du disque ou volume sélectionné, plus une description de la disposition du volume.

Les éléments suivants sont exclus :

- Métadonnées de système, telles que le journal du système de fichiers et l'index Spotlight
- La poubelle
- Chronométrez les sauvegardes de la machine

Physiquement, les disques et volumes d'un Mac sont sauvegardés au niveau du fichier. La restauration à froid à partir des sauvegardes de disque et de volume est possible, mais le mode de sauvegarde secteur par secteur n'est pas disponible.

Règles de stratégie pour les disques et les volumes

Lorsque vous sélectionnez des disques ou des volumes à sauvegarder, vous pouvez utiliser les stratégies de règle suivantes en fonction du système d'exploitation de la ressource protégée.

Windows

- `[All Volumes]` sélectionne tous les volumes sur l'ordinateur.
- Lettre de lecteur (par exemple, `C:\`) sélectionne le volume correspondant à la lettre de lecteur indiquée.
- `[Fixed Volumes (physical machines)]` sélectionne tous les volumes d'une machine physique, à l'exception des supports amovibles. Les volumes fixes incluent les volumes sur les terminaux SCSI, ATAPI, ATA, SSA, SAS et SATA, et sur les grappes RAID.
- `[BOOT+SYSTEM]` sélectionne les volumes système et les volumes de démarrage. Il s'agit de la combinaison minimale à partir de laquelle vous pouvez restaurer un système d'exploitation.

© Acronis International GmbH, 2003-2026

- `[Disk 1]` sélectionne le premier disque de la machine, en prenant en compte l'ensemble de ses volumes. Pour sélectionner un autre disque, saisissez son numéro correspondant.

Linux

- `[All Volumes]` sélectionne tous les volumes montés sur l'ordinateur.
- `/dev/hda1` sélectionne le premier volume du premier disque dur IDE.
- `/dev/sda1` sélectionne le premier volume du premier disque dur SCSI.
- `/dev/md1` sélectionne le premier logiciel de disque dur RAID.
- Pour sélectionnez d'autres volumes de base, spécifiez `/dev/xdyN`, où :
  - « x » correspond au type de disque
  - « y » correspond au numéro de disque (a pour le premier disque, b pour le second, etc.)
  - « N » étant le nombre de volumes.
- Pour sélectionner un volume logique, indiquez son chemin tel qu'il apparaît après l'exécution de la commande `ls /dev/mapper` sous le compte racine.

  Par exemple :

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Cette sortie montre deux volumes logiques, `lv1` et `lv2`, qui appartiennent au groupe de volumes `vg_1`. Pour sauvegarder ces volumes, spécifiez :

  `/dev/mapper/vg_1-lv1`

  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` sélectionne tous les volumes montés sur l'ordinateur.
- `[Disk 1]` sélectionne le premier disque de la machine, en prenant en compte l'ensemble de ses volumes. Pour sélectionner un autre disque, spécifiez le numéro correspondant.

Sélection de fichiers ou de dossiers

Utilisez la sauvegarde de fichier pour ne protéger que des données spécifiques, par exemple les fichiers de votre projet en cours. Les sauvegardes de fichier sont moins volumineuses que les sauvegardes de disque et permettent d'économiser l'espace de stockage.

Important
Vous ne pouvez pas restaurer un système d'exploitation à partir d'une sauvegarde de fichier.

Vous pouvez sélectionner les fichiers et les dossiers à sauvegarder pour chaque ressource figurant dans le plan de protection (sélection directe) ou configurer des règles de stratégie pour plusieurs ressources. Par ailleurs, vous pouvez exclure certains fichiers d'une sauvegarde ou n'inclure que des

© Acronis International GmbH, 2003-2026

fichiers spécifiques en configurant les filtres. Pour plus d'informations, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 620).

Pour sélectionner des fichiers ou des dossiers

Sélection directe

1. Dans **Quoi sauvegarder**, sélectionnez **Fichiers/dossiers**.
2. Dans **Éléments à sauvegarder**, cliquez sur **Spécifier**.
3. Dans **Sélectionner les éléments à sauvegarder**, sélectionnez **Directement**.
4. Spécifiez les fichiers ou dossiers à sauvegarder pour chaque ressource dans le plan de protection.
   a. Cliquez sur **Sélectionner les fichiers et dossiers**.
   b. Cliquez sur **Dossier local** ou sur **Dossier réseau**.
      Les dossiers réseau doivent être accessibles depuis l'ordinateur sélectionné.
      Lorsque vous sélectionnez la source **Dossier réseau**, vous pouvez sauvegarder les données de stockages NAS tels que les terminaux NetApp. Les terminaux NAS de tous les fournisseurs sont pris en charge.
   c. Sélectionnez les fichiers et dossiers que vous souhaitez sauvegarder.
      Vous pouvez sélectionner une combinaison allant jusqu'à 1 000 fichiers et dossiers.
      Alternativement, vous pouvez spécifier le chemin vers un fichier ou dossier, puis cliquer sur le bouton flèche.
   d. [Pour les dossiers partagés] Spécifiez le nom d'utilisateur et le mot de passe du dossier partagé.
      La sauvegarde des dossiers avec accès anonyme n'est pas prise en charge.
   e. Cliquez sur **Terminé**.

Par règles de stratégie

1. Dans **Quoi sauvegarder**, sélectionnez **Fichiers/dossiers**.
2. Dans **Éléments à sauvegarder**, cliquez sur **Spécifier**.
3. Dans **Sélectionner les éléments à sauvegarder**, choisissez **Utilisation des règles de stratégie**.
4. Sélectionnez n'importe quelle règle prédéfinie, créez les vôtres ou combinez les deux.
   Pour plus d'informations sur les règles de stratégie disponibles, voir "Règles de stratégie pour les fichiers et les dossiers" (p. 558).
   Les règles de stratégie seront appliquées à l'ensemble des ressources incluses dans le plan de protection.
   Si aucune des règles spécifiées ne peut être appliquée à une ressource, la sauvegarde de cette ressource échoue.
5. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Limites

- Vous pouvez sélectionner des fichiers et des dossiers lorsque vous sauvegardez des machines physiques ou virtuelles sur lesquelles un agent est installé (sauvegarde avec agent). La sauvegarde de fichier n'est pas disponible pour les machines virtuelles que vous sauvegardez en mode sans agent. Pour plus d'informations sur les différences entre ces types de sauvegarde, voir "Sauvegarde avec et sans agent" (p. 40).
- Vous ne pouvez pas restaurer le contenu du dossier racine de OneDrive à partir d'une sauvegarde **Ordinateur complet** ou **Disque/volumes**, même si le dossier OneDrive est affiché lors de la navigation dans l'archive de sauvegarde dans une application de gestionnaire de fichiers telle que l'Explorateur de fichiers. Lors de la navigation dans l'archive dans la console Cyber Protect, le dossier OneDrive n'est pas affiché. Lors de la navigation dans l'archive dans la console Web Restore, le dossier OneDrive est affiché en tant que fichier, mais la restauration à partir de cette sauvegarde n'est pas possible.

  Pour pouvoir restaurer le contenu du dossier OneDrive, créez une sauvegarde **Fichiers/dossiers**. Les fichiers qui ne sont pas disponibles sur le terminal s'affichent dans l'archive, mais ne peuvent pas être restaurés.
- Vous pouvez sauvegarder des fichiers et des dossiers stockés sur des disques connectés via le protocole iSCSI à une machine physique. Certaines limites s'appliquent si vous utilisez l'agent pour VMware ou l'agent pour Hyper-V pour sauvegarder les données sur des disques connectés à iSCSI.

Règles de stratégie pour les fichiers et les dossiers

Lorsque vous sélectionnez des fichiers ou des dossiers à sauvegarder, vous pouvez utiliser les stratégies de règle suivantes en fonction du système d'exploitation de la ressource protégée.

Windows

- Chemin complet vers un fichier ou un dossier. Par exemple, `D:\Work\Text.doc` ou `C:\Windows`.
- Règles prédéfinies :
  - `[All Files]` sélectionne tous les fichiers sur tous les volumes de la machine.
  - `[All Profiles Folder]` sélectionne le dossier dans lequel se trouvent tous les profils utilisateur. Par exemple, `C:\Users` ou `C:\Documents and Settings`.
- Variables d'environnement :
  - `%ALLUSERSPROFILE%` sélectionne le dossier où se trouvent les données communes à tous les profils des utilisateurs. Par exemple, `C:\ProgramData` ou `C:\Documents and Settings\All Users`.
  - `%PROGRAMFILES%` sélectionne le dossier `Program Files`. Par exemple, `C:\Program Files`.
  - `%WINDIR%` sélectionne le dossier `Windows`. Par exemple, `C:\Windows`.

  Vous pouvez utiliser d'autres variables d'environnement ou une combinaison de variables d'environnement et de texte. Par exemple, pour sélectionner le dossier Java dans le dossier Program Files, spécifiez : `%PROGRAMFILES%\Java`.

Linux

© Acronis International GmbH, 2003-2026

- Chemin complet vers un fichier ou un répertoire.

  Par exemple, pour sauvegarder `file.txt` sur le volume `/dev/hda3` monté sur `/home/usr/docs`, spécifiez `/dev/hda3/file.txt` ou `/home/usr/docs/file.txt`.
- Règles prédéfinies :
  - `[All Profiles Folder]` sélectionne `/home`. Par défaut, tous les profils utilisateur sont stockés dans ce dossier.
  - `/home` sélectionne le répertoire personnel des utilisateurs courants.
  - `/root` sélectionne le répertoire personnel de l'utilisateur racine.
  - `/usr` sélectionne le répertoire de tous les programmes liés aux utilisateurs.
  - `/etc` sélectionne le répertoire des fichiers de configuration du système.

macOS

- Chemin complet vers un fichier ou un répertoire.

  Par exemple :
  - Pour sauvegarder `file.txt` sur le bureau d'un utilisateur, spécifiez `/Users/<user name>/Desktop/file.txt`.
  - Pour sauvegarder les dossiers `Desktop`, `Documents` ou `Downloads` d'un utilisateur, spécifiez `/Users/<user name>/Desktop`, `/Users/<user name>/Documents` ou `/Users/<user name>/Downloads`.
  - Pour sauvegarder le dossier de base de tous les utilisateurs qui possèdent un compte sur cet ordinateur, spécifiez `/Users`.
  - Pour sauvegarder le dossier dans lequel les applications sont installées, spécifiez `/Applications`.
- Règles prédéfinies
  - `[All Profiles Folder]` sélectionne `/Users`. Par défaut, tous les profils utilisateur sont stockés dans ce dossier.

Sélection de l'état du système

Remarque
La sauvegarde de l'état du système est disponible pour les ordinateurs exécutant Windows 7 et versions ultérieures sur lesquels l'agent pour Windows est installé. La sauvegarde de l'état du système n'est pas disponible pour les pour les machines virtuelles qui sont sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent).

Pour sauvegarder l'état du système, dans **Quoi sauvegarder**, sélectionnez **Etat du système**.

Une sauvegarde de l'état du système se compose des fichiers suivants :

- Configuration du planificateur de tâches
- VSS Metadata Store
- Informations de configuration du compteur de performances

© Acronis International GmbH, 2003-2026

- Service MSSearch
- Service de transfert intelligent en arrière-plan (BITS)
- Le registre
- Windows Management Instrumentation (WMI)
- Bases de données d'enregistrement des services de composants

Sélection de la configuration ESXi

La sauvegarde d'une configuration d'hôte ESXi vous permet de restaurer un hôte ESXi de manière complète. La restauration est exécutée sous un support de démarrage.

Les machines virtuelles s'exécutant sur l'hôte ne sont pas incluses dans la sauvegarde. Elles peuvent être sauvegardées et restaurées séparément.

La sauvegarde d'une configuration d'hôte ESXi inclut :

- Le chargeur de démarrage et les partitions de banque de démarrage de l'hôte
- L'état de l'hôte (informations relatives à la configuration de la mise en réseau et du stockage virtuels, aux clés SSL, aux paramètres réseau du serveur, et à l'utilisateur local)
- Les extensions et correctifs installés ou préconfigurés sur l'hôte
- Les fichiers journaux

Prérequis

- SSH doit être activé dans le **Profil de sécurité** de la configuration de l'hôte ESXi.
- Vous devez connaître le mot de passe du compte « racine » sur l'hôte ESXi.

Limites

- La sauvegarde de la configuration ESXi n'est pas prise en charge pour les hôtes exécutant VMware ESXi 7.0 et les versions ultérieures.
- Une configuration ESXi ne peut pas être sauvegardée sur le stockage dans le Cloud.

Pour sélectionner une configuration ESXi

1. Cliquez sur **Terminaux** > **Tous les terminaux**, puis sélectionnez les hôtes ESXi que vous voulez sauvegarder.
2. Cliquez sur **Protection**.
3. Dans **Quoi sauvegarder**, sélectionnez **Configuration ESXi**.
4. Dans **Mot de passe « racine » ESXi**, spécifiez un mot de passe pour le compte « racine » pour chacun des hôtes sélectionnés ou appliquez le même mot de passe pour tous les hôtes.

Sélection d'une destination

Cliquez sur **Où sauvegarder**, puis sélectionnez l'une des options suivantes :

© Acronis International GmbH, 2003-2026

- **Stockage dans le Cloud**

  Les sauvegardes seront stockées dans le centre de données du Cloud.

  Remarque
  Les sauvegardes vers le cloud public nécessitent un quota de stockage de **Sauvegarde locale**.

- **Dossiers locaux**

  Si une seule machine est sélectionnée, naviguez jusqu'au dossier souhaité ou indiquez son chemin sur cette même machine.

  Si plusieurs machines sont sélectionnées, saisissez le chemin du dossier. Les sauvegardes seront stockées dans ce dossier, sur chacune des machines sélectionnées ou sur la machine où l'agent pour machines virtuelles est installé. Si le dossier n'existe pas, il sera créé.
- **Dossier réseau**

  Il s'agit d'un dossier partagé via SMB/CIFS/DFS.

  Accédez au dossier partagé requis ou saisissez le chemin au format suivant, où <host> correspond soit à un nom de domaine DNS complet, soit à une adresse IPv4 :
  - Pour les partages SMB/CIFS :
    - \\<host>\<path>\
    - smb://<host>/<path>/
  - Pour les partages DFS :
    - \\<host>\<DFS root>\<path>

  Cliquez ensuite sur la flèche. Si vous y êtes invité, spécifiez le nom d'utilisateur et le mot de passe requis pour accéder au dossier partagé. Vous pouvez modifier ces identifiants à tout moment en cliquant sur l'icône en forme de clé à côté du nom de dossier.

  La sauvegarde dans un dossier avec accès anonyme n'est pas prise en charge.
- **Cloud public**

  Cette option est disponible si la fonctionnalité **Direct Backup to Public Cloud** est activée pour votre tenant.

  Elle vous permet de configurer une sauvegarde directe vers un stockage compatible avec le cloud public sans avoir à déployer d'autres composants (Microsoft Azure ou d'autres machines virtuelles telles que les passerelles). Sélectionnez le cloud public souhaité pour vous y connecter.

  Remarque
  Les sauvegardes vers le cloud public nécessitent un quota de stockage de **Sauvegarde locale**.

  Pour plus d'informations, voir "Sauvegarde de ressources dans des clouds publics" (p. 745).
- **Dossier NFS** (disponible uniquement sur les machines sous Linux ou macOS)

  Vérifiez que le package nfs-utils est installé sur le serveur Linux sur lequel l'agent pour Linux est installé.

© Acronis International GmbH, 2003-2026

Pour accéder à un dossier NFS, parcourez jusqu'au dossier souhaité ou saisissez le chemin au format suivant, où <host> correspond soit à un nom de domaine DNS complet, soit à une adresse IPv4 :

nfs://<host>/<exported folder>:/<subfolder>

Cliquez ensuite sur la flèche.

Remarque
Il est impossible de sauvegarder un dossier NFS protégé par mot de passe.

- **Secure Zone** (disponible uniquement s'il est présent sur chacune des machines sélectionnées)
  Secure Zone est une partition sécurisée située sur un disque de la machine sauvegardée. Cette partition doit être créée manuellement avant la configuration d'une sauvegarde. Pour savoir comment créer Secure Zone, ainsi que connaître ses avantages et ses limitations, voir "À propos de Secure Zone" (p. 563).

Option de stockage avancée

Remarque
Cette fonctionnalité est disponible uniquement dans l'édition avancée du service Cyber Protection.

Défini par un script (disponible sur les machines fonctionnant sous Windows)

Vous pouvez stocker les sauvegardes de chaque machine dans un dossier défini par un script. Le logiciel prend en charge les scripts écrits en JScript, VBScript ou Python 3.5. Lors du déploiement du plan de protection, le logiciel exécute le script sur chaque machine. La sortie de script pour chaque ordinateur doit être un chemin de dossier local ou réseau. Si un dossier n'existe pas, il sera créé (limite : les scripts écris dans Python ne peuvent pas créer des dossiers sur des partages réseau). Dans l'onglet **Stockage de sauvegarde**, chaque dossier est affiché comme un emplacement de sauvegarde distinct.

Dans **Type de script**, sélectionnez le type de script (**JScript**, **VBScript** ou **Python**), puis importez, ou copiez et collez le script. Pour les dossiers réseau, spécifiez les informations d'identification avec les autorisations de lecture/écriture.

Exemples :

- Le script JScript suivant fournit l'emplacement de sauvegarde pour un ordinateur au format `\\bkpsrv\<machine name>` :

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  De ce fait, les sauvegardes de chaque ordinateur sont sauvegardées dans un dossier du même nom sur le serveur **bkpsrv**.
- Le script JScript suivant fournit l'emplacement de sauvegarde dans un dossier de l'ordinateur sur lequel le script s'exécute :

© Acronis International GmbH, 2003-2026

```
WScript.Echo("C:\\Backup");
```

De ce fait, les sauvegardes de cet ordinateur seront enregistrées dans le dossier `C:\Backup` sur le même ordinateur.

Remarque
Dans ces scripts, le chemin d'accès de l'emplacement est sensible à la casse. Ainsi, `C:\Backup` et `C:\backup` s'affichent en tant qu'emplacements différents dans la console Cyber Protect. Utilisez également la majuscule pour la lettre du lecteur.

À propos de Secure Zone

Secure Zone est une partition sécurisée sur un disque de la machine sauvegardée. Cette partition peut stocker des sauvegardes de disques ou de fichiers sur cette machine.

Si une panne du disque devait se produire, les sauvegardes situées dans Secure Zone pourraient être perdues. C'est pourquoi Secure Zone ne devrait pas être le seul emplacement où une sauvegarde est stockée. Dans un environnement d'entreprise, Secure Zone peut être considérée comme un emplacement intermédiaire utilisé pour la sauvegarde quand un emplacement ordinaire est momentanément indisponible ou connecté sur un canal lent ou occupé.

Pourquoi utiliser Secure Zone ?

Secure Zone :

- Permet la restauration d'un disque sur le même disque où la sauvegarde du disque est située.
- Offre une méthode rentable et pratique pour la protection de données contre les dysfonctionnements logiciels, les virus et les erreurs humaines.
- Élimine le besoin d'un support séparé ou d'une connexion réseau pour sauvegarder ou restaurer les données. Ceci est particulièrement utile pour les utilisateurs itinérants.
- Peut servir en tant que destination primaire lors de l'utilisation de la réplication des sauvegardes.

Limites

- Secure Zone ne peut pas être organisée sur un Mac.
- Secure Zone est une partition sur un disque de base. Cette partition ne peut pas être organisée sur un disque dynamique ou créé en tant que volume logique (géré par LVM).
- Secure Zone est formatée avec le système de fichiers FAT32. FAT32 ayant une limite de taille par fichier de 4 Go, les sauvegardes plus volumineuses sont fractionnées lorsqu'elles sont enregistrées sur Secure Zone. Cela n'affecte pas la procédure ni la vitesse de restauration.

© Acronis International GmbH, 2003-2026

Comment la création de Secure Zone transforme le disque

- Secure Zone est toujours créée à la fin d'un disque dur.
- S'il n'y a pas ou pas assez d'espace non alloué à la fin du disque, mais s'il y a de la place entre les volumes, les volume sont déplacés pour ajouter plus d'espace non-alloué vers la fin du disque.
- Lorsque tout l'espace non alloué est collecté mais que ce n'est toujours pas assez, le logiciel prend de l'espace libre dans les volumes que vous sélectionnez, proportionnellement à la taille des volumes.
- Cependant, il doit toujours y avoir de l'espace libre sur un volume, de façon à ce que le système d'exploitation et les opérations puissent fonctionner ; par exemple, pour la création de fichiers temporaires. Le logiciel ne réduira pas un volume où l'espace libre occupe ou occupera moins de 25 % de la taille totale du volume. Le logiciel continuera la réduction proportionnelle des volumes seulement quand tous les volumes sur le disque auront 25 % d'espace libre ou moins.

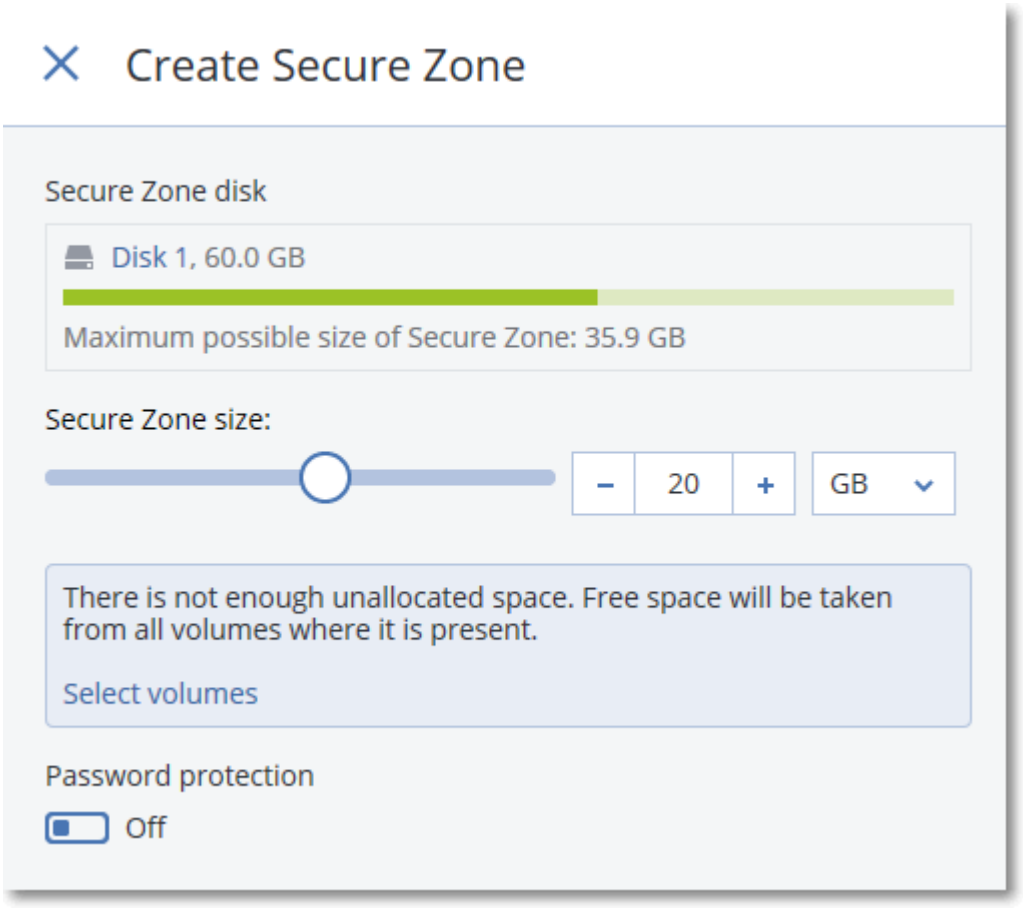
Comme il apparaît clairement ci-dessus, spécifier la taille de Secure Zone la plus grande possible n'est pas conseillé. Vous finirez avec aucun espace libre restant sur les volumes ce qui pourrait causer des problèmes sur le système d'exploitation ou les applications, tels qu'un fonctionnement instable, voire un échec du démarrage.

Important
Le déplacement ou le redimensionnement d'un volume à partir duquel le système a été démarré nécessite un redémarrage.

Comment créer Secure Zone

1. Sélectionnez la machine sur laquelle vous voulez créer Secure Zone.
2. Cliquez sur **Détails** > **Créer Secure Zone**.
3. Sous **disque Secure Zone**, cliquez sur **Sélectionner**, puis choisissez un disque dur (s'il en existe plusieurs) sur lequel vous voulez créer la zone.
   Le logiciel calcule la taille maximale possible de Secure Zone.
4. Entrez la taille de Secure Zone ou utilisez le curseur pour sélectionner n'importe quelle taille entre les tailles minimales et maximales.
   La taille minimale est d'environ 50 Mo, en fonction de la géométrie du disque dur. La taille maximale est égale à l'espace non alloué du disque plus l'espace libre total sur tous les volumes du disque.
5. Lorsque l'espace non alloué n'est pas suffisant pour la taille spécifiée, le logiciel prend de l'espace libre dans les volumes existants. Par défaut, tous les volumes sont sélectionnés. Si vous souhaitez exclure certains volumes, cliquez sur **Sélectionner volumes**. Sinon, ignorez cette étape.

© Acronis International GmbH, 2003-2026



6. [Facultatif] Activez la **Protection par mot de passe** et définissez un mot de passe.
   Ce mot de passe sera nécessaire pour accéder aux sauvegardes situées dans Secure Zone. La sauvegarde sur Secure Zone ne nécessite pas de mot de passe, sauf si elle est effectuée via un support de démarrage.
7. Cliquez sur **Créer**.
   Le logiciel affiche la structure de partition attendue. Cliquez sur **OK**.
8. Patientez pendant que le logiciel crée Secure Zone.

Vous pouvez à présent choisir Secure Zone sous **Où sauvegarder** lors de la création d'un plan de protection.

Comment supprimer Secure Zone

1. Sélectionnez une machine avec Secure Zone.
2. Cliquez sur **Détails**.
3. Cliquez sur l'icône en forme d'engrenage située à côté de **Secure Zone**, puis cliquez sur **Supprimer**.
4. [Facultatif] Sélectionnez les volumes auxquels ajouter l'espace libéré par la zone. Par défaut, tous les volumes sont sélectionnés.
   L'espace est réparti équitablement sur chaque volume sélectionné. Si vous ne sélectionnez aucun volume, l'espace libéré devient non alloué.

© Acronis International GmbH, 2003-2026

Le redimensionnement d'un volume à partir duquel le système a été démarré nécessite un redémarrage.

5. Cliquez sur **Supprimer**.

Secure Zone est alors supprimée avec toutes les sauvegardes qu'elle contient.

Protection continue des données (CDP)

La protection continue des données (CDP) fait partie de la protection standard. Elle sauvegarde les données critiques immédiatement après leur modification, garantissant qu'aucune modification ne sera perdue en cas de défaillance du système entre deux sauvegardes planifiées. Vous pouvez configurer la protection continue des données (CDP) pour les données suivantes :

- Fichiers ou dossiers dans des emplacements spécifiques
- Fichiers modifiés par des applications spécifiques

La protection continue des données n'est prise en charge que pour le système de fichiers NTFS et pour les systèmes d'exploitation suivants :

- Ordinateur de bureau : Windows 7 et versions ultérieures
- Serveur : Windows Server 2008 R2 et versions ultérieures

Seuls les dossiers locaux sont pris en charge. Les dossiers réseau ne peuvent pas être sélectionnés pour la protection continue des données.

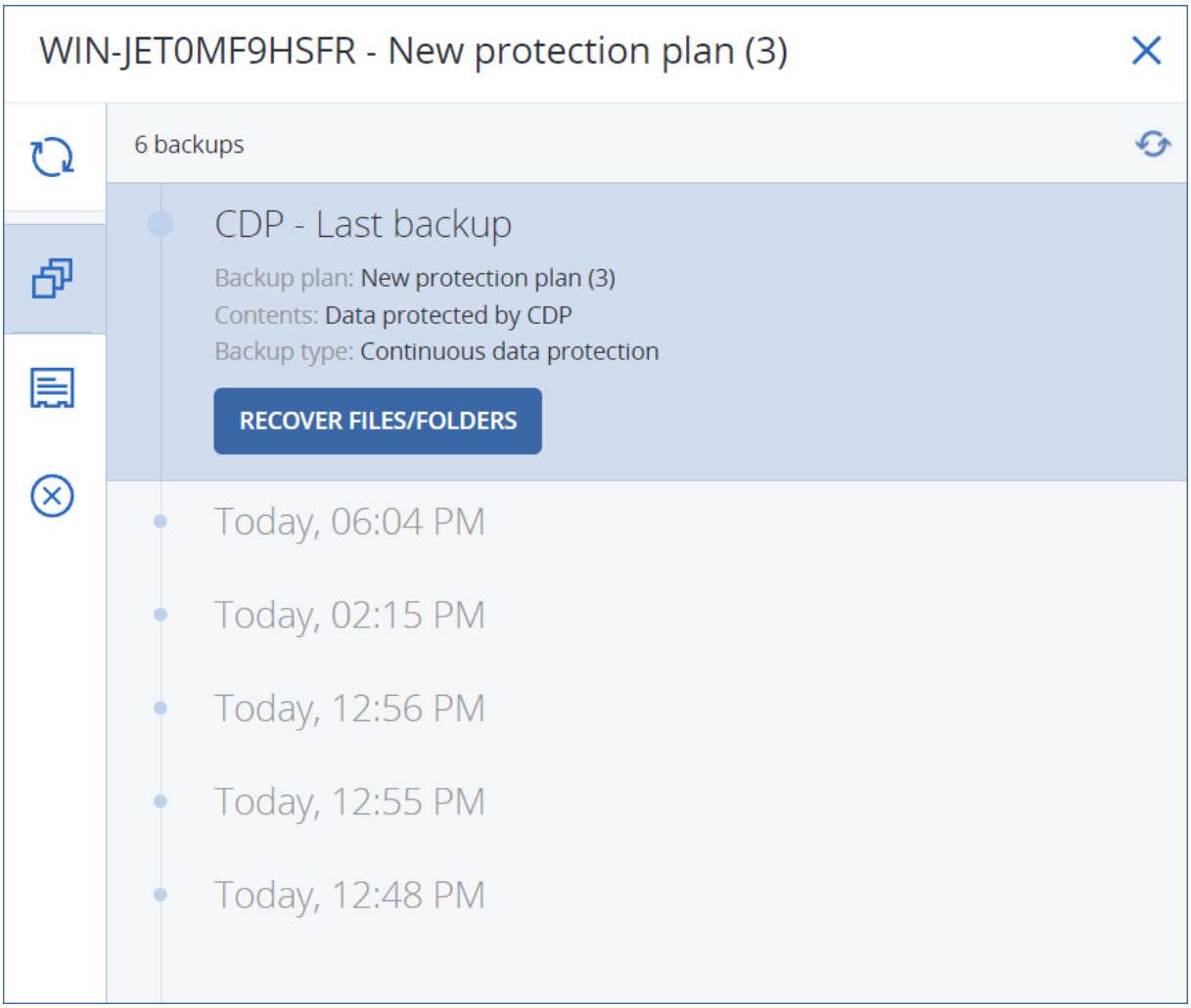
Important
La protection continue des données n'est pas compatible avec l'option **Sauvegarde d'applications**.

Remarque
La protection continue des données empêche la suppression des archives de sauvegarde. Si vous souhaitez supprimer manuellement une sauvegarde créée avec la protection continue des données (CDP) activée, vous devez révoquer ou supprimer le plan de protection correspondant.

Fonctionnement

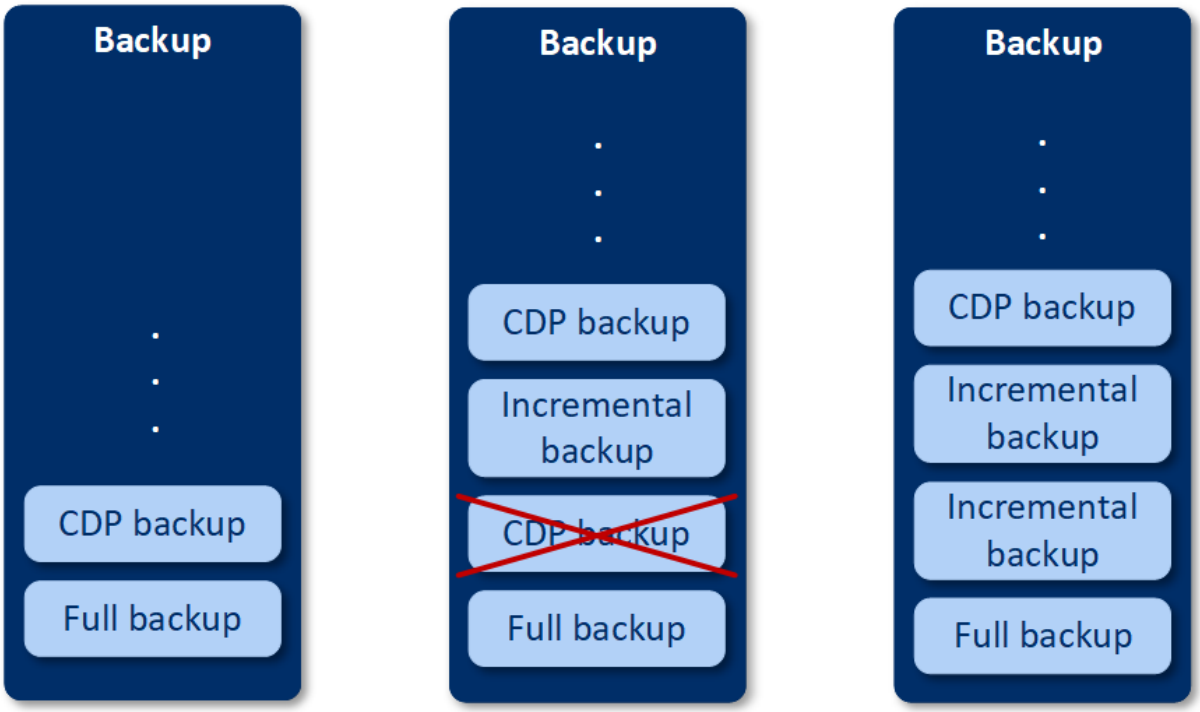
Les modifications apportées aux fichiers et aux dossiers suivis par la protection continue des données sont immédiatement sauvegardées dans une sauvegarde CDP spéciale. Seule une sauvegarde CDP est présente dans un jeu de sauvegarde, et il s'agit toujours de la sauvegarde la plus récente.

© Acronis International GmbH, 2003-2026



Lorsqu'une sauvegarde normale planifiée démarre, la protection continue des données est mise en attente, car les dernières données sont incluses dans la sauvegarde planifiée. Lorsque la sauvegarde planifiée se termine, la protection continue des données reprend, l'ancienne sauvegarde CDP est supprimée, et une nouvelle sauvegarde CDP est créée. Par conséquent, la sauvegarde CDP reste toujours la sauvegarde la plus récente du jeu de sauvegarde et ne stocke que le dernier état des fichiers ou des dossiers suivis.

© Acronis International GmbH, 2003-2026



Si votre ordinateur plante lors d'une sauvegarde normale, la protection continue des données reprend automatiquement au redémarrage de l'ordinateur et crée une sauvegarde CDP au-dessus de la dernière sauvegarde planifiée réussie.

La protection continue des données exige qu'au moins une sauvegarde normale soit créée avant la sauvegarde CDP. Pour cette raison, lorsque vous exécutez un plan de protection avec protection continue des données pour la première fois, une sauvegarde complète est créée, et une sauvegarde CDP est immédiatement ajoutée au-dessus de celle-ci. Si vous activez l'option de **protection continue des données** pour un plan de protection existant, la sauvegarde CDP est ajoutée au jeu de sauvegarde existant.

Remarque
La protection continue des données (CDP) est désactivée par défaut dans les plans de protection nouvellement créés. Elle n'est pas compatible avec l'option **Sauvegarde d'applications** et ne peut pas être activée pour les ordinateurs qui ont cette option activée.

Sources de données prises en charge

Vous pouvez configurer la protection continue des données pour les sources de données suivantes :

- Toute la machine
- Disques/volumes
- Fichiers/dossiers

Après avoir sélectionné la source de données dans la section **Que sauvegarder** du plan de protection, sélectionnez les fichiers, les dossiers ou les applications auxquels appliquer la protection continue des données dans la section **Éléments à protéger continuellement**. Pour en savoir plus

© Acronis International GmbH, 2003-2026

sur la configuration de la protection continue des données, reportez-vous à "Configuration d'une sauvegarde CDP" (p. 569).

Destinations prises en charge

Vous pouvez configurer la protection continue des données pour les destinations suivantes :

- Dossier local
- Dossier réseau
- Stockage dans le Cloud
- Acronis Cyber Infrastructure
- Emplacement défini par un script

Remarque
Seuls les emplacements répertoriés ci-dessus peuvent être définis par un script.

Configuration d'une sauvegarde CDP

Vous pouvez configurer la protection continue des données (CDP) dans le module **Sauvegarde** d'un plan de protection. Pour en savoir plus sur la création d'un plan de protection, reportez-vous à "Création d'un plan de protection" (p. 244).

Pour configurer les paramètres de protection continue des données

1. Dans le module **Sauvegarde** d'un plan de protection, activez le commutateur **Protection continue des données (CDP)**.
   Ce commutateur est disponible uniquement pour les sources de données suivantes :
   - Toute la machine
   - Disque/volumes
   - Fichiers/dossiers
2. Dans **Éléments à protéger continuellement**, configurez la protection continue des données pour **Applications** et/ou **Fichiers/dossiers**.
   - Cliquez sur **Applications** afin de configurer la sauvegarde de protection continue des données pour les fichiers modifiés par des applications spécifiques.
     Vous pouvez sélectionner des applications à partir de catégories prédéfinies ou ajouter d'autres applications en définissant le chemin d'accès à leur fichier exécutable, par exemple :
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`
   - Cliquez sur **Fichiers/dossiers** afin de configurer la sauvegarde de protection continue des données pour les fichiers dans des emplacements spécifiques.
     Vous pouvez définir ces emplacements à l'aide de règles de sélection ou en sélectionnant directement des fichiers et des dossiers.

© Acronis International GmbH, 2003-2026

- [Pour tous les ordinateurs] Pour créer une règle de sélection, servez-vous de la zone de texte.

  Vous pouvez spécifier des chemins d'accès complets aux fichiers ou des chemins d'accès avec des caractères génériques (* et ?). L'astérisque remplace zéro caractère ou plus. Le point d'interrogation remplace un seul caractère.

  Important

  Pour créer une sauvegarde CDP pour un dossier, vous devez spécifier son contenu à l'aide du caractère générique « astérisque » :

  Chemin correct : `D:\Data\*`

  Chemin d'accès incorrect : `D:\Data\`

- [Pour les ordinateurs en ligne] Pour sélectionner des fichiers et des dossiers directement :
  - Dans **Machine à parcourir**, sélectionnez l'ordinateur sur lequel les fichiers ou dossiers se trouvent.
  - Cliquez sur **Sélectionner les fichiers et dossiers** pour parcourir l'ordinateur sélectionné.

    Votre sélection directe crée une règle de sélection. Si vous appliquez le plan de protection à plusieurs ordinateurs et qu'une règle de sélection n'est pas valide pour l'un d'entre eux, elle sera ignorée sur l'ordinateur en question.

3. Dans le volet du plan de protection, cliquez sur **Créer**.

Les données que vous spécifiez seront sauvegardées de manière continue entre les sauvegardes planifiées.

Planification de sauvegarde

Vous pouvez configurer une sauvegarde pour qu'elle s'exécute automatiquement à une heure spécifique, à des intervalles spécifiques ou lors d'un événement spécifique.

Les sauvegardes planifiées pour les ressources autres que de cloud à cloud s'exécutent en fonction des paramètres de fuseau horaire de la ressource sur laquelle l'agent de protection est installé. Par exemple, si vous appliquez le même plan de protection à des ressources dont les paramètres de fuseau horaire sont différents, les sauvegardes démarrent en fonction du fuseau horaire local de chaque ressource.

La planification d'une sauvegarde comprend les actions suivantes :

- Sélection d'un modèle de sauvegarde
- Configuration de l'heure ou sélection de l'événement déclenchant la sauvegarde
- Configuration du paramètre facultatif et des conditions de démarrage

© Acronis International GmbH, 2003-2026

Modèles de sauvegarde

Le modèle de sauvegarde fait partie de la planification du plan de protection ; il définit le type de sauvegarde (complète, différentielle ou incrémentielle) créé, ainsi que le moment de son exécution. Vous pouvez sélectionner l'un des modèles de sauvegarde prédéfinis ou créer un modèle personnalisé.

Les modèles et types de sauvegarde disponibles dépendent de l'emplacement et de la source de la sauvegarde. Par exemple, une sauvegarde différentielle n'est pas disponible lorsque vous sauvegardez les données SQL ou Exchange, ou l'état du système.

Modèle de sauvegarde	Description	Éléments configurables
Toujours incrémentielle (fichier unique)	La première sauvegarde est complète ; elle peut donc prendre un certain temps. Les sauvegardes suivantes seront incrémentielles et considérablement plus rapides. Les sauvegardes utilisent le format de sauvegarde sous forme d'un fichier unique[1]*. Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi. Nous vous recommandons d'utiliser ce modèle lorsque vous stockez vos sauvegardes dans le stockage dans le cloud, car les sauvegardes incrémentielles sont rapides et nécessitent un trafic réseau moindre.	• Type de planification : mensuelle, hebdomadaire, quotidienne, horaire • Déclencheur de sauvegarde : heure ou événement • Heure de démarrage • Conditions de démarrage • Options supplémentaires
Toujours complète	Toutes les sauvegardes de l'ensemble de sauvegarde sont complètes. Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi.	• Type de planification : mensuelle, hebdomadaire, quotidienne, horaire • Déclencheur de sauvegarde : heure ou événement • Heure de démarrage • Conditions de démarrage

[1]Format de sauvegarde, pour lequel les sauvegardes complètes et incrémentielles suivantes sont enregistrées sous forme d'un fichier .tibx unique. Ce format accélère la vitesse de la méthode de sauvegarde incrémentielle, tout en évitant ses principaux inconvénients et la suppression complexe de sauvegardes ayant expiré. Le logiciel définit les blocs de sauvegarde utilisés par des sauvegardes ayant expiré comme étant « libres » et y inscrit les nouvelles sauvegardes. Ce procédé permet un nettoyage extrêmement rapide et une consommation minimale des ressources. Le format de sauvegarde sous forme de fichier unique n'est pas disponible lorsque la sauvegarde est effectuée sur des emplacements qui ne prennent pas en charge les lectures et écritures en accès aléatoire.

© Acronis International GmbH, 2003-2026

Modèle de sauvegarde	Description	Éléments configurables
		• Options supplémentaires
Complète hebdomadaire, incrémentielle journalière	Une sauvegarde complète est créée une fois par semaine et les autres sauvegardes sont incrémentielles. La première sauvegarde est complète et les autres sauvegardes planifiées pendant la semaine sont incrémentielles ; ce cycle se répète ensuite. Pour sélectionner le jour de création de la sauvegarde complète hebdomadaire, cliquez dans le plan de protection sur l'icône représentant un engrenage, puis accédez à **Options de sauvegarde** > **Sauvegarde hebdomadaire**. Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi.	• Déclencheur de sauvegarde : heure ou événement • Heure de démarrage • Conditions de démarrage • Options supplémentaires
Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)	Par défaut, les sauvegardes incrémentielles s'effectuent de manière quotidienne, du lundi au vendredi. Les sauvegardes différentielles sont effectuées tous les samedis. Les sauvegardes complètes sont effectuées le premier jour de chaque mois. **Remarque** Ceci est un schéma personnalisé prédéfini. Dans le plan de protection, il est affiché comme étant **Personnalisé**.	• Modifier la planification existante par type de sauvegarde : ◦ Type de planification : mensuelle, hebdomadaire, quotidienne, horaire ◦ Déclencheur de sauvegarde : heure ou événement ◦ Heure de démarrage ◦ Conditions de démarrage ◦ Options supplémentaires • Ajouter de nouvelles planifications par type de sauvegarde
Personnalisé	Vous devez sélectionner les types de sauvegarde (complète, différentielle et incrémentielle), puis configurer une planification distincte pour chacune	• Modifier la planification existante par type de

© Acronis International GmbH, 2003-2026

Modèle de sauvegarde	Description	Éléments configurables
	d'entre elles*.	sauvegarde : ◦ Type de planification : mensuelle, hebdomadaire, quotidienne, horaire ◦ Déclencheur de sauvegarde : heure ou événement ◦ Heure de démarrage ◦ Conditions de démarrage ◦ Options supplémentaires • Ajouter de nouvelles planifications par type de sauvegarde

* Après avoir créé un plan de protection, vous ne pouvez plus passer du modèle **Toujours incrémentielle (fichier unique)** à l'un des autres modèles de sauvegarde, et inversement. Le modèle **Toujours incrémentielle (fichier unique)** est un modèle de fichier unique et les autres modèles sont des modèles de fichiers multiples. Si vous souhaitez passer d'un format à un autre, créez un plan de protection.

Types de sauvegarde

Les types de sauvegarde suivants sont disponibles :

- Complète : une sauvegarde complète contient toutes les données source. Cette sauvegarde se suffit à elle-même. Pour restaurer les données, vous n'avez pas besoin d'accéder à d'autres sauvegardes.

  Remarque
  La première sauvegarde créée par un plan de protection est toujours une sauvegarde complète.

- Incrémentielle : une sauvegarde incrémentielle stocke les modifications apportées à des données depuis la dernière sauvegarde, qu'elle soit complète, différentielle ou incrémentielle. Pour restaurer les données, vous aurez besoin de toute la chaîne de sauvegardes, jusqu'à la sauvegarde complète initiale, dont dépend la sauvegarde incrémentielle.
- Différentielle : une sauvegarde différentielle stocke les modifications apportées aux données depuis la dernière sauvegarde complète. Pour restaurer les données, vous aurez besoin de la

© Acronis International GmbH, 2003-2026

sauvegarde différentielle et de la sauvegarde complète correspondante dont dépend cette sauvegarde différentielle.

Exécution d'une sauvegarde à partir d'une planification

Pour exécuter une sauvegarde automatiquement, à une heure spécifique ou lors d'un événement spécifique, activez une planification dans le plan de protection.

Pour activer une planification

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Activez le commutateur de planification.
4. Sélectionnez le modèle de sauvegarde.
5. Configurez la planification en fonction de vos besoins, puis cliquez sur **Terminé**.
   Pour plus d'informations sur les options de planification disponibles, voir "Planifier selon l'horaire" (p. 574) et "Planifier par événement" (p. 576).
6. [Facultatif] Configurez les conditions de démarrage ou d'autres options de planification.
7. Enregistrez le plan de protection.

En conséquence, une opération de sauvegarde démarre toutes les heures lorsque les conditions de planification sont satisfaites.

Pour désactiver une planification

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Désactivez le commutateur de planification.
4. Enregistrez le plan de protection.

Par conséquent, la sauvegarde ne s'exécute que si vous la démarrez manuellement.

Remarque
Si la planification est désactivée, les règles de rétention ne sont pas appliquées automatiquement. Pour les appliquer, exécutez la sauvegarde manuellement.

Planifier selon l'horaire

Le tableau suivant récapitule les options de planification basées sur l'heure. La disponibilité de ces options dépend du modèle de sauvegarde. Pour plus d'informations, voir "Modèles de sauvegarde" (p. 571).

Option	Description	Exemples
Mens.	Sélectionnez les mois, les jours du mois ou	Exécuter une sauvegarde le 1er janvier

© Acronis International GmbH, 2003-2026

Option	Description	Exemples
	de la semaine, puis l'heure de début de la sauvegarde.	et le 3 février à 00 h 00. Exécuter une sauvegarde le premier jour de chaque mois à 10 h 00. Exécuter une sauvegarde le 1er mars, le 5 mars, le 1er avril et le 5 avril à 09 h 00. Exécuter une sauvegarde les deuxième et troisième vendredis de chaque mois à 11 h 00. Exécuter une sauvegarde le dernier mercredi du mois à 22 h 30.
Hebdo.	Sélectionnez les jours de la semaine, puis l'heure de début de la sauvegarde.	Exécuter une sauvegarde du lundi au vendredi à 10 h 00. Exécuter une sauvegarde le lundi à 23 h 00. Exécuter une sauvegarde le mardi et le samedi à 08 h 00.
Journ.	Sélectionnez les jours (Tous les jours ou Les jours de la semaine), puis l'heure de début de la sauvegarde.	Exécuter une sauvegarde tous les jours à 11 h 45. Exécuter une sauvegarde du lundi au vendredi à 21 h 30.
Par heure	Sélectionnez les jours de la semaine, puis un intervalle de temps entre deux sauvegardes consécutives, ainsi que la plage de temps au cours de laquelle les sauvegardes s'exécutent. Lorsque vous configurez l'intervalle en minutes, vous pouvez sélectionner un intervalle suggéré entre 10 et 60 minutes, ou indiquer un intervalle personnalisé, par exemple, 45 ou 75 minutes.	Exécuter une sauvegarde toutes les heures entre 08 h 00 et 18 h 00, du lundi au vendredi. Exécuter une sauvegarde toutes les 3 heures entre 01 h 00 et 18 h 00, le samedi et le dimanche.

Options supplémentaires

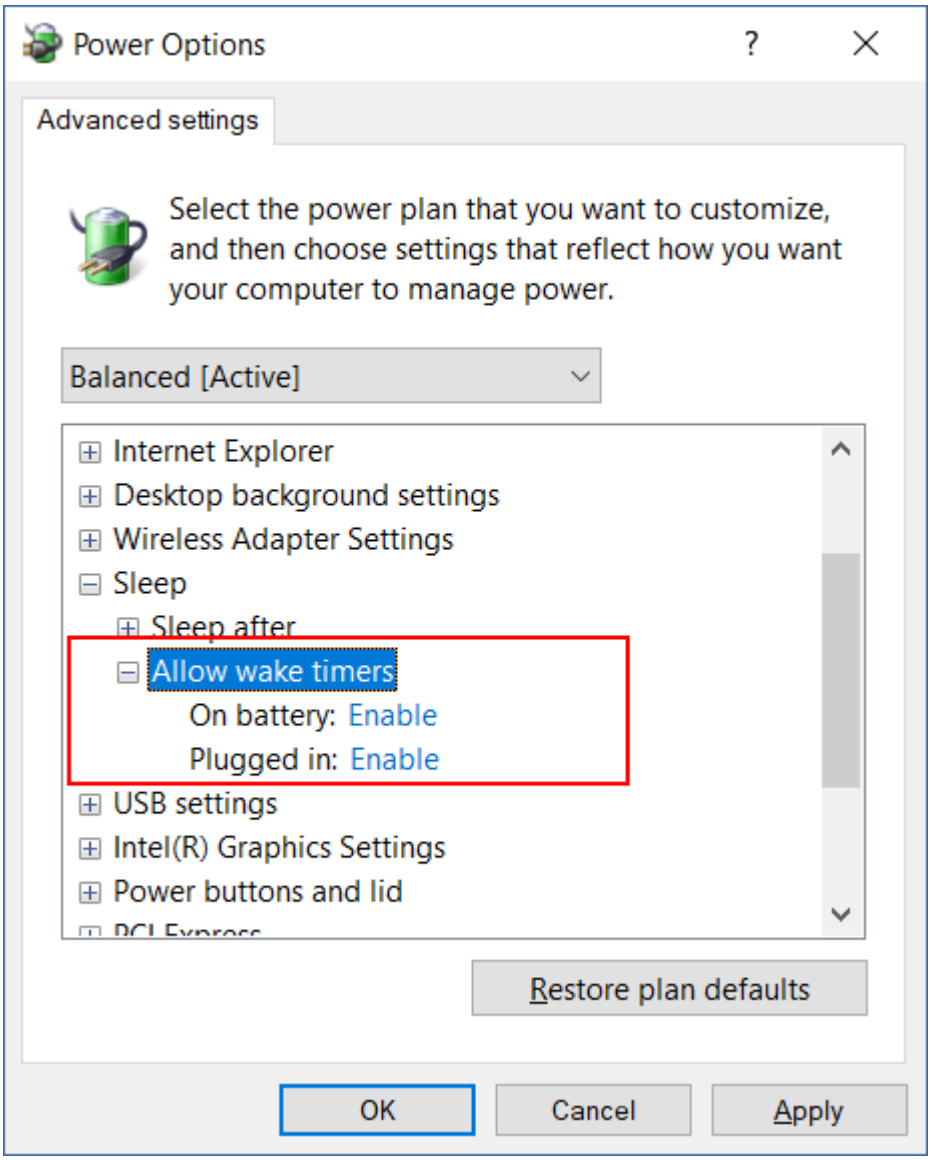
Lorsque vous planifiez une sauvegarde en fonction de l'heure, les options de planification supplémentaires suivantes sont disponibles.

Pour y accéder, cliquez dans le volet **Planification** sur **Afficher plus**.

- **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine**
  Paramètre par défaut : Désactivé.

© Acronis International GmbH, 2003-2026

- **Empêcher l'activation du mode veille ou veille prolongée pendant la sauvegarde**
  Cette option ne s'applique qu'aux ordinateurs exécutant Windows.
  Paramètre par défaut : Activé.
- **Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée**
  Cette option ne s'applique qu'aux ordinateurs exécutant Windows, dans les plans d'alimentation pour lesquels l'option **Autoriser les minuteurs de sortie de veille** est activée.



  Cette option n'utilise pas la fonctionnalité Wake-on-LAN et ne s'applique pas aux ordinateurs éteints.
  Paramètre par défaut : Désactivé.

Planifier par événement

Pour configurer une sauvegarde qui s'exécute lors d'un événement spécifique, sélectionnez l'une des options suivantes.

© Acronis International GmbH, 2003-2026

Option	Description	Exemples
Lors du temps écoulé depuis la dernière sauvegarde	Une sauvegarde démarre après une période spécifiée qui suit la dernière sauvegarde réussie. **Remarque** Cette option dépend du résultat de la sauvegarde précédente. En cas d'échec d'une sauvegarde, la sauvegarde suivante ne démarre pas automatiquement. Dans ce cas, vous devez exécuter la sauvegarde manuellement et veillez à ce qu'elle se termine avec succès pour réinitialiser la planification.	Exécutez une sauvegarde un jour après la dernière sauvegarde réussie. Exécutez une sauvegarde quatre heures après la dernière sauvegarde réussie.
Lorsqu'un utilisateur se connecte au système	Une sauvegarde démarre lorsqu'un utilisateur se connecte à l'ordinateur. Vous pouvez configurer cette option pour toutes les connexions ou pour la connexion d'un utilisateur spécifique. **Remarque** Une connexion à l'aide d'un profil utilisateur temporaire ne démarre pas de sauvegarde.	Exécuter une sauvegarde lorsque l'utilisateur Jean Dupont se connecte.
Lorsqu'un utilisateur se déconnecte du système	Une sauvegarde démarre lorsqu'un utilisateur se déconnecte de l'ordinateur. Vous pouvez configurer cette option pour toutes les déconnexions ou pour la déconnexion d'un utilisateur spécifique. **Remarque** Une déconnexion d'un profil utilisateur temporaire ne démarre pas de sauvegarde. L'arrêt d'un ordinateur ne démarre pas de sauvegarde.	Exécuter une sauvegarde à la déconnexion de chaque utilisateur.
Au démarrage du système	Une sauvegarde s'exécute lorsque la machine protégée démarre.	Exécuter une sauvegarde lorsqu'un utilisateur démarre l'ordinateur.
À l'arrêt du système	Une sauvegarde s'exécute lorsque la machine protégée s'arrête.	Exécuter une sauvegarde lorsqu'un utilisateur arrête l'ordinateur.
Lors d'un	Une sauvegarde s'exécute lors d'un événement Windows que vous spécifiez.	Exécuter une sauvegarde lorsque l'événement 7 de type erreur, avec la

© Acronis International GmbH, 2003-2026

Option	Description	Exemples
événement du Journal des événements Windows		source disque est enregistré dans le journal système Windows.

La disponibilité de ces options dépend de la source de la sauvegarde et du système d'exploitation des ressources protégées. Le tableau ci-dessous répertorie les options disponibles pour Windows, Linux et macOS.

L'événement	Source de sauvegarde (Quoi sauvegarder)					
	Toute la machine, Disques/volumes ou Fichiers/dossiers (machines physiques)	**Toute la machine ou Disques/volumes (machines virtuelles)**	**Configuration ESXi**	**Boîtes aux lettres Microsoft 365**	**Bases de données et boîtes aux lettres Exchange**	**Bases de données SQL**
Lors du temps écoulé depuis la dernière sauvegarde	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Lorsqu'un utilisateur se connecte au système	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Lorsqu'un utilisateur se déconnecte du système	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Au démarrage du système	Windows, Linux, macOS	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
À l'arrêt du système	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Lors d'un événement du Journal des événements Windows	Windows	Sans Objet	Sans Objet	Windows	Windows	Windows

© Acronis International GmbH, 2003-2026

Lors d'un événement du Journal des événements Windows

Vous pouvez exécuter une sauvegarde automatiquement lorsqu'un événement spécifique est enregistré dans un Journal des événements Windows tel que le journal des applications, le journal de sécurité ou le journal système.

Remarque
Vous pouvez parcourir les événements et afficher leurs propriétés dans **Gestion de l'ordinateur** > **Observateur d'événements** sous Windows. Pour ouvrir le journal de sécurité, vous devez disposer des droits d'administrateur.

Paramètres d'événement

Le tableau suivant récapitule les paramètres que vous devez indiquer lors de la configuration de l'option **Lors d'un événement du Journal des événements Windows**.

Paramètre	Description
Nom du journal	Nom du journal. Sélectionnez le nom d'un journal standard (Application, Sécurité ou Système) ou saisissez un autre nom. Par exemple, Sessions Microsoft Office.
Source d'événement	L'événement source indique le programme ou le composant système qui a causé l'événement. Par exemple, disk. Toute source d'événement contenant la chaîne de texte spécifiée déclenchera la sauvegarde planifiée. Cette option n'est pas sensible à la casse. Par exemple, si vous spécifiez `service`, les sources d'événement Gestionnaire de contrôle du service et Time-Service déclencheront toutes les deux une sauvegarde.
Type d'événement	Type de l'événement : Erreur, Avertissement, Information, Succès de l'audit ou Échec de l'audit.
Identifiant d'événement	L'ID d'événement identifie une sorte particulière d'événement dans une source d'événement. Par exemple, un événement Erreur avec la source d'événement disque et l'identifiant d'événement 7 se produit lorsque Windows découvre un bloc défectueux sur un disque, alors qu'un événement Erreur avec la source d'événement disque et l'identifiant d'événement 15 se produit quand un disque n'est pas prêt pour l'accès.

Exemple : Sauvegarde d'urgence en cas de blocs défaillants sur le disque dur

Un ou plusieurs blocs défectueux sur un disque dur indiquent une défaillance imminente. C'est la raison pour laquelle vous souhaiterez peut-être créer une sauvegarde en cas de détection d'un bloc défaillant.

© Acronis International GmbH, 2003-2026

Lorsque Windows détecte un bloc défaillant sur le disque, un événement d'erreur avec la source d'événement disque de et le numéro d'événement 7 est enregistré dans le journal système. Dans le plan de protection, configurez la planification suivante :

- Planification : Lors d'un événement du Journal des événements Windows
- Nom de journal : Système
- Source d'événement : disque
- Type d'événement : Erreur
- ID d'événement : 7

Important
Pour que la sauvegarde s'effectue malgré ces blocs défaillants, accédez à **Options de sauvegarde** > **Gestion erreurs**, puis cochez la case **Ignorer les secteurs défectueux**.

Conditions de démarrage

Pour qu'une sauvegarde s'exécute uniquement si des conditions spécifiques sont remplies, configurez une ou plusieurs conditions de démarrage. Si vous configurez plusieurs conditions, toutes devront être remplies simultanément pour que la sauvegarde puisse démarrer. Vous pouvez spécifier une période après laquelle les sauvegardes s'exécuteront, que les conditions soient remplies ou non. Pour plus d'informations sur cette option de sauvegarde, voir "Conditions de démarrage de tâche" (p. 659).

Les conditions de démarrage ne s'appliquent pas lorsque vous démarrez une sauvegarde manuellement.

Le tableau ci-dessous affiche les conditions de démarrage disponibles pour diverses données sous les systèmes d'exploitation Windows, Linux et macOS.

Condition de démarrage	Source de sauvegarde (Quoi sauvegarder)					
	Toute la machine, Disques/volumes ou Fichiers/dossiers (machines physiques)	**Toute la machine ou Disques/volumes (machines virtuelles)**	**Configuration ESXi**	**Boîtes aux lettres Microsoft 365**	**Bases de données et boîtes aux lettres Exchange**	**Bases de données SQL**
L'utilisateur est inactif	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
L'hôte de l'emplacement de la sauvegarde	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows

© Acronis International GmbH, 2003-2026

Condition de démarrage	Source de sauvegarde (Quoi sauvegarder)					
	Toute la machine, Disques/volumes ou Fichiers/dossiers (machines physiques)	Toute la machine ou Disques/volumes (machines virtuelles)	Configuration ESXi	Boîtes aux lettres Microsoft 365	Bases de données et boîtes aux lettres Exchange	Bases de données SQL
est disponible						
Utilisateurs déconnectés	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Tient dans l'intervalle de temps	Windows, Linux, macOS	Windows, Linux	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Économiser de la batterie	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Ne pas démarrer pendant une connexion mesurée	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet
Vérifier l'adresse IP du terminal	Windows	Sans Objet	Sans Objet	Sans Objet	Sans Objet	Sans Objet

L'utilisateur est inactif

« L'utilisateur est inactif » signifie qu'un écran de veille s'exécute sur la machine ou que la machine est verrouillée.

Exemple

Exécutez une sauvegarde tous les jours à 21 h 00, de préférence lorsque l'utilisateur est inactif. Si l'utilisateur est toujours actif à 23 h 00, exécutez quand même la sauvegarde.

© Acronis International GmbH, 2003-2026

- Planification : **Quotidiennement**, **Exécuter tous les jours**. Démarrage à : **21 h 00**.
- Condition : **L'utilisateur est inactif**.
- Conditions de démarrage de la sauvegarde : **Patienter jusqu'à ce que les conditions soient remplies**, **Lancer quand même la tâche après 2** heures.

En conséquence :

- Si l'utilisateur devient inactif avant 21 h 00, la sauvegarde débute à 21 h 00.
- Si l'utilisateur devient inactif entre 21 h 00 et 23 h 00, la sauvegarde démarre immédiatement.
- Si l'utilisateur est encore actif à 23 h 00, la sauvegarde débute à 23 h 00.

L'hôte de l'emplacement de la sauvegarde est disponible

« L'hôte de l'emplacement de la sauvegarde est disponible » signifie que l'ordinateur hébergeant l'emplacement de la sauvegarde est disponible sur le réseau.

Cette condition s'applique aux dossiers réseau, au stockage dans le cloud et aux emplacements gérés par un nœud de stockage.

Cette condition ne couvre pas la disponibilité de l'emplacement en soi, seulement la disponibilité de l'hôte. Par exemple, si l'hôte est disponible, mais que le dossier du réseau sur cet hôte n'est pas partagé ou que les accréditations pour ce dossier ne sont plus valides, la condition est toujours considérée comme étant remplie.

Exemple

Vous exécutez des sauvegardes dans un dossier réseau tous les jours ouvrés à 21 h 00. Si l'ordinateur qui héberge le dossier n'est pas disponible à ce moment-là (à cause, par exemple, d'un travail de maintenance), ignorez la sauvegarde et attendez le démarrage planifié du jour ouvré suivant.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **L'hôte de l'emplacement de la sauvegarde est disponible**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- Si l'hôte est disponible à 21 h 00, la sauvegarde débute immédiatement.
- Si l'hôte n'est pas disponible à 21 h 00, la sauvegarde débute le jour ouvré suivant (si l'hôte est disponible à 21 h 00 ce jour-là).
- Si l'hôte n'est jamais disponible lors des jours ouvrés à 21 h 00, la sauvegarde ne démarre jamais.

Utilisateurs déconnectés

Utilisez cette condition de démarrage pour reporter une sauvegarde jusqu'à ce que tous les utilisateurs se déconnectent d'un ordinateur Windows.

© Acronis International GmbH, 2003-2026

Exemple

Vous exécutez une sauvegarde tous les vendredis à 20 h 00, de préférence lorsque tous les utilisateurs sont déconnectés. Si l'un des utilisateurs est toujours connecté à 23 h 00, lancer quand même la sauvegarde.

- Planification : **Hebdomadaire**, le vendredi. Démarrage à : **20 h 00**.
- Condition : **Utilisateurs déconnectés**.
- Conditions de démarrage de la sauvegarde : **Patienter jusqu'à ce que les conditions soient remplies**, **Lancer quand même la sauvegarde après 3** heures.

En conséquence :

- Si tous les utilisateurs sont déconnectés à 20 h 00, la sauvegarde débute à 20 h 00.
- Si le dernier utilisateur se déconnecte entre 20 h 00 et 23 h 00, la sauvegarde démarre immédiatement.
- Si des utilisateurs sont encore connectés à 23 h 00, la sauvegarde débute à 23 h 00.

Tient dans l'intervalle de temps

Utilisez cette condition de démarrage pour limiter le début d'une sauvegarde à un intervalle spécifié.

Exemple

Une société sauvegarde des données utilisateur et des serveurs dans différents emplacements d'un même stockage réseau.

Le jour ouvré débute à 08 h 00 et se termine à 17 h 00. Les données utilisateur doivent être sauvegardées dès que les utilisateurs se déconnectent, mais pas avant 16 h 30.

Les serveurs de la société sont sauvegardés tous les jours à 23 h 00. Les données utilisateur doivent être sauvegardées de préférence avant 23 h 00 afin de libérer la bande passante du réseau pour les sauvegardes des serveurs.

La sauvegarde des données utilisateur ne prend pas plus d'une heure ; par conséquent, l'heure de début de la dernière sauvegarde est 22 h 00. Si un utilisateur est toujours connecté dans l'intervalle de temps spécifié, ou se déconnecte à un autre moment, la sauvegarde des données utilisateur doit être ignorée.

- Événement : **Lorsqu'un utilisateur se déconnecte du système**. Spécifiez le compte utilisateur : **Tout utilisateur**.
- Condition : **Tient dans l'intervalle de temps** de **16 h 30** à **22 h 00**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

© Acronis International GmbH, 2003-2026

- Si l'utilisateur se déconnecte entre 16 h 30 et 22 h 00, la sauvegarde démarre immédiatement.
- Si l'utilisateur se déconnecte à un autre moment, la sauvegarde est ignorée.

Économiser de la batterie

Utilisez cette condition de démarrage pour empêcher une sauvegarde si un ordinateur (portable ou tablette, par exemple) n'est pas connecté à une source d'alimentation. En fonction de la valeur de l'option Conditions de démarrage de la sauvegarde, la sauvegarde ignorée démarrera ou ne démarrera pas après la connexion de l'ordinateur à une source d'alimentation.

Les options suivantes sont disponibles :

- **Ne pas démarrer lors d'une alimentation sur batterie**
  Une sauvegarde démarrera uniquement si l'ordinateur est connecté à une source d'alimentation.
- **Démarrer pendant l'alimentation sur batterie si le niveau de batterie est supérieur à**
  Une sauvegarde démarrera si l'ordinateur est connecté à une source d'alimentation ou si le niveau de batterie est supérieur à la valeur spécifiée.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si votre ordinateur n'est pas connecté à une source d'alimentation, il est préférable d'ignorer la sauvegarde pour économiser de la batterie et d'attendre que vous le connectiez à une source d'alimentation.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **Économiser de la batterie**, **Ne pas démarrer lors d'une alimentation sur batterie**.
- Conditions de démarrage de la sauvegarde : **Attendre que les conditions soient satisfaites**.

En conséquence :

- Si l'ordinateur est connecté à une source d'alimentation à 21 h 00, la sauvegarde démarre immédiatement.
- Si l'ordinateur s'exécute sur batterie à 21 h 00, la sauvegarde démarre lorsque vous le connectez à une source d'alimentation.

Ne pas démarrer pendant une connexion mesurée

Utilisez cette condition de démarrage pour empêcher une sauvegarde (y compris une sauvegarde sur un disque local) si l'ordinateur est connecté à Internet via une connexion mesurée dans Windows. Pour plus d'informations sur les connexions mesurées dans Windows, consultez l'article https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

La condition de démarrage supplémentaire **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants** est activée automatiquement lorsque vous activez la condition **Ne pas démarrer pendant une connexion mesurée**. Il s'agit d'une mesure supplémentaire qui empêche

© Acronis International GmbH, 2003-2026

les sauvegardes via une connexion mobile. Les noms de réseaux suivants sont spécifiés par défaut : android, téléphone, mobile et modem.

Pour supprimer ces noms de la liste, cliquez sur le symbole X. Pour ajouter un nouveau nom, saisissez-le dans le champ vide.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si l'ordinateur est connecté à Internet via une connexion mesurée, il est préférable d'ignorer la sauvegarde pour économiser du trafic réseau et d'attendre le démarrage planifié le jour ouvré suivant.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **Ne pas démarrer pendant une connexion mesurée**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- À 21 h 00, si l'ordinateur n'est pas connecté à Internet par l'intermédiaire d'une connexion mesurée, la sauvegarde démarre immédiatement.
- À 21 h 00, si l'ordinateur est connecté à Internet par l'intermédiaire d'une connexion mesurée, la sauvegarde démarre le jour ouvré suivant.
- Si l'ordinateur est toujours connecté à Internet par l'intermédiaire d'une connexion mesurée les jours ouvrés à 21 h 00, la sauvegarde ne démarre jamais.

Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants

Utilisez cette condition de démarrage pour empêcher une sauvegarde (y compris une sauvegarde sur un disque local) si l'ordinateur est connecté à l'un des réseaux sans fil spécifiés (par exemple, si vous souhaitez limiter les sauvegardes via une connexion mobile).

Vous pouvez spécifier les noms des réseaux Wi-Fi, également connus sous le nom de Service Set Identifiers (SSID). La restriction s'applique à tous les réseaux qui contiennent le nom spécifié comme sous-chaîne dans leur nom, quelle que soit la casse. Par exemple, si vous spécifiez `phone` comme nom de réseau, la sauvegarde ne démarrera pas lorsque le ordinateur sera connecté à l'un des réseaux suivants : `John's iPhone`, `phone_wifi` ou `my_PHONE_wifi`.

La condition de démarrage **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants** est activée automatiquement lorsque vous activez la condition **Ne pas démarrer pendant une connexion mesurée**. Les noms de réseaux suivants sont spécifiés par défaut : android, `téléphone`, `mobile` et modem.

Pour supprimer ces noms de la liste, cliquez sur le symbole X. Pour ajouter un nouveau nom, saisissez-le dans le champ vide.

© Acronis International GmbH, 2003-2026

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si l'ordinateur est connecté à Internet via une connexion mobile, il est préférable d'ignorer la sauvegarde et d'attendre le démarrage programmé le jour ouvré suivant.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à : **21 h 00**.
- Condition : **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants**, **Nom du réseau** : `<SSID of the hotspot network>`.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

- Si l'ordinateur n'est pas connecté au réseau spécifié à 21 h 00, la sauvegarde démarre immédiatement.
- Si l'ordinateur est connecté au réseau spécifié à 21 h 00, la sauvegarde démarre le jour ouvré suivant.
- Si l'ordinateur est toujours connecté au réseau spécifié les jours ouvrés à 21 h 00, la sauvegarde ne démarre jamais.

Vérifier l'adresse IP du terminal

Utilisez cette condition de démarrage pour empêcher une sauvegarde (y compris une sauvegarde sur un disque local) si l'une des adresses IP de l'ordinateur est située dans ou en dehors de la plage d'adresses IP spécifiée. Par exemple, vous pouvez éviter les frais élevés de transit de données lors de la sauvegarde d'ordinateurs d'utilisateurs à l'étranger, ou empêcher les sauvegardes sur connexion VPN (Virtual Private Network).

Les options suivantes sont disponibles :

- **Démarrer si en dehors de la plage d'adresses IP**
- **Démarrer si dans la plage d'adresses IP**

Quelle que soit l'option, vous pouvez spécifier plusieurs plages. Prend en charge uniquement les adresses IPv4.

Exemple

Vous sauvegardez vos données tous les jours ouvrés à 21 h 00. Si le terminal est connecté au réseau de l'entreprise via un tunnel VPN, il est préférable d'ignorer la sauvegarde.

- Planification : **Quotidienne**, **Exécuter de lundi à vendredi**. Démarrage à **21 h 00**.
- Condition : **Vérifier l'adresse IP du terminal**, **Démarrer si en dehors de la plage d'adresses IP**, **De** : `<beginning of the VPN IP address range>`, **À** : `<end of the VPN IP address range>`.
- Conditions de démarrage de la sauvegarde : **Attendre que les conditions soient satisfaites**.

En conséquence :

© Acronis International GmbH, 2003-2026

- Si l'adresse IP de l'ordinateur se situe en dehors de la plage spécifiée à 21 h 00, la sauvegarde démarre immédiatement.
- Si l'adresse IP de l'ordinateur se situe dans la plage spécifiée à 21 h 00, la sauvegarde démarre lorsque l'ordinateur obtient une adresse IP non-VPN.
- Si l'adresse IP de l'ordinateur se situe toujours dans la plage spécifiée à 21 h 00, la sauvegarde ne démarre jamais.

Options de planification supplémentaires

Vous pouvez configurer les sauvegardes pour qu'elles s'exécutent uniquement si des conditions spécifiques sont remplies, uniquement pendant une période spécifiée ou avec un retard par rapport à la planification.

Pour configurer des conditions de démarrage

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Dans le volet **Planification**, cliquez sur click **Afficher plus**.
4. Cochez les cases situées à côté des conditions de démarrage que vous souhaitez inclure, puis cliquez sur **Terminé**.
   Pour plus d'informations sur les conditions de démarrage disponibles et sur leur configuration, voir "Conditions de démarrage" (p. 580).
5. Enregistrez le plan de protection.

Pour configurer un intervalle de temps

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Planification**.
3. Cochez la case **Exécuter le plan dans une plage de dates**.
4. Spécifiez la période en fonction de vos besoins, puis cliquez sur **Terminé**.
5. Enregistrez le plan de protection.

Par conséquent, les sauvegardes s'exécuteront uniquement pendant la période spécifiée.

Pour configurer un délai

Afin d'éviter toute charge excessive sur le réseau lorsque vous sauvegardez plusieurs ressources dans un emplacement réseau, un petit délai aléatoire est configuré comme option de sauvegarde. Vous pouvez le désactiver ou modifier son paramètre.

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Options de sauvegarde**, puis sélectionnez **Planification**.
   La valeur de délai de chaque ressource est sélectionnée de façon aléatoire entre zéro et la valeur maximale que vous spécifiez. Par défaut, la valeur maximale est de 30 minutes.
   Pour plus d'informations sur cette option de sauvegarde, voir "Planification" (p. 657)

© Acronis International GmbH, 2003-2026

La valeur du délai pour chaque ressource est calculée lorsque vous appliquez le plan de protection à cette ressource, et reste la même tant que vous n'avez pas modifié la valeur de délai maximal.

3. Spécifiez la période en fonction de vos besoins, puis cliquez sur **Terminé**.
4. Enregistrez le plan de protection.

Exécution manuelle d'une sauvegarde

Vous pouvez exécuter manuellement des sauvegardes planifiées et non planifiées.

Pour exécuter une sauvegarde manuellement

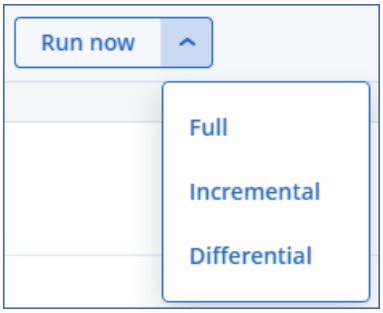
1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Sélectionnez la ressource pour laquelle vous souhaitez exécuter une sauvegarde, puis cliquez sur **Protéger**.
3. Sélectionnez le plan de protection dont vous souhaitez créer la sauvegarde.

   Si aucun plan de protection n'est appliqué à la ressource, appliquez un plan existant ou créez-en un nouveau.

   Pour plus d'informations sur la création d'un plan de protection, voir "Création d'un plan de protection" (p. 244).
4. [Pour créer le type de sauvegarde par défaut] Dans le plan de protection, cliquez sur l'icône **Exécuter maintenant**.



   Vous pouvez également, dans le plan de protection, développer le module **Sauvegarde**, puis cliquer sur le bouton **Exécuter maintenant**.
5. [Pour créer un type de sauvegarde spécifique] Dans le plan de protection, développez le module **Sauvegarde**, cliquez sur la flèche située à côté du bouton **Exécuter maintenant**, puis sélectionnez le type de sauvegarde.



© Acronis International GmbH, 2003-2026

Remarque
La sélection du type n'est pas disponible pour les modèles de sauvegarde qui utilisent une seule méthode de sauvegarde, par exemple, **Toujours incrémentielle (fichier unique)** ou **Toujours complète**.

Par conséquent, l'opération de sauvegarde démarre. Vous pouvez vérifier sa progression et ses résultats dans l'onglet **Terminaux**, colonne **État**.

Règles de rétention

Pour supprimer automatiquement les anciennes sauvegardes, configurez les règles de rétention de sauvegarde dans le plan de protection.

Vous pouvez baser les règles de rétention sur l'une des propriétés de sauvegarde suivantes :

- Numéro
- Âge
- Taille

Les règles de rétention disponibles et leurs options dépendent du schéma de sauvegarde. Les règles s'appliquent également aux agents, aux ressources et aux sauvegardes de cloud à cloud. Pour plus d'informations, voir "Règles de rétention en fonction du modèle de sauvegarde" (p. 590).

Selon la configuration du plan de protection, les règles de rétention sont appliquées à une archive avant ou après une sauvegarde.

Vous pouvez désactiver le nettoyage automatique des anciennes sauvegardes en sélectionnant l'option **Conserver les sauvegardes indéfiniment** lors de la configuration des règles de rétention. L'utilisation du stockage risque d'augmenter et vous devrez supprimer manuellement les anciennes sauvegardes inutiles.

Conseils importants

- Les règles de rétention font partie du plan de protection. Si vous révoquez ou supprimez un plan, ses règles de rétention ne sont plus appliquées. Pour plus d'informations sur la suppression des sauvegardes dont vous n'avez plus besoin, voir "Suppression de sauvegardes" (p. 737).
- Vous pouvez configurer une règle de rétention pour qu'elle s'exécute avant ou après l'opération de sauvegarde, ce qui entraîne un nombre ou une taille différents des sauvegardes conservées.

  Par exemple, dans **Combien conserver** > **Par nombre de sauvegardes**, vous sélectionnez 2. Le tableau suivant compare les résultats de l'application des règles de rétention avant ou après la sauvegarde.

Avant la sauvegarde	Après la sauvegarde
◦ Une opération de nettoyage est exécutée.	◦ Une opération de sauvegarde est exécutée.

© Acronis International GmbH, 2003-2026

Avant la sauvegarde	Après la sauvegarde
Deux sauvegardes sont conservées. ◦ Une opération de sauvegarde est exécutée. Une nouvelle sauvegarde est créée. Résultat : trois sauvegardes sont disponibles.	Une nouvelle sauvegarde est créée. ◦ Une opération de nettoyage est exécutée. Deux sauvegardes sont conservées. Résultat : deux sauvegardes sont disponibles.

- Si, conformément au modèle et au format de sauvegarde, chaque sauvegarde est stockée dans un fichier distinct, vous ne pouvez pas supprimer une sauvegarde dont dépendent d'autres sauvegardes incrémentielles ou différentielles. Cette sauvegarde sera supprimée conformément aux règles de rétention appliquées aux sauvegardes dépendantes. Cette configuration peut entraîner une augmentation de l'utilisation de l'espace de stockage, car la suppression de certaines sauvegardes est reportée. En outre, l'âge, le nombre ou la taille des sauvegardes peuvent dépasser les valeurs que vous avez spécifiées. Pour plus d'informations sur la modification de ce comportement, voir "Consolidation de sauvegarde" (p. 608).
- Par défaut, la dernière sauvegarde créée par un plan de protection n'est jamais supprimée. Toutefois, si vous configurez une règle de rétention pour nettoyer les sauvegardes avant de lancer une nouvelle opération de sauvegarde et que vous définissez le nombre de sauvegardes à conserver sur zéro, la dernière sauvegarde est également supprimée.

Avertissement !
Si vous appliquez cette règle de rétention à un ensemble de sauvegardes ne comportant qu'une seule sauvegarde et que l'opération de sauvegarde échoue, vous ne pourrez pas restaurer vos données, car la sauvegarde existante sera supprimée avant la création d'une nouvelle.

Règles de rétention en fonction du modèle de sauvegarde

Les règles de rétention disponibles et leurs paramètres dépendent du modèle de sauvegarde que vous utilisez dans le plan de protection. Pour plus d'informations sur les modèles de sauvegarde, voir "Modèles de sauvegarde" (p. 571).

Le tableau suivant récapitule les règles de rétention disponibles et leurs paramètres.

Modèle de sauvegarde	Planification	Règles de rétention et paramètres disponibles
Toujours incrémentielle (fichier unique)	Mens. Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires) Conserver les sauvegardes indéfiniment
Toujours complète	Mens.	Par nombre de sauvegardes

© Acronis International GmbH, 2003-2026

Modèle de sauvegarde	Planification	Règles de rétention et paramètres disponibles
	Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par âge des sauvegardes (paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment
Complète hebdomadaire, incrémentielle journalière	Journ. Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes hebdomadaires et quotidiennes) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment
Complète mensuelle, Différentielle hebdomadaire, Incrémentielle quotidienne	Mens. Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes complètes, différentielles et incrémentielles) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment
Personnalisé	Mens. Hebdo. Journ. Par heure Sauvegardes déclenchées par un événement	Par nombre de sauvegardes Par âge des sauvegardes (paramètres distincts pour les sauvegardes complètes, différentielles et incrémentielles) Par volume total de sauvegardes Conserver les sauvegardes indéfiniment

Pourquoi y a-t-il des sauvegardes mensuelles avec un modèle horaire ?

Selon le modèle de sauvegarde, vous pouvez configurer l'option **Par âge des sauvegardes** pour l'une des sauvegardes suivantes :

- Sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires.

  Ces paramètres sont disponibles avec tous les modèles de sauvegarde non personnalisés et sont basés sur le temps. Toutes ces sauvegardes (mensuelles, hebdomadaires, quotidiennes et horaires) sont disponibles, même si vous configurez vos sauvegardes pour qu'elles s'exécutent toutes les heures. Voir l'exemple ci-dessous.

© Acronis International GmbH, 2003-2026

Sauvegarde	Description
Mens.	Une sauvegarde mensuelle correspond à la première sauvegarde de chaque mois.
Hebdo.	Une sauvegarde hebdomadaire correspond à la première sauvegarde du jour de la semaine que vous spécifiez dans l'option Sauvegarde hebdomadaire. Ce jour est considéré comme étant le début de la semaine dans les règles de rétention. Si une sauvegarde hebdomadaire est également la première sauvegarde du mois, elle est considérée comme étant mensuelle. Dans ce cas, une sauvegarde hebdomadaire est créée lors du jour sélectionné de la semaine suivante.
Journ.	Une sauvegarde quotidienne correspond à la première sauvegarde du jour, sauf si elle répond à la définition d'une sauvegarde mensuelle ou hebdomadaire. Dans ce cas, une sauvegarde quotidienne est créée le jour suivant.
Par heure	Une sauvegarde horaire correspond à la première sauvegarde de l'heure, sauf si elle répond à la définition d'une sauvegarde mensuelle, hebdomadaire ou quotidienne. Dans ce cas, une sauvegarde horaire est créée à l'heure suivante.

- Sauvegardes complètes, différentielles et incrémentielles.

  Ces paramètres sont disponibles pour le modèle de sauvegarde **Personnalisé** et sont basés sur la méthode de sauvegarde. Le modèle **Complète mensuelle, Différentielle hebdomadaire, Incrémentielle quotidienne** est un modèle personnalisé préconfiguré.

Exemple

Vous utilisez le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** avec le paramètre par défaut des sauvegardes horaires :

- Planifier selon l'horaire.
- Les sauvegardes s'exécutent toutes les heures : Du lundi au vendredi, toutes les heures, de 08 h 00 à 18 h 00.
- L'option **Sauvegarde hebdomadaire** est définie sur Lundi.

Dans la section **Durée de conservation** du plan de protection, vous pouvez appliquer des règles de rétention à des sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires.

Le tableau suivant récapitule les types de sauvegarde créés pendant une période de 8 jours.

Date	Jour de la semaine	Description
1er juillet	Lundi	La première sauvegarde de chaque mois est mensuelle, si bien que la première sauvegarde du jour est mensuelle. Les

© Acronis International GmbH, 2003-2026

Date	Jour de la semaine	Description
		autres sauvegardes planifiées pendant la journée sont horaires. Cette semaine, la première sauvegarde est considérée comme étant mensuelle. C'est la raison pour laquelle il n'y a pas de sauvegarde hebdomadaire. La première sauvegarde de la semaine suivante sera une sauvegarde hebdomadaire.
2 juillet	Mardi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
3 juillet	Mercredi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
4 juillet	Jeudi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
5 juillet	Vendredi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
6 juillet	Samedi	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
7 juillet	Dimanche	La première sauvegarde est quotidienne ; les autres sauvegardes planifiées pendant la journée sont horaires.
8 juillet	Lundi	La première sauvegarde est hebdomadaire ; les autres sauvegardes planifiées pendant la journée sont horaires.

Configuration des règles de rétention

Les règles de rétention font partie du plan de protection, et leur disponibilité et leurs options dépendent du modèle de sauvegarde. Pour plus d'informations, voir "Règles de rétention en fonction du modèle de sauvegarde" (p. 590).

Pour configurer les règles de rétention

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Cliquez sur **Quantité à conserver**.
3. Sélectionnez l'une des options suivantes :
   - **Par nombre de sauvegardes**
   - **Par âge des sauvegardes**

     Des paramètres distincts pour les sauvegardes mensuelles, hebdomadaires, quotidiennes et horaires sont disponibles. La valeur maximale de tous les types est 9999.

     Vous pouvez également utiliser un seul paramètre pour toutes les sauvegardes.
   - **Par volume total de sauvegardes**

© Acronis International GmbH, 2003-2026

Ce paramètre n'est pas disponible avec le modèle de sauvegarde **Toujours incrémentielle (fichier unique)**.

- **Conserver les sauvegardes indéfiniment**

4. [Si vous n'avez pas sélectionné **Conserver les sauvegardes indéfiniment**] Configurez les valeurs de l'option sélectionnée.
5. [Si vous n'avez pas sélectionné **Conserver les sauvegardes indéfiniment**] Sélectionnez le moment où les règles de rétention sont appliquées :
   - Après la sauvegarde
   - Avant la sauvegarde

     Cette option n'est pas disponible lors de la sauvegarde de clusters Microsoft SQL Server ou Microsoft Exchange Server.
6. Cliquez sur **Terminé**.
7. Enregistrez le plan de protection.

Réplication

Avec la réplication, chaque nouvelle sauvegarde est automatiquement copiée dans un emplacement de réplication. Les sauvegardes de l'emplacement de réplication ne dépendent pas des sauvegardes de l'emplacement source, et vice versa.

Seule la dernière sauvegarde de l'emplacement source est répliquée. Toutefois, si des sauvegardes antérieures ne sont pas répliquées (par exemple, en raison d'un problème de connexion réseau), l'opération de réplication inclura toutes les sauvegardes créées après la dernière réplication réussie.

Si une opération de réplication est interrompue, les données traitées seront utilisées par l'opération de réplication suivante.

Remarque
Cette rubrique décrit la réplication dans le cadre d'un plan de protection. Vous pouvez également créer un plan de réplication des sauvegardes distinct. Pour plus d'informations, voir "Réplication de sauvegarde" (p. 255).

Exemples d'utilisation

- Garantir une restauration fiable

  Stockez vos sauvegardes à la fois sur site (pour une restauration immédiate) et hors site (pour garantir que les sauvegardes restent en sécurité même en cas de défaillance du stockage ou de catastrophe naturelle affectant le site principal).
- Utiliser le stockage cloud pour protéger les données en cas de catastrophe naturelle

  Répliquer les sauvegardes vers le stockage sur le Cloud en transférant uniquement les modifications de données.
- Conserver seulement les points de restauration les plus récents

© Acronis International GmbH, 2003-2026

Configurez des règles de rétention pour supprimer les anciennes sauvegardes d'un stockage rapide, afin d'économiser sur les coûts de stockage.

Emplacements pris en charge

Emplacement	En tant qu'emplacement de la source	En tant qu'emplacement de réplication
Dossier local	+	+
Dossier réseau	+	+
Stockage dans le Cloud	-*	+
Secure Zone	+	+
Cloud public	- *	+

*La réplication depuis un cloud public est disponible uniquement dans les plans de traitement des données hors hôte. Voir "Emplacements pris en charge pour le traitement des données hors hôte" (p. 258).

Pour activer la réplication

1. Dans un plan de protection, développez le module **Sauvegarde**, puis cliquez sur **Ajouter un emplacement**.

   Remarque
   L'option **Ajouter un emplacement** n'est pas disponible lorsque vous sélectionnez le stockage dans le cloud dans **Où sauvegarder**.

2. Dans la liste des emplacements disponibles, sélectionnez l'emplacement de réplication.
   L'emplacement apparaît dans le plan de protection en tant que **2e emplacement**, **3e emplacement**, **4e emplacement** ou **5e emplacement**, en fonction du nombre d'emplacements ajoutés pour la réplication.
3. [Facultatif] Cliquez sur l'icône en forme d'engrenage pour configurer les options de l'emplacement de réplication.
   - **Performance et créneau de sauvegarde** – définir la fenêtre de sauvegarde pour l'emplacement sélectionné, comme décrit dans "Performance et créneau de sauvegarde" (p. 645). Ces paramètres définissent les performances de réplication.
   - **Supprimer l'emplacement** : supprime l'emplacement de réplication actuellement sélectionné.
   - [Uniquement pour le stockage dans le cloud] **Envoi de données physiques** – enregistrer la sauvegarde initiale sur un périphérique de stockage amovible et l'expédier pour qu'elle soit transférée vers le stockage dans le cloud, au lieu de la répliquer via Internet.
     Cette option convient aux emplacements où la connexion réseau est lente ou lorsque vous souhaitez économiser de la bande passante lors de transferts de fichiers volumineux sur le

© Acronis International GmbH, 2003-2026

réseau. L'activation de l'option ne nécessite pas de quotas de service avancés pour Cyber Protect, mais vous aurez besoin d'un quota de service d'envoi de données physiques pour créer un ordre d'expédition et en assurer le suivi. Voir "Envoi de données physiques" (p. 649).

Remarque
Cette option est prise en charge avec l'agent de protection à partir de la version C21.06.

4. [Facultatif] Dans la ligne **Combien conserver** sous l'emplacement de réplication, configurez les règles de rétention pour cet emplacement, comme décrit dans "Règles de rétention" (p. 589).
5. [Facultatif] Répétez les étapes 1 à 4 pour ajouter d'autres emplacements de réplication.
   Vous pouvez configurer jusqu'à quatre emplacements de réplication (**2e emplacement**, **3e emplacement**, **4e emplacement** et **5e emplacement**). Si vous sélectionnez le **stockage dans le cloud**, vous ne pouvez pas ajouter d'autres emplacements de réplication.

Important
Si vous activez la sauvegarde et la réplication dans le même plan de protection, assurez-vous que la réplication se termine avant la prochaine sauvegarde planifiée. Si la réplication est toujours en cours, la sauvegarde planifiée ne démarrera pas. Par exemple, une sauvegarde planifiée exécutée une fois toutes les 24 heures ne démarrera pas si l'exécution de la réplication dure 26 heures.

Pour éviter cette dépendance, utilisez un plan séparé pour la réplication de sauvegarde. Pour plus d'informations sur ce plan spécifique, voir "Réplication de sauvegarde" (p. 255).

Chiffrement

Cyber Protect utilise deux niveaux de sécurité pour protéger les données sauvegardées contre tout accès non autorisé.

Les données sauvegardées sont chiffrées avec une clé de 256 bits, qui est à son tour chiffrée en utilisant le hachage SHA-2 (256 bits) d'un mot de passe de chiffrement fourni par l'utilisateur comme clé, comme suit :

1. Lors de la création d'un plan de protection avec chiffrement activé, l'utilisateur spécifie un mot de passe de chiffrement.

   Avertissement !
   Cyber Protect ne stocke pas ce mot de passe. La restauration d'un mot de passe perdu n'est pas possible.

2. La fonction de dérivation de clé basée sur un mot de passe 2 (PBKDF2) est appliquée au mot de passe de chiffrement fourni par l'utilisateur 1 048 576 fois (2 à la puissance 20). En conséquence, un hachage SHA-2 (256 bits) est créé. C'est la première clé, qui est utilisée pour chiffrer la deuxième clé.
3. Une clé aléatoire de 256 bits est créée à l'aide d'OpenSSL. Il s'agit de la deuxième clé, qui est utilisée pour chiffrer les données sauvegardées.

© Acronis International GmbH, 2003-2026

4. La deuxième clé est chiffrée à l'aide de l'AES (AES-256) et du hachage dérivé du mot de passe de chiffrement fourni par l'utilisateur.
5. La seconde clé chiffrée est ajoutée à l'archive de sauvegarde.
6. Les données sauvegardées sont chiffrées à l'aide de l'AES avec le mode Galois/Compteur (AES-256 GCM) et la deuxième clé.
7. Lors de la restauration de données, l'utilisateur doit fournir le mot de passe de chiffrement. Le hachage de ce mot de passe est la première clé de chiffrement. Cette clé est utilisée pour déchiffrer la seconde clé. Avec la seconde clé, l'archive de sauvegarde peut être déchiffrée et restaurée.

Remarque
L'utilisation de l'algorithme AES-256 avec un mot de passe fort offre un chiffrement de cryptographie post-quantique qui protège des attaques cryptanalytiques reposant sur l'informatique quantique.

Nous vous recommandons de chiffrer toutes les sauvegardes stockées dans le stockage sur le Cloud, en particulier si votre société est soumise à la conformité réglementaire.

Vous pouvez configurer le chiffrement comme suit :

- Dans le plan de protection
- En tant que propriété de l'ordinateur, à l'aide de Cyber Protect Monitor ou de l'interface de ligne de commande

Configuration du chiffrement dans le plan de protection

Dans un plan de protection, le chiffrement est activé par défaut. L'algorithme AES-256 est utilisé.

Avec un mot de passe fort, l'algorithme AES-256 fournit un chiffrement de cryptographie post-quantique.

Pour les comptes en mode de Conformité, vous ne pouvez pas configurer le chiffrement dans le plan de protection. Pour plus d'informations sur la configuration du chiffrement sur le terminal protégé, voir "Configuration du chiffrement en tant que propriété de l'ordinateur" (p. 598).

Pour configurer le chiffrement

1. Dans un plan de protection, développez le module **Sauvegarde**.
2. Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
3. Indiquez et confirmez le mot de passe de chiffrement.
4. Cliquez sur **OK**.

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

© Acronis International GmbH, 2003-2026

Vous ne pouvez pas modifier les paramètres de chiffrement après avoir appliqué le plan de protection. Pour utiliser d'autres paramètres de chiffrement, créez un nouveau plan.

Configuration du chiffrement en tant que propriété de l'ordinateur

Vous pouvez configurer le chiffrement de sauvegarde en tant que propriété de l'ordinateur. Dans ce cas, le chiffrement n'est pas configuré dans le plan de protection, mais sur la ressource protégée. Le chiffrement en tant que propriété de l'ordinateur utilise l'algorithme AES avec une clé de 256 bits (AES-256).

Remarque
L'utilisation de l'algorithme AES-256 avec un mot de passe fort offre un chiffrement de cryptographie post-quantique qui protège des attaques cryptanalytiques reposant sur l'informatique quantique.

La configuration du chiffrement en tant que propriété de l'ordinateur affecte les plans de protection de la manière suivante :

- **Plans de protection déjà appliqués à la machine.** Si les paramètres de chiffrement d'un plan de protection sont différents, les sauvegardes échouent.
- **Plans de protection appliqués à l'ordinateur ultérieurement.** Les paramètres de chiffrement sauvegardés sur l'ordinateur remplacent les paramètres de chiffrement dans le plan de protection. Toute sauvegarde est chiffrée, même si le chiffrement est désactivé dans les paramètres du module de sauvegarde.

Pour les comptes en mode de Conformité, seul le chiffrement en tant que propriété de la machine est disponible.

Si vous avez plusieurs agents pour VMware connecté au même vCenter Server, et que vous configurez le chiffrement comme une propriété de l'ordinateur, vous devez utiliser le même mot de passe de chiffrement sur tous les ordinateurs avec l'agent pour VMware, en raison de l'équilibrage de la charge entre les agents.

Vous pouvez configurer le chiffrement en tant que propriété de l'ordinateur de la manière suivante :

- Sur la ligne de commande
- Dans Cyber Protect Monitor (disponible pour Windows et macOS)

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Pour configurer le chiffrement en tant que propriété de l'ordinateur

Sur la ligne de commande

1. Connectez-vous en tant qu'administrateur sous Windows ou en tant qu'utilisateur root (superutilisateur) sous Linux.
2. Accédez à l'outil **acropsh** comme suit :

© Acronis International GmbH, 2003-2026

- Pour Windows :

```
<installation_path>\PyShell\bin\
```

Où <installation_path> est %ProgramFiles%\BackupClient.

- Pour Linux :

```
/usr/sbin/
```

- Pour une appliance virtuelle :

```
/./sbin/
```

3. [Pour spécifier le mot de passe dans la ligne de commande]
   - Exécuter la commande suivante :
     - Pour Windows

```
acropsh.exe -m manage_creds --set-password
```

     - Pour Linux et appliance virtuelle

```
acropsh -m manage_creds --set-password
```

   - À l'invite interactive, spécifiez le mot de passe de chiffrement.
4. [Pour spécifier le mot de passe à l'aide d'un fichier]
   - Préparez un fichier texte dans lequel vous spécifiez le mot de passe de chiffrement.
     Le fichier doit avoir le contenu suivant :

```
--set-password <password>
```

     Où <password> est le mot de passe de chiffrement.

     Avertissement !
     Pour des raisons de sécurité, assurez-vous que seul vous pouvez accéder à ce fichier.
     Supprimez le fichier après avoir terminé cette procédure.

   - Dans la ligne de commande, exécutez la commande suivante :
     - Pour Windows

```
acropsh.exe -m manage_creds @<file_path>
```

     - Pour Linux et appliance virtuelle

```
acropsh -m manage_creds @<file_path>
```

     Où <file_path> est le chemin d'accès complet au fichier dans lequel le mot de passe est

© Acronis International GmbH, 2003-2026

spécifié.

Par exemple, `/home/JohnDoe/MyFile.txt` ou `C:\Users\JohnDoe\MyFile.txt`.

Dans Cyber Protect Monitor

1. Connectez-vous en tant qu'administrateur.
2. Cliquez sur l'icône Cyber Protect Monitor dans la zone de notification (dans Windows) ou la barre de menus (dans macOS).
3. Cliquez sur l'icône en forme d'engrenage, puis cliquez sur **Paramètres** > **Chiffrement**.
4. Sélectionnez **Définir un mot de passe pour cet ordinateur**, puis spécifiez et confirmez le mot de passe de chiffrement.
5. Cliquez sur **Enregistrer**.

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Pour réinitialiser les paramètres de chiffrement

1. Connectez-vous en tant qu'administrateur sous Windows ou en tant qu'utilisateur root (superutilisateur) sous Linux.
2. Accédez à l'outil **acropsh** comme suit :
   - Pour Windows :

     ```
     <installation_path>\PyShell\bin\
     ```

     Où `<installation_path>` est `%ProgramFiles%\BackupClient`.
   - Pour Linux :

     ```
     /usr/sbin/
     ```

   - Pour une appliance virtuelle :

     ```
      /./sbin/
     ```

3. Exécuter la commande suivante :
   - Pour Windows

     ```
     acropsh.exe -m manage_creds --reset
     ```

   - Pour Linux et appliance virtuelle

     ```
     acropsh -m manage_creds --reset
     ```


© Acronis International GmbH, 2003-2026

Important
Si vous réinitialisez le chiffrement en tant que propriété de l'ordinateur ou changez le mot de passe de chiffrement après la création d'une sauvegarde par un plan de protection, l'opération de sauvegarde suivante échoue. Pour continuer à sauvegarder la ressource, créez un nouveau plan de protection.

Notarisation

La notarisation vous permet de prouver qu'un fichier est authentique et inchangé depuis sa sauvegarde. Nous vous recommandons d'activer la notarisation lors de la sauvegarde de vos fichiers juridiques ou tout autre fichier requérant une authentification.

La notarisation est disponible uniquement pour les sauvegardes au niveau du fichier. Les fichiers avec une signature numérique sont ignorés, car ils n'ont pas besoin d'être notariés.

La notarisation *n'est pas* disponible :

- Si le format de sauvegarde est défini sur **Version 11**
- Si la destination de sauvegarde est Secure Zone

Comment utiliser la notarisation

Pour activer la notarisation de tous les fichiers sélectionnés pour la sauvegarde (à l'exception des fichiers avec une signature numérique), activez le commutateur **Notarisation** lors de la création d'un plan de protection.

Lors de la configuration de la restauration, les fichiers notariés seront marqués d'une icône spéciale. Vous pourrez ainsi vérifier l'authenticité du fichier.

Fonctionnement

Lors d'une sauvegarde, l'agent calcule les code de hachage des fichiers sauvegardés, crée un arbre de hachage (basé sur la structure du dossier), enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données blockchain Ethereum pour s'assurer que cette valeur ne change pas.

Lors de la vérification de l'authenticité d'un fichier, l'agent calcule le hachage du fichier, puis le compare avec le hachage stocké dans l'arbre de hachage sauvegardé. Si ces hachages ne correspondent pas, le fichier n’est pas authentique. Sinon, l'authenticité du fichier est garantie par l'arbre de hachage.

Pour vérifier que l'arbre de hachage n'a pas été compromis, l'agent envoie la racine de l'arbre de hachage au service Notary. Le service Notary la compare avec celle stockée dans la base de données blockchain. Si les hachages correspondent, le fichier sélectionné est authentique. Sinon, le logiciel affiche un message indiquant que le fichier n’est pas authentique.

© Acronis International GmbH, 2003-2026

Options de sauvegarde par défaut

Les valeurs par défaut des options de sauvegarde existent aux niveaux de la société, de l'unité et de l'utilisateur. Lorsqu'une unité ou un compte utilisateur sont créés au sein d'une société ou d'une unité, ils héritent des valeurs par défaut pour la société ou l'unité.

Les administrateurs de la société, les administrateurs de l'unité et tous les utilisateurs ne disposant pas de droits d'administrateur peuvent modifier une valeur d'option par défaut en utilisant la valeur prédéfinie. La nouvelle valeur sera utilisée par défaut pour tous les plans de protection que vous créerez à leur niveau respectif après la prise d'effet de la modification.

Lors de la création d'un plan de protection, un utilisateur peut remplacer une valeur par défaut par une valeur personnalisée qui sera spécifique à ce plan.

Pour changer une valeur d'option par défaut

1. Effectuez l'une des actions suivantes :
   - Pour modifier la valeur par défaut pour la société, connectez-vous à la console Cyber Protect en tant qu'administrateur de la société.
   - Pour modifier la valeur par défaut d'une unité, connectez-vous à la console Cyber Protect en tant qu'administrateur de l'unité.
   - Pour modifier la valeur par défaut pour vous-même, connectez-vous à la console Cyber Protect à l'aide d'un compte qui ne dispose pas des droits d'administrateur.
2. Cliquez sur **Paramètres** > **Paramètres système**.
3. Développez la section **Options de sauvegarde par défaut**.
4. Sélectionnez l'option, puis effectuez les modifications nécessaires.
5. Cliquez sur **Enregistrer**.

Options de sauvegarde

Pour modifier les options de sauvegarde d'un plan de protection, accédez au module **Sauvegarde**, puis cliquez dans le champ **Options de sauvegarde** sur **Modifier**.

Disponibilité des options de sauvegarde

L'ensemble des options de sauvegarde disponibles dépendent des éléments suivants :

- l'environnement dans lequel l'agent fonctionne (Windows, Linux, macOS) ;
- le type de données en cours de sauvegarde (disques, fichiers, machines virtuelles, données d'application) ;
- la destination de la sauvegarde (dossier réseau, local ou stockage sur le Cloud).

Le tableau suivant résume la disponibilité des options de sauvegarde.

© Acronis International GmbH, 2003-2026

La colonne « Autre » sous « Machines virtuelles (sauvegarde sans agent) » contient des informations agrégées pour tous les hyperviseurs pris en charge qui ne disposent pas d'une colonne dédiée dans le tableau :

- Virtuozzo Hybrid Server
- Virtuozzo Hybrid Infrastructure
- Scale Computing
- oVirt
- Proxmox VE
- Nutanix AHV

Les exceptions dans le support des fonctionnalités sont listées en notes de bas de page sous le tableau.

Option	Sauvegarde au niveau disque			Sauvegarde au niveau fichier			Machines virtuelles (Sauvegarde sans agent)				SQL et Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Azure	Autre	Windows
Alertes	+	+	+	+	+	+	+	+	-	+	+
Points de restauration Azure : rétention	-	-	-	-	-	-	-	-	+	-	-
Points de restauration Azure : niveau de cohérence	-	-	-	-	-	-	-	-	+	-	-
Points de restauration Azure : gestion des disques non pris en charge	-	-	-	-	-	-	-	-	+	-	-
Consolidation de sauvegarde	+	+	+	+	+	+	+	+	-	+	-
Nom de fichier de la sauvegarde	+	+	+	+	+	+	+	+	+	+	+
Format de la sauvegarde	+	+	+	+	+	+	+	+	-	+	+
Validation de la	+	+	+	+	+	+	+	+	-	+	+

© Acronis International GmbH, 2003-2026

sauvegarde											
Suivi des blocs modifiés (CBT)	+	-	-	-	-	-	+	+	-	+ [1]	-
Mode de sauvegarde de cluster	-	-	-	-	-	-	-	-	-	-	+
Niveau de compression	+	+	+	+	+	+	+	+	+	+	+
Gestion erreurs											
Réessayer si une erreur se produit	+	+	+	+	+	+	+	+	+	+	+
Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux)	+	+	+	+	+	+	+	+	+	+	+
Ignorer les secteurs défectueux	+	-	+	+	-	+	+	+	+	+	-
Réessayer si une erreur se produit lors de la création d'instantané de MV	-	-	-	-	-	-	+	+	+	+	-
Sauvegarde incrémentielle/différentielle rapide	+	+	+	-	-	-	-	-	-	-	-
Instantané de sauvegarde de niveau fichier	-	-	-	+	+	+	-	-	-	-	-
Filtres de fichiers	+	+	+	+	+	+	+	+	+	+	-
Données d'investigation	+	-	-	-	-	-	-	-	-	-	-
Troncation de journal	-	-	-	-	-	-	+	+	-	-	SQL uniquement
Prise d'instantanés LVM	-	+	-	-	-	-	-	-	-	-	-

© Acronis International GmbH, 2003-2026

Points de montage	-	-	-	+	-	-	-	-	-	-	-
Snapshot Multi-volume	+	+	-	+	+	-	-	-	-	-	-
Restauration en un seul clic	+	+	-	-	-	-	-	-	-	-	-
Performance et créneau de sauvegarde	+	+	+	+	+	+	+	+	-	+	+
Envoi de données physiques	+	+	+	+	+	+	+	+	-	+	-
Commandes Pré/Post	+	+	+	+	+	+	+[2]	+	-	+	+
Commandes de capture de données Pré/Post	+	+	+	+	+	+	+	-	-	-	+
Planification											
Répartir les heures de démarrage dans une fenêtre de temps	+	+	+	+	+	+	+	+	-	+	+
Limiter le nombre de sauvegardes simultanées	-	-	-	-	-	-	+	+	-	+	-
Sauvegarde secteur par secteur	+	+	-	-	-	-	+	+	+	+	-
Fractionnement	+	+	+	+	+	+	+	+	-	+	+
Traitement de l'échec de tâche	+	+	+	+	+	+	+	+	-	+	+
Conditions de démarrage de tâche	+	+	-	+	+	-	+	+	-	+	+
Service de cliché instantané des volumes	+	-	-	+	-	-	-	+	-	-	+
Service de cliché instantané des	-	-	-	-	-	-	+	+	-	+	-

© Acronis International GmbH, 2003-2026

volumes (VSS) pour les machines virtuelles											
Sauvegarde hebdomadaire	+	+	+	+	+	+	+	+	+	+	+
Journal des événements Windows	+	-	-	+	-	-	+	+	-	-	+

[1] Non pris en charge dans oVirt.

[2] Pris en charge uniquement lorsque l'Agent pour VMware est installé directement sur l'hôte ESXi. Non pris en charge dans les configurations basées sur une appliance, par exemple lors de l'utilisation avec l'Agent pour VMware (appliance virtuelle).

Alertes

Aucune sauvegarde réussie sur plusieurs jours d'affilée

Le préréglage est le suivant : **Désactivé**.

Cette option permet de déterminer s'il faut ou non générer une alerte lorsque le plan de protection n'a créé aucune sauvegarde pendant une période définie. Outre les échecs de sauvegarde, le logiciel fait le compte des sauvegardes qui n'ont pas été exécutées à l'heure prévue (sauvegardes manquées).

Les alertes sont générées sur une base « par machine » et sont affichées sous l'onglet **Alertes**.

Vous pouvez spécifier le nombre de jours consécutifs sans sauvegarde après lesquels l'alerte est générée.

Points de restauration Azure

Trois options de sauvegarde Microsoft Azure sont disponibles lors de la configuration de la sauvegarde sans agent des machines virtuelles Microsoft Azure :

- Points de restauration Azure : rétention
- Points de restauration Azure : niveau de cohérence
- Points de restauration Azure : gestion des disques non pris en charge

Points de restauration Azure : rétention

Cette option vous permet de définir le nombre de points de restauration Microsoft Azure à conserver après une sauvegarde (la valeur par défaut est de 3). Ces points de restauration améliorent les performances des sauvegardes incrémentielles qui utilisent la fonction Changed Block Tracking (CBT).

© Acronis International GmbH, 2003-2026

Le nombre maximal de points de restauration Azure que vous pouvez conserver est de 200 (recommandation de Microsoft), et il ne doit y avoir qu'une seule collecte de points de restauration créée pour chaque machine virtuelle.

Lors de la restauration sur la machine virtuelle Microsoft Azure d'origine, à partir d'une sauvegarde pour laquelle le point de restauration Azure correspondant est toujours disponible dans Microsoft Azure, le processus de restauration utilise ce point de restauration pour rétablir automatiquement l'état de la machine virtuelle, au lieu de récupérer les données à partir du fichier de sauvegarde. Cela permet d'optimiser le trafic et les performances de la restauration.

Notez que la logique de rotation des points de restauration est gérée par le plan de protection. Si deux plans sont appliqués à la même machine virtuelle, chaque plan traite tous les points de restauration de la collection comme les siens et fait tourner les sauvegardes selon la valeur **Points de restauration** définie.

Points de restauration Azure : niveau de cohérence

Cela vous permet de sélectionner le niveau de cohérence des points de restauration, tels que les points de restauration cohérents d'application ou les points de restauration cohérents du système de fichiers.

Remarque
Cette option s'applique uniquement aux machines virtuelles qui sont sous tension.

Vous pouvez sélectionner l'une des options suivantes :

- **Exiger des points de restauration cohérents avec l'application** : si le point de restauration n'est pas cohérent avec l'application, la sauvegarde échouera.

  Notez que les points de restauration de machines virtuelles prennent en charge la cohérence des applications pour les machines virtuelles exécutant des systèmes d'exploitation Windows, et la cohérence des systèmes de fichiers pour les machines virtuelles exécutant des systèmes d'exploitation Linux. Les points de restauration cohérents pour les applications utilisent des enregistreurs VSS (ou des scripts de prétraitement/post-traitement pour Linux) pour garantir la cohérence des données de l'application avant la création d'un point de restauration.
- **Avertissement sur les points de restauration cohérents du système de fichiers ou en cas de plantage** : si le point de restauration est cohérent au niveau du système de fichiers ou en cas de plantage, la sauvegarde s'effectue avec un avertissement.

  Cette option ajoute un avertissement au journal et marque l'activité avec un avertissement si le niveau de cohérence de l'instantané est cohérent au niveau du système de fichiers et en dessous (cohérent en cas de plantage).
- **Avertissement sur les points de restauration cohérents en cas de plantage** : si le point de restauration est cohérent en cas de plantage, la sauvegarde s'effectue avec un avertissement. Les points de restauration cohérents au niveau du système de fichiers et de l'application ne déclenchent pas d'avertissement. Cette option est sélectionnée par défaut.

  Cette option ajoute un avertissement au journal et marque l'activité avec un avertissement.

© Acronis International GmbH, 2003-2026

- **Ignorer le niveau de cohérence** : quel que soit le niveau de cohérence du point de restauration, la sauvegarde s'effectuera avec succès.

  Cette option ajoute un message d'informations au journal et exécute le plan de protection avec succès.

Points de restauration Azure : gestion des disques non pris en charge

Cette option vous permet de déterminer l'action à effectuer si une machine virtuelle avec un disque non géré, partagé ou éphémère est sauvegardée. Notez que ces types de disques ne sont pas pris en charge dans les points de restauration Microsoft Azure et ne peuvent pas être sauvegardés en mode sans agent. Si vous devez sauvegarder les données sur ces disques, installez l'agent de protection dans le système d'exploitation invité de la machine virtuelle.

Vous pouvez sélectionner l'une des options suivantes :

- **Ignorer les disques non pris en charge** : la sauvegarde s'effectue avec succès et les disques non pris en charge sont ignorés.
- **Avertissement en cas de disques non pris en charge** : la sauvegarde s'effectue avec un avertissement concernant le disque non pris en charge. Cette option est sélectionnée par défaut.
- **Échec sur les disques non pris en charge** : la sauvegarde échoue si la machine virtuelle avec un disque pris en charge est en cours de sauvegarde.

Consolidation de sauvegarde

Cette option définit s'il faut consolider les sauvegardes durant le nettoyage ou supprimer les chaînes de sauvegarde entières.

Le préréglage est le suivant : **Désactivé**.

La consolidation est un processus qui associe deux sauvegardes subséquentes ou plus dans une même sauvegarde.

Si cette option est activée, une sauvegarde qui devrait être supprimée pendant le nettoyage est consolidée avec la sauvegarde dépendante suivante (incrémentielle ou différentielle).

Dans le cas contraire, la sauvegarde est conservée jusqu'à ce que toutes les autres sauvegardes dépendantes puissent également être supprimées. Cela permet d'éviter la consolidation qui pourrait nécessiter un temps considérable, mais il nécessite de l'espace supplémentaire pour le stockage des sauvegardes dont la suppression est différée. L'âge ou le nombre de sauvegardes peut dépasser les valeurs spécifiées dans les règles de rétention.

Important
Sachez que la consolidation n'est qu'une méthode de suppression et non une alternative à la suppression. La sauvegarde obtenue ne contiendra pas les données qui étaient présentes dans la sauvegarde supprimée et absentes de la sauvegarde incrémentielle ou différentielle conservée.

Elle *n'est pas* effective si l'une des conditions suivantes est remplie :

© Acronis International GmbH, 2003-2026

- La destination de la sauvegarde est le stockage sur le Cloud.
- Le modèle de sauvegarde est défini sur **Toujours incrémentielle (fichier unique)**.
- Le format de sauvegarde est défini sur **Version 12**.

Les sauvegardes stockées sur le Cloud, ainsi que les sauvegardes sous forme d'un fichier unique (formats Version 11 et 12), sont toujours consolidées, car leur structure interne permet une consolidation rapide et facile.

Toutefois, si le format Version 12 est utilisé et que plusieurs chaînes de sauvegarde sont présentes (chaque chaîne étant stockée dans un fichier .tibx séparé), la consolidation ne fonctionne qu'avec la dernière chaîne. Toute autre chaîne est supprimée en bloc, à l'exception de la première, qui est réduite à la taille minimum pour conserver les méta-informations (environ 12 Ko). Ces méta-informations sont requises pour assurer la cohérence des données lors d'opérations de lecture et écriture simultanées. Les sauvegardes incluses dans ces chaînes disparaissent de l'interface graphique dès que la règle de rétention est appliquée, même si elles existent physiquement tant que la chaîne entière n'est pas supprimée.

Dans tous les autres cas, les sauvegardes dont la suppression est différée sont marquées de l'icône d'une corbeille () dans l'interface utilisateur graphique. Si vous supprimez une telle sauvegarde en cliquant sur le signe X, la consolidation sera exécutée.

Nom de fichier de sauvegarde

Cette option définit le nom des fichiers de sauvegarde créés par le plan de protection ou par le plan de sauvegarde des applications dans le cloud.

Pour les fichiers de sauvegarde créés par des plans de protection, vous pouvez voir ces noms dans un gestionnaire de fichiers lorsque vous parcourez l'emplacement de sauvegarde.

Qu'est-ce qu'un fichier de sauvegarde ?

Chaque plan de protection crée un ou plusieurs fichiers à l'emplacement de sauvegarde, selon le modèle et le format de sauvegarde utilisés. Le tableau suivant répertorie les fichiers qui peuvent être créés par machine ou par boîte aux lettres.

	Toujours incrémentielle (fichier unique)	**Autres modèles de sauvegarde**
Format de sauvegarde **Version 11**	Un fichier TIB et un fichier de métadonnées XML	Plusieurs fichiers TIB et un fichier de métadonnées XML
Format de sauvegarde **Version 12**	Un fichier TIBX par chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent). Si la taille d'un fichier stocké dans un dossier local ou réseau (SMB) dépasse 200 Go, le fichier est divisé par défaut en fichiers de 200 Go.	

© Acronis International GmbH, 2003-2026

Tous les fichiers ont le même nom, avec ou sans ajout d'une estampille ou d'un numéro séquentiel. Vous pouvez définir ce nom (appelé nom de fichier de sauvegarde) lors de la création ou de la modification d'un plan de protection ou d'plan de sauvegarde d'applications dans le cloud.

Remarque
La date et l'heure sont ajoutées au nom de fichier de la sauvegarde uniquement dans la version 11 du format de sauvegarde.

Si vous changez le nom d'un fichier de sauvegarde dans un plan de protection ou un plan de sauvegarde d'applications dans le cloud, la sauvegarde suivante sera une sauvegarde complète.

Si vous spécifiez le nom de fichier d'une sauvegarde existante du même ordinateur, une sauvegarde complète, incrémentielle ou différentielle est créée en fonction de la planification du plan.

Remarque
Si vous déplacez des fichiers de sauvegarde (.tibx) depuis leur stockage d'origine, ne les renommez pas. Les fichiers renommés apparaîtront comme étant endommagés et vous ne pouvez pas en restaurer les données.

Il est possible de définir des noms de fichier de sauvegarde pour des emplacements qui ne peuvent pas être parcourus par un gestionnaire de fichiers (tel que le stockage dans le cloud). Dans ce cas, vous voyez les noms personnalisés dans l'onglet **Stockage de sauvegarde**.

Où puis-je voir les noms des fichiers de sauvegarde ?

Pour les plans de protection, sélectionnez dans l'onglet **Stockage de sauvegarde** l'emplacement, puis l'archive de sauvegardes.

- Le nom de fichier de sauvegarde par défaut s'affiche dans le volet **Détails**.
- Si vous définissez un nom de fichier de sauvegarde non par défaut, il s'affichera directement dans l'onglet **Stockage de sauvegarde**, dans la colonne **Nom**.

Pour les plans de sauvegarde d'applications dans le cloud, sélectionnez dans l'onglet **Stockage de sauvegarde** l'emplacement et l'archive de sauvegardes, puis cliquez sur l'icône en forme d'engrenage.

Limites des noms de fichier de sauvegarde

- Un nom de fichier de sauvegarde ne peut pas se terminer par un numéro.
  La lettre A est ajoutée à la fin du nom de fichier de sauvegarde par défaut afin d'éviter qu'il se termine par un numéro. Si vous créez un nom personnalisé, assurez-vous toujours qu'il ne se termine pas par un numéro. Si vous utilisez des variables, le nom ne doit pas se terminer par une variable, car cette dernière peut finir par un numéro.
- Un nom de fichier de sauvegarde ne peut pas contenir les symboles suivants : **()&?*$<>":\|/#**, renvoi à la ligne (**\n**) et tabulations (**\t**).

© Acronis International GmbH, 2003-2026

Remarque
Choisissez des noms de fichier de sauvegarde conviviaux. De cette manière, vous pourrez distinguer facilement les sauvegardes en parcourant l'emplacement de sauvegarde avec un gestionnaire de fichiers.

Nom de fichier de sauvegarde par défaut

Le nom du fichier de sauvegarde par défaut pour les sauvegardes de machines physiques et virtuelles intégrales, disques/volumes, fichiers/dossiers, base de données Microsoft SQL Server, bases de données Microsoft Exchange Server et configuration ESXi est `[Machine Name]-[Plan ID]-[Unique ID]A`.

Le nom par défaut des sauvegardes de boîte aux lettres Exchange et de sauvegardes de boîte aux lettres Microsoft 365 créées par un Agent local pour Microsoft 365 est `[Mailbox ID]_mailbox_[Plan ID]A`.

Le nom par défaut des sauvegardes Microsoft Azure est préfixé avec `[Mailbox ID]_`. Ce préfixe ne peut pas être retiré.

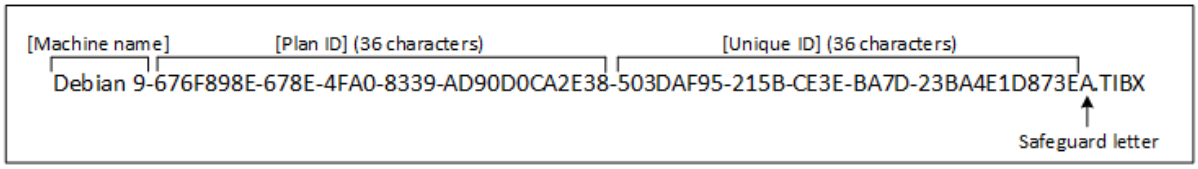
Le nom par défaut pour les sauvegardes d'application Cloud créées par les agents dans le Cloud est `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

Le nom par défaut est constitué des variables suivantes :

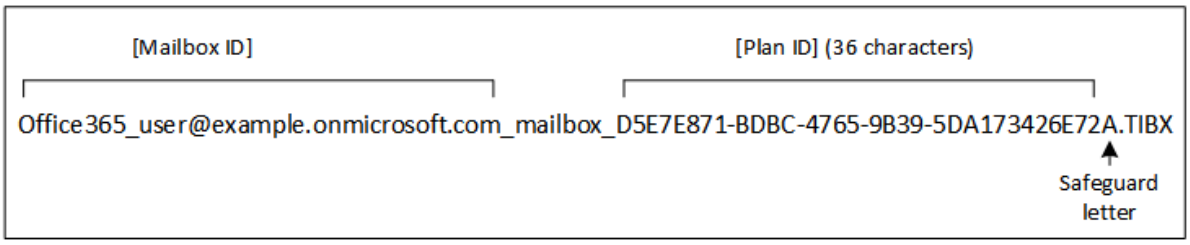
- `[Machine Name]` Cette variable est remplacée par le nom de l'ordinateur (celui qui est affiché dans la console Cyber Protect).
- `[Plan ID]`, `[Plan Id]` Ces variables sont remplacées par l'identifiant unique du plan de protection. Cette valeur ne change pas si le plan est renommé.
- `[Unique ID]` Cette variable est remplacée par l'identificateur unique de la machine sélectionnée. Cette valeur ne change pas si la machine est renommée.
- `[Mailbox ID]` Cette variable est remplacée par le nom principal de l'utilisateur (UPN) de la boîte aux lettres.
- `[Resource Name]` Cette variable est remplacée par le nom de la source de données Cloud, comme le nom principal de l'utilisateur (UPN), l'URL du site SharePoint ou le nom du Drive partagé.
- `[Resource Type]` Cette variable est remplacée par le type de source des données Cloud, comme `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` Cette variable est remplacée par l'identificateur unique de la source de données Cloud. Cette valeur ne change pas si la source de données Cloud est renommée.
- `"A"` est une lettre de protection ajoutée à la fin du nom de fichier de sauvegarde afin d'éviter qu'il se termine par un numéro.

Le diagramme ci-dessous affiche le nom de fichier de sauvegarde par défaut.

© Acronis International GmbH, 2003-2026



Le diagramme ci-dessous affiche le nom de fichier de sauvegarde par défaut pour les sauvegardes de boîte aux lettres Microsoft 365 réalisées par un agent local.



Noms sans variables

Si vous remplacez le nom du fichier de sauvegarde par `MyBackup`, les fichiers de sauvegarde ressembleront aux exemples suivants. Dans les deux exemples, on suppose des sauvegardes incrémentielles quotidiennes planifiées à 14h40 à partir du 13 septembre 2016.

Pour le format version 12 avec le modèle de sauvegarde **« Toujours incrémentielle (fichier unique) »** :

```
MyBackup.tibx
```

Pour le format version 12 avec un autre modèle de sauvegarde :

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Utilisation de variables

Outre les variables utilisées par défaut, vous pouvez utiliser les variables suivantes :

- La variable `[Plan name]`, qui est remplacée par le nom du plan de protection.
- La variable `[Virtualization Server Type]`, qui est remplacée par « vmwesx » si les machines virtuelles sont sauvegardées par l'agent pour VMware ou par « mshyperv » si les machines virtuelles sont sauvegardées par l'agent pour Hyper-V.

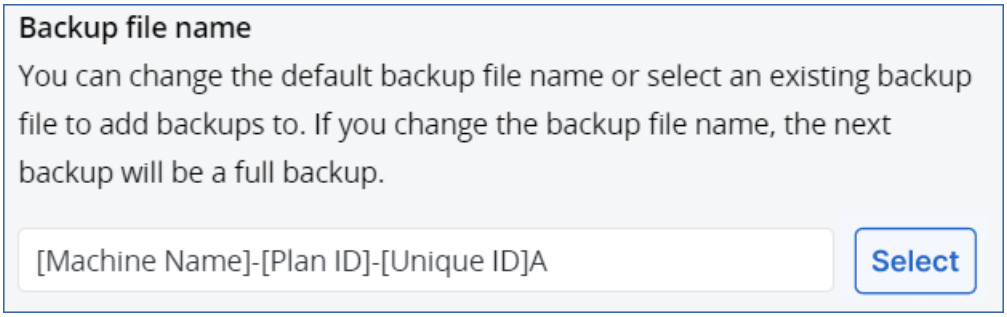
Si plusieurs machines ou boîtes aux lettres sont sélectionnées pour la sauvegarde, le nom du fichier de sauvegarde doit contenir la variable `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]`, la variable `[Resource Id]`.

© Acronis International GmbH, 2003-2026

Création de sauvegardes dans une archive de sauvegarde existante

Vous pouvez configurer les sauvegardes d'une ressource pour qu'elles soient ajoutées à une archive de sauvegardes existante.

Cette option peut être utile, par exemple, lorsqu'un plan de protection est appliqué à un seul ordinateur, et que vous devez supprimer cet ordinateur de la console Cyber Protect ou désinstaller l'agent avec ses paramètres de configuration. Après avoir rajouté l'ordinateur ou réinstallé l'agent, vous pouvez forcer le plan de protection à poursuivre la sauvegarde vers l'archive d'origine.



Pour configurer les sauvegardes d'une ressource à ajouter à une archive de sauvegardes existante

Ressources autres que de cloud à cloud

1. Dans l'écran **Tous les terminaux**, cliquez sur la ressource, puis sur **Protéger**.
2. Dans les paramètres du plan de protection, développez le module **Sauvegarde**.
3. Cliquez sur **Options de sauvegarde**, puis sur **Modifier**.
4. Dans l'onglet **Nom de fichier de la sauvegarde**, cliquez sur **Sélectionner**.
   Le bouton **Sélectionner** affiche les sauvegardes à l'emplacement sélectionné dans la section **Où sauvegarder** du plan de protection.

   Remarque
   Le bouton **Sélectionner** n'est disponible que pour les plans de protection créés pour une seule ressource à laquelle ils sont appliqués.
5. Sélectionnez une archive, puis cliquez sur **Terminé**.
6. Cliquez sur **Terminé**, puis sur **Appliquer**.

Ressources de cloud à cloud

1. Dans l'onglet **Gestion** > **Sauvegarde d'applications dans le Cloud**, sélectionnez le plan.
2. Cliquez sur **Modifier**, puis sur l'icône en forme d'engrenage située à côté du nom du plan.
3. Dans l'onglet **Nom de la sauvegarde**, cliquez sur **Sélectionner**.

© Acronis International GmbH, 2003-2026

Remarque
Le bouton **Sélectionner** n'est disponible que pour les plans de sauvegarde créés (et appliqués) pour une seule ressource.

4. Sélectionnez une archive de sauvegardes, puis cliquez sur **Terminé**.
5. Cliquez sur **Terminé**, puis sur **Enregistrer**.

Format de sauvegarde

L'option **Format de sauvegarde** définit le format des sauvegardes créées par le plan de protection. Cette option est disponible uniquement pour les plans de protection qui utilisent déjà le format de sauvegarde version 11. Si tel est le cas, vous pouvez modifier le format de sauvegarde en version 12. Après le passage du format de sauvegarde en version 12, l'option deviendra indisponible.

- **Version 11**
  Le format hérité conservé pour une compatibilité descendante.

  Remarque
  Vous ne pouvez pas sauvegarder de groupes de disponibilité de la base de données (DAG) à l'aide du format de sauvegarde version 11. La sauvegarde de groupes DAG est prise en charge uniquement au format version 12.

- **Version 12**
  Le format de sauvegarde qui a été introduit dans Acronis Backup 12 pour une sauvegarde et une restauration plus rapides. Chaque chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent) est enregistrée dans un fichier TIBX unique.

Format et fichiers de sauvegarde

Pour les emplacements de sauvegarde qui peuvent être parcourus avec un gestionnaire de fichiers (comme les dossiers locaux et réseau), le format de sauvegarde détermine le nombre de fichiers et leur extension. Le tableau suivant répertorie les fichiers qui peuvent être créés par machine ou par boîte aux lettres.

	Toujours incrémentielle (fichier unique)	**Autres modèles de sauvegarde**
Format de sauvegarde **Version 11**	Un fichier TIB et un fichier de métadonnées XML	Plusieurs fichiers TIB et un fichier de métadonnées XML
Format de sauvegarde **Version 12**	Un fichier TIBX par chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent). Si la taille d'un fichier stocké dans un dossier local ou réseau (SMB) dépasse 200 Go, le fichier est divisé par défaut en fichiers de 200 Go.	

© Acronis International GmbH, 2003-2026

Modification du format de sauvegarde en version 12 (TIBX)

Si vous faites passer le format de sauvegarde de la version 11 (format TIB) à la version 12 (format TIBX) :

- La sauvegarde suivante sera complète.
- Dans les emplacements de sauvegarde qui peuvent être parcourus avec un gestionnaire de fichiers (comme les dossiers locaux et réseau), un nouveau fichier TIBX sera créé. Le nouveau fichier aura le même nom que l'original, avec le suffixe **_v12A**.
- Les règles de rétention et de réplication seront appliquées uniquement aux nouvelles sauvegardes.
- Les anciennes sauvegardes ne seront pas supprimées et resteront disponibles dans l'onglet **Stockage de sauvegarde**. Vous pouvez les supprimer manuellement.
- Les anciennes sauvegardes dans le Cloud ne consommeront pas le quota de **Stockage dans le Cloud**.
- Les anciennes sauvegardes locales consommeront le quota de **sauvegarde locale** jusqu'à ce que vous les supprimiez manuellement.

Déduplication dans l'archive

Le format de sauvegarde TIBX de la version 12 est compatible avec la déduplication dans l'archive, qui offre les avantages suivants :

- Taille des sauvegardes considérablement réduite, avec déduplication intégrée au niveau du bloc pour n'importe quel type de données
- Une gestion efficace des liens directs garantit l'absence de doublons de stockage.
- Segmentation basée sur le hachage

Remarque
La déduplication dans l'archive est activée par défaut pour toutes les sauvegardes au format TIBX. Il n'est pas nécessaire que vous l'activiez dans les options de sauvegarde, et vous ne pouvez pas la désactiver.

Compatibilité des formats de sauvegarde dans différentes versions de solution

Pour obtenir des informations sur la compatibilité des formats de sauvegarde, voir cet article de la base de connaissances.

Validation de la sauvegarde

La validation est une opération qui vérifie la possibilité de restauration de données à partir d'une sauvegarde. Lorsque cette option est activée, chaque sauvegarde créée par le plan de protection est

© Acronis International GmbH, 2003-2026

validée immédiatement après sa création à l'aide de la méthode de vérification de somme de contrôle. Cette opération est effectuée par l'agent de protection.

Le préréglage est le suivant : **Désactivé**.

Pour en savoir plus sur la validation par vérification de somme de contrôle, reportez-vous à "Vérification de la somme de contrôle" (p. 261).

Remarque
Selon les paramètres choisis par votre fournisseur de services, il se peut que la validation ne soit pas disponible lors d'une sauvegarde sur le stockage dans le Cloud. La validation est également indisponible pour les emplacements de sauvegarde dans le cloud public.

Suivi des blocs modifiés (CBT)

Cette option est effective pour les sauvegardes suivantes :

- Sauvegardes de disque de machines virtuelles
- Sauvegardes de disque de machines physiques fonctionnant sous Windows
- Sauvegardes de bases de données Microsoft SQL Server
- Sauvegardes de bases de données Microsoft Exchange Server

Le préréglage est le suivant : **Activé**.

Cette option détermine l'utilisation du suivi des blocs modifiés (CBT) lors de l'exécution d'une sauvegarde incrémentielle ou différentielle.

La technologie CBT accélère le processus de sauvegarde. Les modifications apportées au disque ou à la base de données sont continuellement suivies au niveau des blocs. Lorsqu'une sauvegarde commence, les modifications peuvent être immédiatement enregistrées sur la sauvegarde.

Mode de sauvegarde de cluster

Ces options sont effectives pour les sauvegardes de niveau base de données de Microsoft SQL Server et de Microsoft Exchange Server.

Ces options ne sont effectives que si le cluster lui-même (groupes de disponibilité Always On (AAG) de Microsoft SQL Server ou groupe de disponibilité de la base de données (DAG) de Microsoft Exchange Server) est sélectionné pour la sauvegarde plutôt que les nœuds ou bases de données qu'il contient. Si vous sélectionnez des éléments individuels au sein du cluster, la sauvegarde ne prendra pas en charge le cluster et seules les copies sélectionnées des éléments seront sauvegardées.

Microsoft SQL Server

Cette option détermine le mode de sauvegarde des groupes de disponibilité Always On (AAG) de Microsoft SQL Server. Pour que cette option prenne effet, l'agent pour SQL doit être installé sur tous

© Acronis International GmbH, 2003-2026

les nœuds AAG. Pour plus d'informations sur la sauvegarde des groupes de disponibilité Always On, consultez la section « Protection des groupes de disponibilité Always On (AAG) ».

Le préréglage est le suivant : **Réplica secondaire si possible.**

Vous pouvez choisir l'une des options suivantes:

- **Réplica secondaire si possible**
  Si tous les réplicas secondaires sont hors ligne, le réplica principal est sauvegardé. La sauvegarde du réplica principal peut ralentir les performances de SQL Server, mais les données seront sauvegardées dans leur état le plus récent.
- **Réplica secondaire**
  Si tous les réplicas secondaires sont hors ligne, la sauvegarde échouera. La sauvegarde des réplicas secondaires n'affecte pas les performances de SQL Server et vous permet d'agrandir le créneau de sauvegarde. Toutefois, les réplicas passifs peuvent contenir des informations qui ne sont pas à jour parce qu'ils sont souvent configurés pour être mis à jour de façon asynchrone (décalée).
- **Réplica principal**
  Si le réplica principal est hors ligne, la sauvegarde échouera. La sauvegarde du réplica principal peut ralentir les performances de SQL Server, mais les données seront sauvegardées dans leur état le plus récent.

Quelle que soit la valeur de cette option, afin d'assurer la cohérence de la base de données, le logiciel ignore les bases de données qui ne sont *pas* dans l'état **SYNCHRONISÉ** ou **SYNCHRONISATION** au démarrage de la sauvegarde. Si toutes les bases de données sont ignorées, la sauvegarde échoue.

Microsoft Exchange Server

Cette option détermine le mode de sauvegarde des groupe de disponibilité de la base de données (DAG) Exchange Server. Afin que cette option prenne effet, l'agent pour Exchange doit être installé sur tous les nœuds DAG. Pour plus d'informations sur la sauvegarde des groupes de disponibilité de la base de données, consultez la section « Protection des groupes de disponibilité de la base de données (DAG) ».

Le préréglage est le suivant : **Copie passive si possible**

Vous pouvez choisir l'une des options suivantes:

- **Copie passive si possible**
  Si toutes les copies passives sont hors ligne, la copie active est sauvegardée. La sauvegarde de la copie active peut ralentir les performances d'Exchange Server, mais les données seront sauvegardées dans leur état le plus récent.
- **Copie passive**
  Si toutes les copies passives sont hors ligne, la sauvegarde échouera. La sauvegarde des copies passives n'affecte pas les performances du serveur Exchange et vous permet d'agrandir le créneau de sauvegarde. Toutefois, les copies passives peuvent contenir des informations qui ne

© Acronis International GmbH, 2003-2026

sont pas à jour parce que ces copies sont souvent configurées pour être mises à jour de façon asynchrone (décalées).

- **Copie active**

  Si la copie active est hors ligne, la sauvegarde échouera. La sauvegarde de la copie active peut ralentir les performances d'Exchange Server, mais les données seront sauvegardées dans leur état le plus récent.

Quelle que soit la valeur de cette option, afin d'assurer la cohérence de la base de données, le logiciel ignore les bases de données qui ne sont *pas* dans l'état **SAIN** ou **ACTIF** au démarrage de la sauvegarde. Si toutes les bases de données sont ignorées, la sauvegarde échoue.

Niveau de compression

Remarque
Cette option n'est pas disponible pour les sauvegardes cloud à cloud. La compression pour ces sauvegardes est activée par défaut avec un niveau fixe correspondant au niveau **Normale** ci-dessous.

L'option définit le niveau de compression appliqué aux données sauvegardées. Les niveaux disponibles sont les suivants : **Aucune**, **Normale**, **Élevée**, **Maximale**.

Le préréglage est le suivant : **Normale**.

Un niveau de compression supérieur signifie que le processus de sauvegarde prend plus de temps, mais que la sauvegarde en résultant occupe moins d'espace. Pour le moment, le fonctionnement des niveaux **Élevée** et **Maximale** est identique.

Le niveau de compression des données optimal dépend du type de données en cours de sauvegarde. Par exemple, même une compression maximale ne réduira pas de manière significative la taille de la sauvegarde si cette dernière contient essentiellement des fichiers comprimés tels que des fichiers .jpg, .pdf ou .mp3. Cependant, des formats tels que .doc ou .xls seront bien comprimés.

Gestion erreurs

Ces options vous permettent de spécifier comment traiter des erreurs qui peuvent se produire pendant la restauration.

Réessayer si une erreur se produit

Le préréglage est le suivant : **Activé. Nombre de tentatives : 30. Intervalle entre les tentatives : 30 secondes.**

Lorsqu'une erreur récupérable se produit, Cyber Protect tente de réexécuter l'opération qui a échoué. Vous pouvez définir le nombre maximal de tentatives et l'intervalle entre chaque réexécution. Si l'opération n'aboutit pas après le nombre maximal de tentatives, elle échoue.

© Acronis International GmbH, 2003-2026

Pour les sauvegardes vers un emplacement réseau ou un stockage dans le cloud (stockage dans l'Acronis Cloud ou dans un cloud public tel qu'Amazon, Azure, compatible S3 ou Impossible Cloud), la gestion des erreurs dépend du moment où l'erreur se produit.

Une erreur s'est produite au démarrage de la sauvegarde	Une erreur s'est produite pendant une sauvegarde
Le nombre de nouvelles tentatives dépend de la réponse de l'API de stockage. Si l'API renvoie une réponse indiquant qu'une nouvelle tentative est possible (par exemple, erreur « 503 Service non disponible »), l'opération peut échouer au bout de deux heures. Ce scénario est généralement plus probable pour un stockage dans le cloud que pour un emplacement réseau.	Le nombre de nouvelles tentatives dépend des paramètres **Gestion erreurs** configurés dans le plan de protection. Il peut s'agir, par exemple, de 30 nouvelles tentatives avec un intervalle de 30 secondes entre les nouvelles tentatives.

Pour les sauvegardes vers des dossiers locaux, les paramètres **Gestion erreurs** s'appliquent uniquement aux erreurs qui se produisent pendant une sauvegarde. Si une erreur se produit au démarrage de la sauvegarde, l'opération de sauvegarde échoue immédiatement.

Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux)

Le préréglage est le suivant : **Activé**.

Avec le mode silencieux activé, le programme gérera automatiquement les situations qui nécessitent l'intervention de l'utilisateur (sauf pour le traitement des secteurs défectueux, qui est défini comme une option séparée). Si une opération ne peut pas se poursuivre sans l'intervention de l'utilisateur, elle échouera. Les détails de l'opération, y compris les erreurs, le cas échéant, apparaissent dans le journal des opérations.

Ignorer les secteurs défectueux

Le préréglage est le suivant : **Désactivé**.

Lorsque cette option est désactivée, chaque fois que le programme rencontre un secteur défectueux, l'activité de sauvegarde présente l'état **Intervention nécessaire**. Afin de pouvoir sauvegarder les informations valides d'un disque se détériorant rapidement, activez la fonction ignorer les secteurs défectueux. Le programme continuera de sauvegarder les autres données et vous pourrez monter la sauvegarde de disque en résultant et extraire les fichiers valides vers un autre disque.

© Acronis International GmbH, 2003-2026

Remarque
La fonctionnalité permettant d'ignorer les secteurs défectueux n'est pas prise en charge sous Linux. Vous pouvez sauvegarder les systèmes Linux avec des secteurs défectueux en mode hors ligne à l'aide de l'outil de création de supports de démarrage dans la version sur site de Cyber Protect. L'utilisation de l'outil de création de supports de démarrage sur site nécessite une licence distincte. Contactez le support pour obtenir de l'aide.

Réessayer si une erreur se produit lors de la création d'instantané de MV

Le préréglage est le suivant : **Activé. Nombre de tentatives : 3. Intervalle entre les tentatives : 5 minutes.**

Lorsque la prise d'un instantané de machine virtuelle échoue, le programme essaie à nouveau d'effectuer l'opération qui a échoué. Vous pouvez définir l'intervalle de temps ainsi que le nombre de tentatives. Les tentatives s'arrêteront dès que l'opération réussira OU que le nombre de tentatives sera atteint, le premier de ces deux cas prévalant.

Sauvegarde incrémentielle/différentielle rapide

Cette option est effective pour une sauvegarde incrémentielle et différentielle de niveau disque.

Cette option n'est pas efficace (toujours désactivée) pour les volumes formatés avec les systèmes de fichiers JFS, ReiserFS3, ReiserFS4, ReFS ou XFS.

Le préréglage est le suivant : **Activé**.

Une sauvegarde incrémentielle ou différentielle capture uniquement des modifications de données. Pour accélérer le processus de sauvegarde, le programme détermine si un fichier a été modifié ou non grâce à la taille du fichier et à la date / l'heure à laquelle le fichier a été modifié pour la dernière fois. Si cette fonctionnalité est désactivée, le programme comparera les contenus entiers des fichiers à ceux stockés dans la sauvegarde.

Filtres de fichiers (Inclusions/Exclusions)

Utilisez les filtres de fichiers pour inclure certains fichiers et dossiers dans une sauvegarde, ou pour en exclure d'une sauvegarde.

Sauf indication contraire, les filtres de fichiers sont disponibles pour les sauvegardes d'un ordinateur complet, de disque et de niveau fichier.

Les filtres de fichiers ne sont pas disponibles avec les systèmes de fichiers XFS, JFS, exFAT et ReiserFS4. Pour plus d'informations, voir "Systèmes de fichiers pris en charge" (p. 539).

Les filtres de fichiers ne s'appliquent pas aux disques dynamiques (volumes LVM ou LDM) de machines virtuelles sauvegardées en mode sans agent, par Agent pour VMware, Agent pour Hyper-V ou Agent pour Scale Computing, par exemple.

© Acronis International GmbH, 2003-2026

Types de filtres de fichiers

Les filtres de fichiers sont des types suivants :

- Filtres d'inclusion (**Incluez uniquement les fichiers correspondant aux critères suivants**)
  Si vous indiquez `C:\File.exe` dans le filtre d'inclusion, ce fichier sera le seul à être sauvegardé, même si vous sélectionnez la sauvegarde **Machine complète**. Pour plus d'informations, voir "Exemples de filtres" (p. 623).

  Remarque
  Ce filtre n'est pas pris en charge pour les sauvegardes de niveau fichier de la **version 11** qui ne sont pas stockées dans le stockage dans le cloud.

- Filtres d'exclusion (**Excluez les fichiers correspondant aux critères suivants**)
  Si vous indiquez `C:\File.exe` dans un filtre d'exclusion, ce fichier est ignoré lors de la sauvegarde, même si vous sélectionnez la sauvegarde **Machine complète**.

Valeurs de filtre de fichier

Dans un filtre de fichier, vous pouvez utiliser les valeurs suivantes :

- Nom du fichier ou du dossier
  Spécifiez le nom du fichier ou du dossier, par exemple, `Document.txt`. Tous les fichiers et dossiers portant ce nom seront sélectionnés.
- Chemin complet vers un fichier ou un dossier
  Spécifiez le chemin d'accès complet au fichier ou dossier, en commençant par la lettre du lecteur (sauvegarde de données Windows) ou le répertoire racine (sauvegarde de données Linux ou macOS). Sous Windows, Linux et macOS, vous pouvez utiliser des barres obliques (par exemple, `C:/Temp/File.tmp`). Sous Windows, vous pouvez également utiliser les barres obliques inverses traditionnelles (par exemple, `C:\Temp\File.tmp`).

  Important
  Si le système d'exploitation de l'ordinateur sauvegardé n'est pas détecté correctement pendant la sauvegarde de disque, les filtres de chemin complet vers les fichiers ne fonctionneront pas. Pour un filtre d'exclusion, un avertissement s'affiche. Dans le cas d'un filtre d'inclusion, la sauvegarde échoue.
  Par exemple, un chemin d'accès complet à un fichier peut être `C:\Temp\File.tmp`. Si le système d'exploitation n'est pas détecté correctement, un filtre de chemin d'accès complet, qui inclut la lettre du lecteur ou le répertoire racine (par exemple `C:\Temp\File.tmp` ou `C:\Temp\*`) entraîne un avertissement ou une erreur.
  Un filtre qui n'inclut ni la lettre du lecteur ni le répertoire racine (par exemple `Temp\*` ou `Temp\File.tmp`), ou un filtre qui commence par un astérisque (par exemple, `*C:\`) n'entraîne ni avertissement ni erreur. Toutefois, si le système d'exploitation de l'ordinateur sauvegardé n'est pas détecté correctement, ces filtres ne fonctionneront pas.

© Acronis International GmbH, 2003-2026

Caractères génériques

Vous pouvez utiliser les caractères génériques suivants avec les noms de fichiers ou de dossiers et les chemins de fichiers ou de dossiers :

- Astérisque (*)

  L'astérisque représente zéro caractère ou plus.

  Par exemple, le critère de filtre `Doc*.txt` englobe les fichiers tels que `Doc.txt` et `Document.txt`.
- Double astérisque (**)

  Le double astérisque représente zéro caractère ou plus, y compris le caractère barre oblique.

  Par exemple, le critère `**/Docs/**.txt` correspond à tous les fichiers TXT dans tous les sous-dossiers de tous les dossiers `Docs`.

  Vous ne pouvez utiliser le caractère générique de double astérisque que pour les sauvegardes au format Version 12.
- Point d'interrogation (?)

  Le point d'interrogation représente un seul caractère.

  Par exemple, `Doc?.txt` englobe les fichiers tels que `Doc1.txt` et `Docs.txt`, mais pas les fichiers `Doc.txt` ou `Doc11.txt`.

Remarque

Utilisez le caractère générique point d'interrogation si le nom du fichier ou du dossier contient une virgule ou un point-virgule. La virgule et le point-virgule sont interprétés comme des délimiteurs et divisent le filtre en deux parties. Par exemple, si vous souhaitez utiliser le dossier `MyCompany,Inc` dans un filtre, utilisez `MyCompany?Inc` lorsque vous spécifiez la valeur du filtre. Sinon, vous créerez deux filtres distincts, comme suit :

- `MyCompany`
- `Inc`

Configuration des filtres de fichiers

Vous pouvez configurer les filtres de fichiers dans le plan de protection.

Pour configurer les filtres de fichiers

1. Dans un plan de protection, développez le module **Sauvegarde**.
2. Dans **Options de sauvegarde**, cliquez sur **Modifier**.
3. Sélectionnez **Filtres de fichiers (Inclusions/Exclusions)**.
4. Configurez les filtres de fichiers.

   Vous pouvez configurer un filtre (inclusion ou exclusion) ou les deux filtres. Le filtre d'exclusion est prioritaire sur le filtre d'inclusion. Par exemple, si vous spécifiez `C:\File.exe` dans les deux filtres, ce fichier `C:\File.exe` sera ignoré lors d'une sauvegarde.

© Acronis International GmbH, 2003-2026

L'utilisation de filtres n'affecte pas la sélection de fichiers spécifiques dans l'étendue de la sauvegarde (**Éléments à sauvegarder**). Pour plus d'informations, voir "Exemples de filtres" (p. 623).

Remarque
Si un nom ou un chemin d'accès contient une virgule ou un point-virgule, remplacez-les par le caractère générique point d'interrogation (?). La virgule et le point-virgule sont interprétés comme des délimiteurs et divisent le filtre en deux parties. Pour plus d'informations, voir "Caractères génériques " (p. 622).

5. Cliquez sur **Terminé**.
6. Enregistrez le plan de protection.

Les filtres de fichiers seront appliqués à la portée configurée dans la section **Éléments à sauvegarder** du plan de protection.

Exemples de filtres

Les tableaux ci-dessous présentent des exemples de configurations de filtres de fichiers.

Filtre d'inclusion			
Quoi sauvegarder	**Valeur du filtre**	**L'archive de sauvegarde contient**	**Description**
`C:\Folder1` (contient `MyFile.txt` et d'autres fichiers) `C:\Folder2` (contient `MyDocument.txt` et d'autres fichiers)	`MyFile.txt` `C:\Folder2\MyDocument.txt`	`C:\Folder1\MyFile.txt` `C:\Folder2\MyDocument.txt`	Le filtre d'inclusion correspond à l'étendue de la sauvegarde (**Éléments à sauvegarder**). Seuls les fichiers spécifiés dans le filtre d'inclusion sont présents dans les dossiers sauvegardés. Vous pouvez configurer un filtre de fichier en utilisant des noms de

© Acronis International GmbH, 2003-2026

Filtre d'inclusion			
Quoi sauvegarder	**Valeur du filtre**	**L'archive de sauvegarde contient**	**Description**
			fichiers ou de dossiers, ou en utilisant des chemins de fichiers ou de dossiers.
`C:\Folder1` (contient plusieurs fichiers)	`C:\Folder2\MyDocument.txt`	`C:\Folder1` (comme dossier vide)	Le filtre d'inclusion ne correspond pas à l'étendue de la sauvegarde (**Éléments à sauvegarder**). `Folder1` est sauvegardé, mais il est vide car il ne contient pas le fichier dans le filtre d'inclusion. Le fichier dans le filtre d'inclusion n'est pas sauvegardé, car il ne fait pas partie de la portée de la sauvegarde.
`C:\Folder1` (contient `MyFile.txt` et d'autres fichiers) `C:\Folder2` (contient `MyDocument.txt` et d'autres fichiers)	`MyFile.txt`	`C:\Folder1\MyFile.txt` `C:\Folder2` (en tant que dossier vide)	Le filtre d'inclusion correspond partiellement à l'étendue de la sauvegarde (**Éléments à sauvegarder**). `Folder1` est

© Acronis International GmbH, 2003-2026

Filtre d'inclusion			
Quoi sauvegarder	**Valeur du filtre**	**L'archive de sauvegarde contient**	**Description**
			sauvegardé, mais il ne contient que le fichier spécifié dans le filtre d'inclusion. `Folder2` est sauvegardé, mais il est vide car il ne contient pas le fichier dans le filtre d'inclusion.
`C:\Folder1` (contient `MyFile.txt` et d'autres fichiers) `C:\Folder2\MyDocument.txt`	`MyFile.txt`	`C:\Folder1\MyFile.txt` `C:\Folder2\MyDocument.txt`	`Folder1` est sauvegardé, mais il ne contient que le fichier spécifié dans le filtre d'inclusion. Le deuxième fichier sélectionné est également sauvegardé. L'utilisation de filtres n'affecte pas la sélection de fichiers spécifiques dans la portée de la sauvegarde (**Éléments à sauvegarder**).

© Acronis International GmbH, 2003-2026

Filtre d'exclusion			
Quoi sauvegarder	**Valeur du filtre**	**L'archive de sauvegarde contient**	**Description**

`C:\Folder1` (contient `MyFile.txt` et d'autres fichiers)
 	
`C:\Folder2` (contient `MyDocument.txt` et d'autres fichiers)
	`MyFile.txt`
	
	`C:\Folder2\MyDocument.txt`
		`C:\Folder1` – tous les fichiers sauf `MyFile.txt`
		
		`C:\Folder2` – tous les fichiers sauf `MyDocument.txt`
			Le filtre d'exclusion correspond à l'étendue de la sauvegarde (**Éléments à sauvegarder**).
			
			Les fichiers spécifiés dans le filtre d'exclusion sont manquants dans les dossiers sauvegardés.
			
			Vous pouvez configurer un filtre de fichier en utilisant des noms de fichiers ou de dossiers, ou en utilisant des chemins de fichiers ou de dossiers.

`C:\Folder1` (contient plusieurs fichiers)	`C:\Folder2\MyDocument.txt`	`C:\Folder1` – tous les fichiers	Le filtre d'exclusion ne correspond pas à l'étendue de la sauvegarde (**Éléments à sauvegarder**). Tout le contenu de `Folder1` est sauvegardé.
`C:\Folder1` (contient	`MyFile.txt`	`C:\Folder1` – tous les	Le filtre

© Acronis International GmbH, 2003-2026

Filtre d'exclusion			
Quoi sauvegarder	**Valeur du filtre**	**L'archive de sauvegarde contient**	**Description**
`MyFile.txt` et d'autres fichiers) `C:\Folder2` (contient `MyDocument.txt` et d'autres fichiers)		fichiers sauf `MyFile.txt` `C:\Folder2` – tous les fichiers	d'inclusion correspond partiellement à l'étendue de la sauvegarde (**Éléments à sauvegarder**). `Folder1` est sauvegardé, mais le fichier spécifié dans le filtre d'exclusion est manquant. Tout le contenu de `Folder2` est sauvegardé.
`C:\Folder1` (contient `MyFile.txt` et d'autres fichiers) `C:\Folder2\MyDocument.txt`	`MyFile.txt`	`C:\Folder1` – tous les fichiers sauf `MyFile.txt` `C:\Folder2\MyDocument.txt`	`Folder1` est sauvegardé, mais le fichier spécifié dans le filtre d'exclusion est manquant. Le deuxième fichier sélectionné est sauvegardé, car il ne correspond pas au filtre d'exclusion.

Instantané de sauvegarde de niveau fichier

Cette option est effective uniquement pour une sauvegarde de niveau fichier.

Cette option définit s'il faut sauvegarder des fichiers un par un ou en prenant une image statique instantanée des données.

© Acronis International GmbH, 2003-2026

Remarque
Les fichiers situés sur des réseaux partagés sont toujours sauvegardés un à la fois.

Le préréglage est le suivant :

- Si des machines sous Linux uniquement sont sélectionnées pour la sauvegarde : **Ne pas créer d'instantané.**
- Sinon : **Créer un instantané si cela est possible.**

Vous pouvez sélectionner l'une des options suivantes :

- **Créer un instantané si cela est possible**
  Sauvegarder directement les fichiers s'il n'est pas possible de prendre une image statique.
- **Toujours créer un instantané**
  Utiliser une image statique permet la sauvegarde de tous les fichiers, y compris les fichiers ouverts en accès exclusif. Les fichiers seront sauvegardés au même point dans le temps. Choisissez ce paramètre uniquement si ces facteurs sont critiques, c'est à dire que sauvegarder des fichiers sans image statique ne sert à rien. Si une image statique ne peut pas être prise, la sauvegarde échoue.
- **Ne pas créer d'instantané**
  Toujours sauvegarder les fichiers directement. Essayer de sauvegarder des fichiers qui sont ouverts en accès exclusif entraînera une erreur de lecture. Les fichiers dans la sauvegarde peuvent ne pas être constants dans le temps.

Données d'investigation

Les virus, malware et ransomware peuvent réaliser des activités malveillantes comme des vols ou des modifications de données. De telles activités doivent être examinées, mais cela est possible uniquement si vous en conservez une preuve numérique. Cependant, ces preuves numériques, par ex. des fichiers ou des traces d'activité, peuvent être supprimées ou l'ordinateur sur lequel l'activité malveillante s'est produite peut devenir indisponible.

Les sauvegardes avec données d'investigation numérique permettent aux enquêteurs d'analyser des zones de disque qui ne sont généralement pas incluses dans une sauvegarde de disque classique. En activant l'option de sauvegarde **Données d'investigation**, vous pouvez collecter les éléments de preuve numérique suivants qui peuvent être utilisés dans des investigations numériques :

- Instantanés de l'espace disque inutilisé
- Vidages de mémoire
- Instantanés des processus en cours d'exécution

Les sauvegardes avec données d'investigation sont automatiquement notarisées.

© Acronis International GmbH, 2003-2026

L'option de sauvegarde **Données d'investigation** est disponible pour les sauvegardes **Machine complète** de ressources Windows exécutant les systèmes d'exploitation suivants :

- Windows 8.1 et versions ultérieures
- Windows Server 2012 R2 et versions ultérieures

Les sauvegardes avec données d'investigation numérique ne sont pas disponibles pour les ressources suivantes :

- Ressources qui sont connectées au réseau via VPN et n'ont pas d'accès direct à Internet.
- Ressources avec disques chiffrés par BitLocker.

Les sauvegardes avec données d'investigation numérique sont prises en charge par les emplacements de sauvegarde suivants :

- Stockage dans le Cloud
- Dossier réseau
- Dossier local

Remarque
Le dossier local est pris en charge uniquement sur les disques durs connectés à la ressource sauvegardée via USB.
Le stockage sur les disques dynamiques locaux n'est pas pris en charge pour les sauvegardes avec données d'investigation.

Processus de sauvegarde de données d'investigation

Lors d'une sauvegarde de données d'investigation numérique, les opérations suivantes sont effectuées :

1. Un vidage de mémoire brut et une liste des processus en cours de traitement sont capturés.
2. La ressource sauvegardée redémarre et l'interface du support de démarrage s'ouvre.
3. Une sauvegarde incluant l'espace utilisé et l'espace non alloué est créée.
4. Les disques sauvegardés sont notarisés.
5. Le système d'exploitation de la ressource redémarre et d'autres opérations configurées s'exécutent (réplication, rétention, validation, par exemple).

Configuration de la collecte de données d'investigation numérique

Vous pouvez configurer la collecte de données d'investigation numérique en utilisant les options de sauvegarde d'un plan de protection.

Pour configurer la collecte de données d'investigation numérique

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez une ressource, puis cliquez sur **Protéger**.

© Acronis International GmbH, 2003-2026

3. Cliquez sur **Ajouter un plan**, puis sur **Créer un plan** > **Protection**.
4. Dans le plan de protection, assurez-vous que le module **Sauvegarde** est activé et développé.
5. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine**.
6. Pour configurer la collecte de données d'investigation numérique, cliquez dans **Options de sauvegarde** sur **Modifier**.
   a. Cliquez sur **Données d'investigation**.
   b. Activez le commutateur **Collecter les données d'investigation**.
   c. Cliquez sur **Terminé**.

   Remarque
   Vous ne pouvez pas modifier les paramètres de données d'investigation numérique après avoir appliqué le plan de protection. Pour utiliser d'autres paramètres d'investigation numérique, créez et appliquez un nouveau plan.
7. Dans **Où sauvegarder**, spécifiez un emplacement de sauvegarde.
8. Dans **Planification**, configurez la planification du plan.
9. Pour configurer le mot de passe de chiffrement, cliquez dans **Chiffrement** sur **Spécifier un mot de passe**.
   a. Saisissez et confirmez le mot de passe.
   b. Cliquez sur **OK**.
10. Cliquez sur **Créer**.

Un plan de protection est créé et appliqué. Pendant la sauvegarde, un vidage de mémoire et un instantané des processus en cours d'exécution sont capturés. Une fois la sauvegarde terminée, vous pouvez récupérer les données d'investigation numérique et les analyser.

Important
Le vidage mémoire peut contenir des données sensibles telles que des mots de passe.

Récupération des données d'investigation numérique

Vous pouvez récupérer des données d'investigation numérique à partir d'une sauvegarde en téléchargeant ou en restaurant ces données.

Pour récupérer des données d'investigation numérique

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez un emplacement de sauvegarde qui prend en charge les archives de sauvegarde avec des données d'investigation numérique.
3. Sélectionnez une archive de sauvegarde contenant des données d'investigation numérique, puis cliquez sur **Afficher les sauvegardes**.

© Acronis International GmbH, 2003-2026

4. Sélectionnez une sauvegarde (point de restauration) qui contient des données d'investigation numérique, puis cliquez sur **Restaurer**.
5. [Pour télécharger ou restaurer uniquement les fichiers de données d'investigation numérique] Cliquez sur **Données d'investigation**.

   Les fichiers contenant des données d'investigation numérique sont affichés.

   a. [Pour télécharger des fichiers] Sélectionnez un ou plusieurs fichiers, puis cliquez sur **Télécharger**.

   b. [Pour restaurer des fichiers] Sélectionnez un ou plusieurs fichiers, puis cliquez sur **Restaurer**.

   Remarque

   Dans la console Cyber Protect, vous ne pouvez pas télécharger des fichiers de plus de 100 Mo. En général, le fichier de vidage de mémoire (`raw.dmp`) est plus volumineux. Vous pouvez le restaurer, puis le copier.

   Vous pouvez utiliser le vidage mémoire avec un logiciel d'analyse forensique tiers. Par exemple, vous pouvez utiliser Volatility Framework (https://www.volatilityfoundation.org/) pour une analyse mémoire plus approfondie.

6. [Pour restaurer l'intégralité de la sauvegarde] Cliquez sur **Machine complète**.

   a. Configurez les options de restauration.

   b. Cliquez sur **Démarrer la restauration**.

   c. Pour confirmer que vous souhaitez écraser les disques de la machine cible, cliquez sur **Démarrer la restauration**.

   Important

   Pour garantir qu'aucun changement ne soit effectué sur le disque pendant le processus de démarrage, l'ordinateur restauré n'a pas de capacité de démarrage.

Affichage des archives de sauvegarde contenant des données d'investigation numérique

Vous pouvez identifier les archives de sauvegarde qui contiennent des données d'investigation numérique dans la console Cyber Protect.

Pour afficher les archives de sauvegarde contenant des données d'investigation numérique

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Sauvegardes**.
2. Sélectionnez un emplacement de sauvegarde qui prend en charge les archives de sauvegarde avec des données d'investigation numérique.
3. Cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit du tableau, puis sélectionnez **Données d'investigation**.

   La colonne **Données d'investigation** apparaît.
4. Cliquez sur le nom de la colonne pour trier les archives de sauvegarde par la présence de données d'investigation numérique.

© Acronis International GmbH, 2003-2026

Notarisation des sauvegardes avec les données d'investigation

Pour garantir qu'une sauvegarde avec données d'investigation est exactement l'image qui a été prise et qu'elle n'a pas été compromise, le module de sauvegarde fournit la notarisation des sauvegardes avec données d'investigation.

Fonctionnement

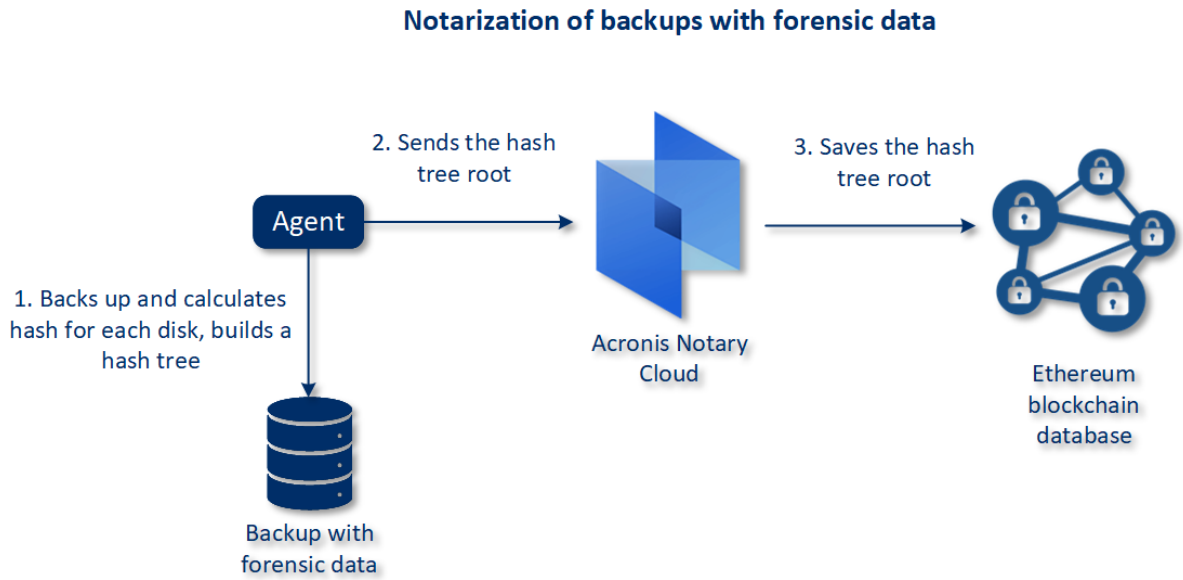
La notarisation vous permet de prouver qu'un disque contenant des données d'investigation est authentique et inchangé depuis sa sauvegarde.

Lors d'une sauvegarde, l'agent calcule les codes de hachage des disques sauvegardés, crée un arbre de hachage, enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données blockchain Ethereum pour s'assurer que cette valeur ne change pas.

Lors de la vérification de l'authenticité d'un disque contenant des données d'investigation, l'agent calcule le hachage du disque, puis le compare avec le hachage stocké dans l'arbre de hachage sauvegardé. Si ces hachages ne correspondent pas, le disque n'est pas authentique. Sinon, l'authenticité du disque est garantie par l'arbre de hachage.

Pour vérifier que l'arbre de hachage n'a pas été compromis, l'agent envoie la racine de l'arbre de hachage au service Notary. Le service Notary la compare avec celle stockée dans la base de données blockchain. Si les hachages correspondent, le disque sélectionné est authentique. Sinon, le logiciel affiche un message indiquant que le disque n'est pas authentique.

Le schéma ci-dessous montre brièvement le processus de notarisation pour les sauvegardes avec données d'investigation.



Pour vérifier manuellement la sauvegarde de disque notarisée, vous pouvez en obtenir le certificat et suivre la procédure de vérification affichée avec le certificat, en utilisant l'outil tibxread.

© Acronis International GmbH, 2003-2026

Obtenir le certificat pour les sauvegardes avec données d'investigation

Pour obtenir le certificat pour une sauvegarde avec données d'investigation, procédez comme suit :

1. Accédez à **Stockage de sauvegarde** et sélectionnez la sauvegarde avec données d'investigation.
2. Restaurez la machine entière.
3. Le système ouvre la vue **Mappage de disque**.
4. Cliquez sur l'icône **Obtenir certificat** pour le disque.
5. Le système génèrera le certificat et ouvrira une nouvelle fenêtre dans votre navigateur, avec le certificat. Sous le certificat s'afficheront les instructions concernant la vérification manuelle de la sauvegarde de disque notarisée.

L'outil « tibxread » pour obtenir les données sauvegardées

Cyber Protection fournit l'outil, intitulé `tibxread`, pour la vérification manuelle de l'intégrité du disque sauvegardé. L'outil vous laisse toujours obtenir les données d'une sauvegarde et calcule le hachage du disque indiqué. L'outil est installé automatiquement avec les composants suivants : Agent pour Windows, agent pour Linux et agent pour Mac.

Le chemin d'installation : le même dossier que celui que détient l'agent (par exemple, `C:\Program Files\BackupClient\BackupAndRecovery`).

Les emplacements pris en charge sont les suivants :

- Le disque local
- Le dossier réseau (CIFS/SMB) auquel vous pouvez accéder sans identifiants.
  En cas de dossier réseau protégé par mot de passe, vous pouvez monter le dossier réseau sur le dossier local à l'aide des outils OS, puis le dossier local comme source pour cet outil.
- Le stockage sur le Cloud
  Vous devez fournir l'URL, le port et le certificat. Vous pouvez obtenir l'URL et le port à partir de la clé de registre Windows ou des fichiers de configuration sur les machines Linux/Mac.
  Pour Windows :

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Pour Linux :

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Pour macOS :

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Vous pouvez trouver le certificat dans les emplacements suivants :

© Acronis International GmbH, 2003-2026

Pour Windows :

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

Pour Linux :

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

Pour macOS :

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

L'outil contient les commandes suivantes :

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

Répertorie les points de restaurations dans une sauvegarde.

SYNOPSIS :

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Modèle de sortie :
```

```
GUID Date Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – un GUID de sauvegarde.

<date> – une date de création de la sauvegarde. Le format est « JJ.MM.AAAA HH24:MM:SS ». En fuseau horaire local par défaut (peut être modifié à l'aide de l'option --utc).

Exemple de sortie :

© Acronis International GmbH, 2003-2026

```
GUID Date Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Répertorie le contenu dans un point de restauration.

SYNOPSIS :

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Modèle de sortie :

```
Disk Size Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> – identificateur du disque.

<size> – taille in octets.

<notarization_status> – les statuts suivants sont possibles : Sans notarisation, Notarisé, Prochaine sauvegarde.

Exemple de sortie :

```
Disk Size Notary status
-------- ------ --------------
1 123123465798 Notarized
2 123123465798 Notarized
```

obtenir le contenu

Écrit le contenu du disque indiqué dans le point de restauration sur la sortie standard (stdout).

SYNOPSIS :

© Acronis International GmbH, 2003-2026

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculer le hachage

Calcule le hachage du disque indiqué dans le point de restauration à l'aide de l'algorithme SHA-2 (256 bits) et l'écrit sur le stdout.

SYNOPSIS :

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Description des options

Option	Description
--arc=BACKUP_NAME	Le nom du fichier de sauvegarde que vous pouvez obtenir depuis les propriétés de sauvegarde de la console Cyber Protect. Le fichier de sauvegarde doit être indiqué par l'extension .tibx.
--backup=RECOVERY_POINT_ID	L'identificateur du point de restauration
--disk=DISK_NUMBER	Numéro de disque (le même que celui écrit sur la sortie de la commande « Obtenir le contenu »)

© Acronis International GmbH, 2003-2026

--loc=URI	Une URI d'emplacement de sauvegarde. Les formats possibles de l'option « --loc » sont :
	• Nom du chemin local (Windows)
	`c:/upload/backups`
	• Nom du chemin local (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Stockage dans le Cloud
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>` – vous le trouverez dans la clé de registre dans Windows : HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
	`<path_to_certificate>` – un chemin vers le fichier du certificat, pour accéder à Cyber Protect Cloud. Par exemple, sous Windows, ce certificat est situé dans `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt` où <username> – est le nom de compte nécessaire pour accéder à Cyber Protect Cloud.

--log=PATH	Permet d'écrire les journaux via le chemin indiqué (chemin local uniquement, le format est le même que pour le paramètre `--loc=URI`). Le niveau de journalisation est DÉBOGAGE.
--password=PASSWORD	Un mot de passe de chiffrement pour votre sauvegarde. Si la sauvegarde n'est pas chiffrée, laissez cette valeur vierge.

--raw	Masque l'en-tête (deux premières lignes) dans la sortie de commande. Ceci est utilisé lorsque la sortie de commande doit être analysée.
	Exemple de sortie sans « `--raw` » :
	`GUID Date Date timestamp`
	`----  ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Sortie avec « `--raw` » :
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Affiche les dates en UTC
--progress	Affiche la progression de l'opération. Par exemple :

© Acronis International GmbH, 2003-2026

	1 % 2 % 3 % 4 % ... 100 %

Troncation de journal

Cette option est effective pour les sauvegardes de bases de données Microsoft SQL Server et pour les sauvegardes de niveau disque avec option de sauvegarde de l'application Microsoft SQL Server activée.

L'option définit si les journaux des transactions SQL Server font l'objet d'une troncation avant la prise d'un instantané au début de l'opération de sauvegarde.

Le préréglage est le suivant : **Activé**.

Lorsque cette option est activée, une base de données peut être restaurée uniquement à un point dans le temps d'une sauvegarde créée par Cyber Protection.

Remarque
Désactivez cette option si vous sauvegardez les journaux de transaction en utilisant le moteur de sauvegarde natif de Microsoft SQL Server.

Prise d'instantanés LVM

Cette option est effective uniquement pour les machines physiques.

Cette option est effective pour la sauvegarde de volumes de niveau disque gérée par Linux Logical Volume Manager (LVM). Ces volumes sont également appelés volumes logiques.

Cette option définit comment prendre un instantané d'un volume logique. Le logiciel de sauvegarde peut effectuer cette opération ou la confier à Linux Logical Volume Manager (LVM).

Le préréglage est le suivant : **Par le logiciel de sauvegarde**.

- **Par le logiciel de sauvegarde**. Les données de l'instantané sont principalement conservées dans RAM. La sauvegarde est plus rapide et l'espace non alloué sur le groupe de volumes n'est pas requis. Par conséquent, nous vous recommandons de ne modifier le préréglage que si vous rencontrez des problèmes avec la sauvegarde de volumes logiques.
- **Par LVM**. L'instantané est stocké dans un espace non alloué du groupe de volumes. Si l'espace non alloué est manquant, l'instantané sera pris par le logiciel de sauvegarde.

L'instantané est utilisé uniquement pendant l'opération de sauvegarde et il est supprimé automatiquement lorsque cette opération est terminée. Aucun fichier temporaire n'est conservé.

© Acronis International GmbH, 2003-2026

Points de montage

Cette option est efficace uniquement sous Windows, pour la sauvegarde de niveau fichier d'une source de données qui inclut des volumes montés ou des volumes partagés de cluster.

Remarque
Pour Linux et macOS, l'option **Points de montage de sauvegarde** est ignorée et le comportement est le suivant :

- Les données des points de montage locaux tels que les disques locaux, les lecteurs USB, etc., sont toujours sauvegardées.
- Les données des points de montage distants tels que les partages CIFS/NFS, etc., ne sont jamais sauvegardées.

Cette option est efficace seulement lorsque vous sélectionnez un dossier à sauvegarder qui est supérieur au point de montage dans l'arborescence des dossiers. (Un point de montage est un dossier sur lequel un volume supplémentaire est logiquement attaché.)

- Si un tel dossier (un dossier parent) est sélectionné pour la sauvegarde, et que l'option **Points de montage** est activée, tous les fichiers situés sur le volume monté seront inclus dans la sauvegarde. Si l'option **Points de montage** est désactivée, le point de montage dans la sauvegarde sera vide.

  Pendant la restauration d'un dossier parent, le contenu du point de montage est ou n'est pas restauré, selon que l'option **Points de montage** pour la restauration est activée ou désactivée.
- Si vous sélectionnez directement le point de montage, ou sélectionnez n'importe quel dossier dans le volume monté, les dossiers sélectionnés seront considérés comme des dossiers ordinaires. Ils seront sauvegardés, peu importe l'état de l'option **Points de montage**, et restaurés peu importe l'état de l'option **Points de montage** pour la restauration.

Le préréglage est le suivant : **Désactivé**.

Remarque
Vous pouvez sauvegarder des machines virtuelles Hyper-V résidant sur un volume partagé de cluster en sauvegardant les fichiers nécessaires ou l'ensemble du volume avec une sauvegarde de niveau fichier. Mettez simplement les machines virtuelles hors tension afin de vous assurer qu'elles sont sauvegardées dans un état cohérent.

Exemple

Supposons que le dossier **C:\Data1** est un point de montage pour le volume monté. Le volume contient les dossiers **Folder1** et **Folder2**. Vous créez un plan de protection pour la sauvegarde de niveau fichier de vos données.

Si vous cochez la case pour le volume C et activez l'option **Points de montage**, le dossier **C:\Data1** dans votre sauvegarde contiendra les dossiers **Folder1** et **Folder2**. Lorsque vous restaurez les

© Acronis International GmbH, 2003-2026

données sauvegardées, soyez conscient de la bonne utilisation de l'option **Points de montage** pour la restauration.

Si vous cochez la case pour le volume C et désactivez l'option **Points de montage**, le dossier **C:\Data1** dans votre sauvegarde sera vide.

Si vous cochez la case pour les dossiers **Data1**, **Folder1** ou **Folder2**, les dossiers cochés seront inclus dans la sauvegarde comme des dossiers ordinaires, peu importe l'état de l'option **Points de montage**.

Snapshot Multi-volume

Cette option est effective pour les sauvegardes des machines physiques sous Windows ou Linux.

Cette option s'applique à une sauvegarde de niveau disque. Cette option s'applique également à une sauvegarde de niveau fichier lorsque la sauvegarde de niveau fichier est effectuée en réalisant un instantané. (L'option « Image statique de sauvegarde de niveau fichier » détermine si un instantané est pris pendant la sauvegarde de niveau fichier).

Cette option détermine si des instantanés de plusieurs volumes doivent être pris simultanément ou un par un.

Le préréglage est le suivant :

- Si au moins une machine sous Windows est sélectionnée pour la sauvegarde : **Activé**.
- Sinon : **Désactivé**.

Lorsque cette option est activée, des instantanés de tous les volumes en cours de sauvegarde sont créés simultanément. Utilisez cette option pour créer une sauvegarde cohérente dans le temps de données éparpillées sur plusieurs volumes, par exemple pour une base de données Oracle.

Lorsque cette option est désactivée, les instantanés des volumes sont pris l'un après l'autre. Par conséquent, si les données sont éparpillées sur plusieurs volumes, la sauvegarde en résultant peut ne pas être cohérente.

Restauration en un seul clic

Avec la restauration en un clic, vous pouvez restaurer automatiquement une sauvegarde de disque de votre ordinateur Windows ou Linux. La sauvegarde peut être de l'ordinateur entier ou de disques ou volumes spécifiques sur l'ordinateur. Les ordinateurs avec démarrage sécurisé et chiffrement BitLocker sont pris en charge.

La restauration en un seul clic prend en charge les opérations suivantes :

- Restauration automatique à partir de la dernière sauvegarde
- Restauration à partir d'une sauvegarde spécifique (également appelée point de restauration) dans l'archive de sauvegarde

La restauration en un seul clic prend en charge les stockages de sauvegarde suivants :

© Acronis International GmbH, 2003-2026

- Secure Zone
- Dossier réseau
- Stockage dans le Cloud

Important
Suspendez le chiffrement BitLocker jusqu'au prochain redémarrage de votre ordinateur lorsque vous effectuez l'une des opérations suivantes :

- Créer, modifier ou supprimer Secure Zone.
- Activer ou désactiver Startup Recovery Manager.
- [Uniquement si Startup Recovery Manager n'a pas déjà été activé] Exécuter la première sauvegarde après avoir activé la restauration en un seul clic dans le plan de protection. Cette opération active automatiquement Startup Recovery Manager.
- Mettre à jour Startup Recovery Manager, par exemple en mettant à jour la protection.

Si le chiffrement BitLocker n'a pas été suspendu au cours de ces opérations, vous devrez spécifier votre code PIN BitLocker après avoir redémarré votre ordinateur.

Activation de la restauration en un clic

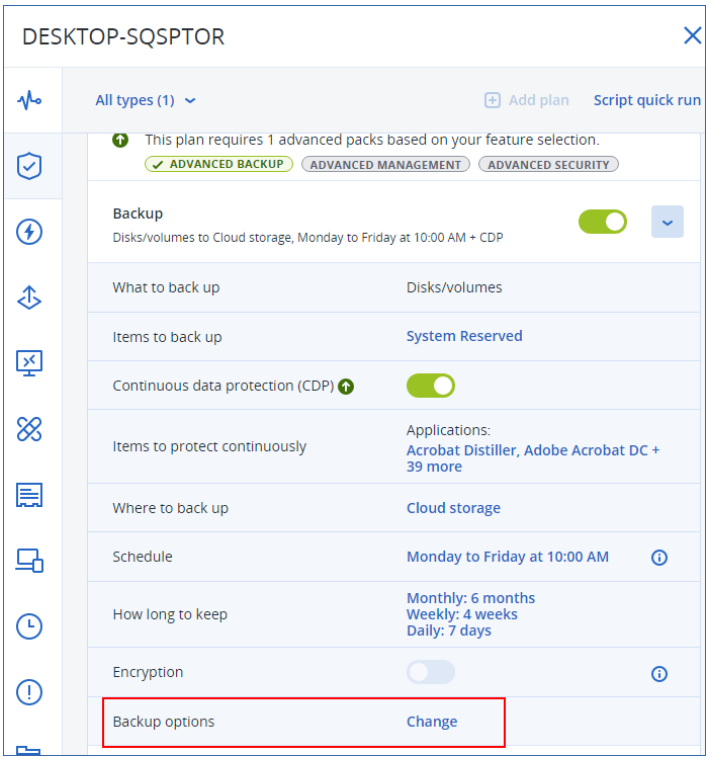
La restauration en un clic est une option de sauvegarde dans le plan de protection. Pour plus d'informations sur la création d'un plan, voir "Création d'un plan de protection" (p. 244).

Remarque
L'activation de la restauration en un clic active également Startup Recovery Manager sur la machine cible. Si Startup Recovery Manager ne peut pas être activé, l'opération de sauvegarde qui crée des sauvegardes de restauration en un clic échouera. Pour plus d'informations sur Startup Recovery Manager, voir "Startup Recovery Manager" (p. 1012).

Pour activer la restauration en un clic

1. Dans le plan de protection, développez le module **Sauvegarde**.
2. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine** ou **Disque/volumes**.
3. [Si vous avez sélectionné **Disque/volumes**]. Dans **Éléments à sauvegarder**, spécifiez le disque ou les volumes à sauvegarder.
4. Dans **Options de sauvegarde**, cliquez sur **Modifier**, puis sélectionnez **Restauration en un seul clic**.

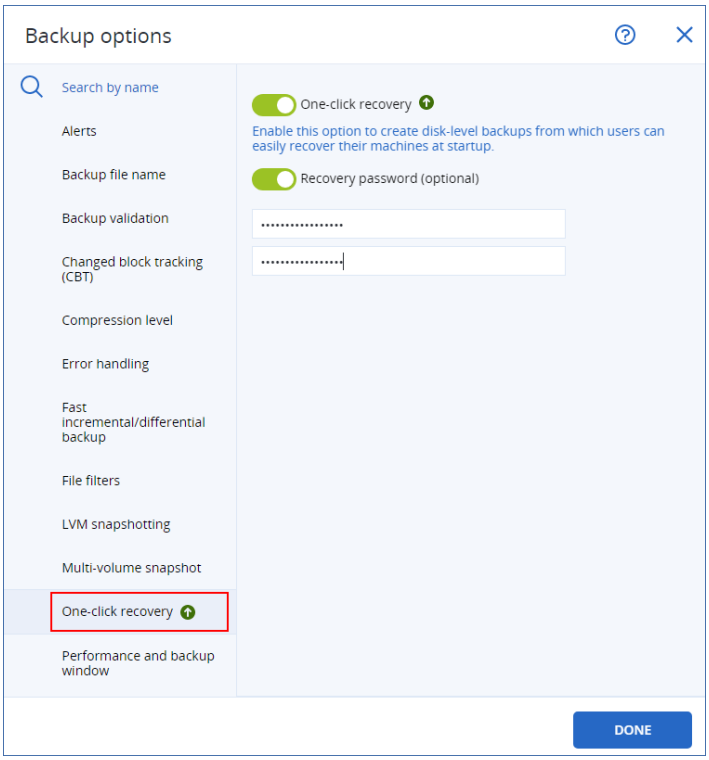
© Acronis International GmbH, 2003-2026



5. Activez le commutateur **Restauration en un seul clic**.
6. [Facultatif] Activez le commutateur **Mot de passe de restauration**, puis définissez un mot de passe.

Important
Nous vous recommandons vivement de spécifier un mot de passe de reprise. Assurez-vous que l'utilisateur qui exécute la restauration en un seul clic sur la machine cible connaît ce mot de passe.

© Acronis International GmbH, 2003-2026



7. Cliquez sur **Terminé**.
8. Configurez les autres éléments du plan de protection selon vos besoins, puis enregistrez le plan.

En conséquence, après que le plan de protection a été exécuté et a créé une sauvegarde, la restauration en un seul clic devient accessible aux utilisateurs de la machine protégée.

Désactivation de la Restauration en un clic

Vous pouvez désactiver la Restauration en un clic pour une ressource spécifique de la manière suivante :

- Désactivez l'option **Restauration en un clic** dans le plan de protection appliqué à la ressource.
- Révoquez le plan de protection dans lequel l'option **Restauration en un clic** est activée.
- Supprimez le plan de protection dans lequel l'option **Restauration en un clic** est activée.

Restauration d'une machine à l'aide de la restauration en un seul clic

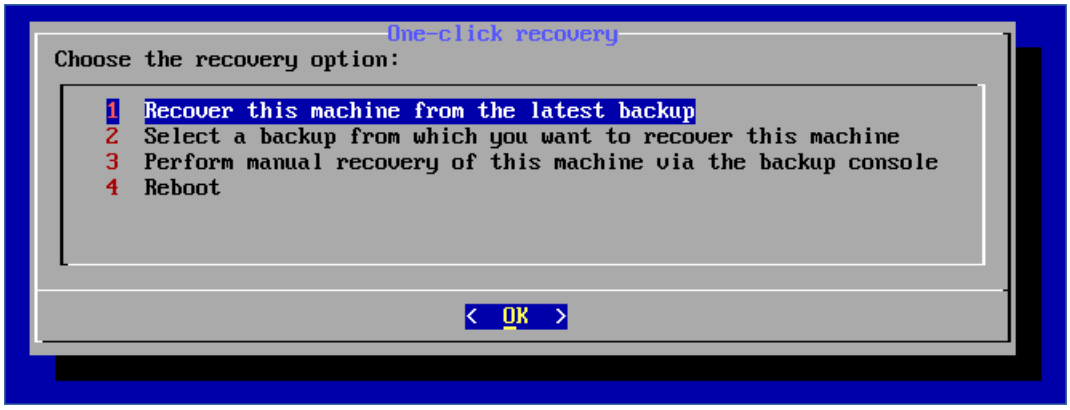
Prérequis

- Un plan de protection avec l'option de sauvegarde **Restauration en un seul clic** activée est appliqué à l'ordinateur.
- Il existe au moins une sauvegarde de disque de l'ordinateur.

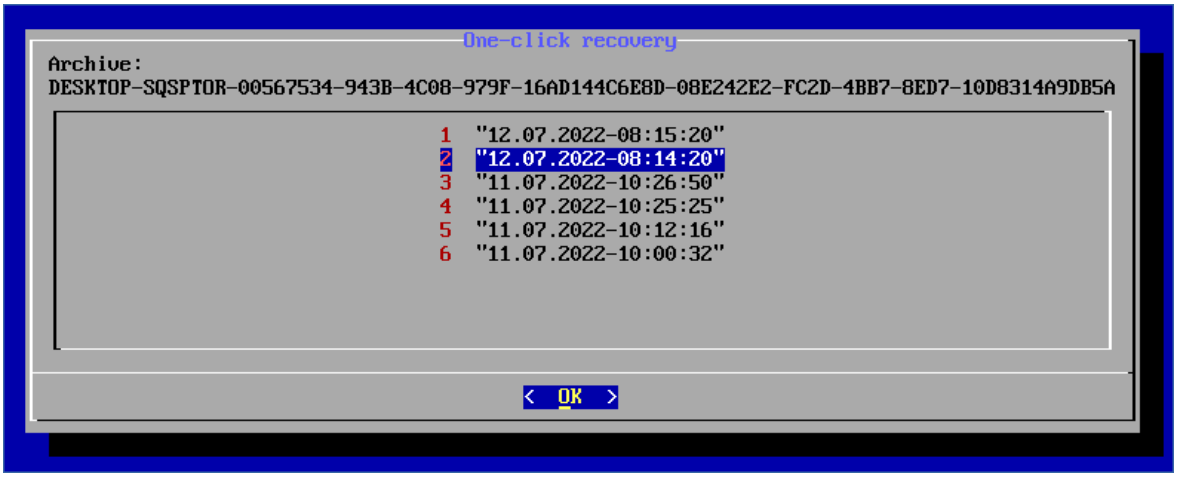
Pour restaurer une machine

© Acronis International GmbH, 2003-2026

1. Redémarrez la machine que vous voulez restaurer.
2. Lors du redémarrage, appuyez sur F11 pour entrer dans Startup Recovery Manager.
   La fenêtre de support de secours s'ouvre.
3. Sélectionnez **Acronis Cyber Protect**.
4. [Si un mot de passe de restauration a été indiqué dans le plan de protection] Saisissez le mot de passe de restauration, puis, cliquez sur **OK**.
5. Sélectionnez une option de restauration en un seul clic.
   - Pour restaurer automatiquement la dernière sauvegarde en date, sélectionnez la première option, puis cliquez sur **OK**.
   - Pour restaurer une autre sauvegarde dans l'archive de sauvegardes, sélectionnez la deuxième option, puis cliquez sur **OK**.

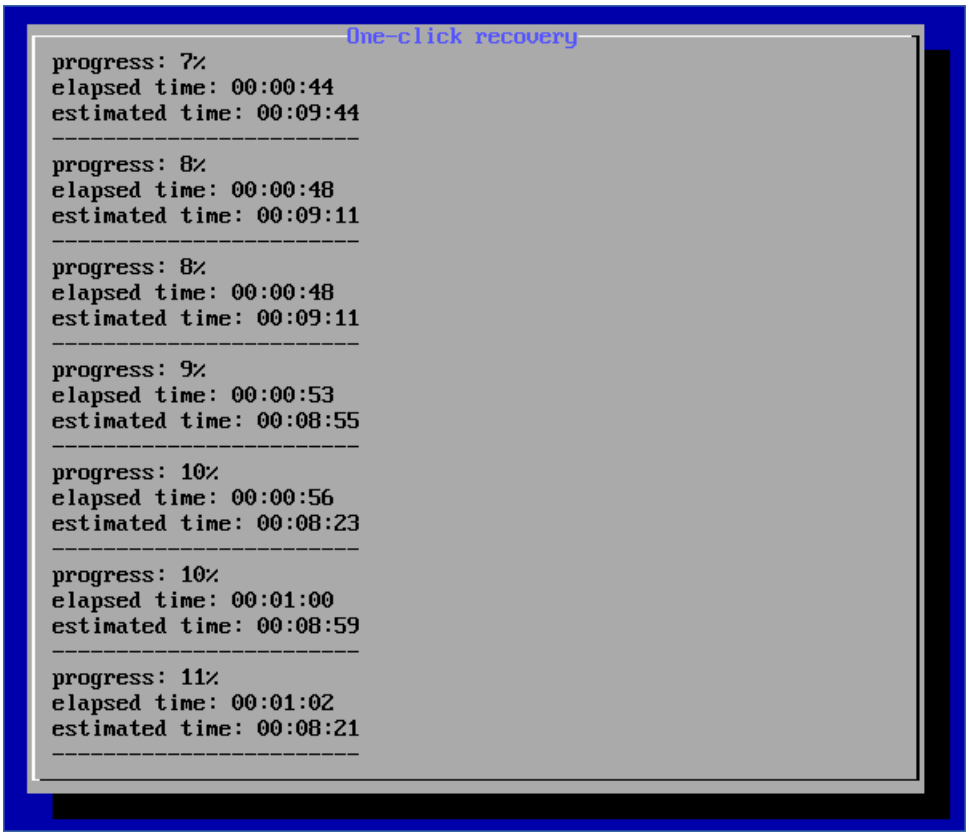


6. Confirmez votre choix en cliquant sur **Oui**.
   La fenêtre de support de secours s'ouvre, puis disparaît. La procédure de restauration se poursuit sans cette interface.
7. [Si vous avez choisi de restaurer une sauvegarde spécifique] Sélectionnez la sauvegarde que vous souhaitez restaurer, puis cliquez sur **OK**.



Au bout d'un temps, la restauration commence et sa progression s'affiche. Une fois la restauration terminée, votre ordinateur redémarre.

© Acronis International GmbH, 2003-2026



Performance et créneau de sauvegarde

Cette option vous permet de définir l'un de trois niveaux de performances de sauvegarde (faibles, élevées, interdites) pour chaque heure au cours d'une semaine. Ainsi, vous pouvez définir une fenêtre de temps pendant laquelle les sauvegardes seront autorisées à démarrer et s'exécuter. Les performances faibles et élevées sont configurables sur le plan de la priorité du processus et de la vitesse de sortie.

Cette option n'est pas disponible pour les sauvegardes exécutées par les agents Cloud, telles que les sauvegardes de sites Web ou celles de serveurs situés sur le site de restauration du Cloud.

Cette option est effective uniquement pour les processus de sauvegarde et de réplication de sauvegarde. Les commandes post-sauvegarde et d'autres opérations incluses dans un plan de protection (par exemple, la validation) s'exécuteront en dépit de cette option.

Le préréglage est le suivant : **Désactivé**.

Quand cette option est désactivée, les sauvegardes sont autorisées à s'exécuter à tout moment, avec les paramètres suivants (cela n'a pas d'importance si les paramètres ont été modifiés par rapport à la valeur préréglée) :

- Priorité du processeur : **Faible** (dans Windows, cela correspond à **Inférieure à la normale**)
- Vitesse de sortie : **Illimitée**

© Acronis International GmbH, 2003-2026

Lorsque cette option est activée, les sauvegardes planifiées sont autorisées ou bloquées en fonction des paramètres de performances spécifiés pour l'heure courante. Au début d'une heure où les sauvegardes sont bloquées, un processus de sauvegarde est automatiquement arrêté et une alerte est générée. Même si les sauvegardes planifiées sont bloquées, une sauvegarde peut être lancée manuellement. Elle utilisera les paramètres de performances de la dernière heure au cours de laquelle les sauvegardes ont été autorisées.

Remarque
Vous pouvez configurer les performances et la fenêtre de sauvegarde pour chaque emplacement de réplication individuellement. Pour accéder aux paramètres de l'emplacement de réplication, cliquez dans le plan de protection sur l'icône en forme d'engrenage située à côté du nom de l'emplacement, puis sur **Performances et fenêtre de sauvegarde**.

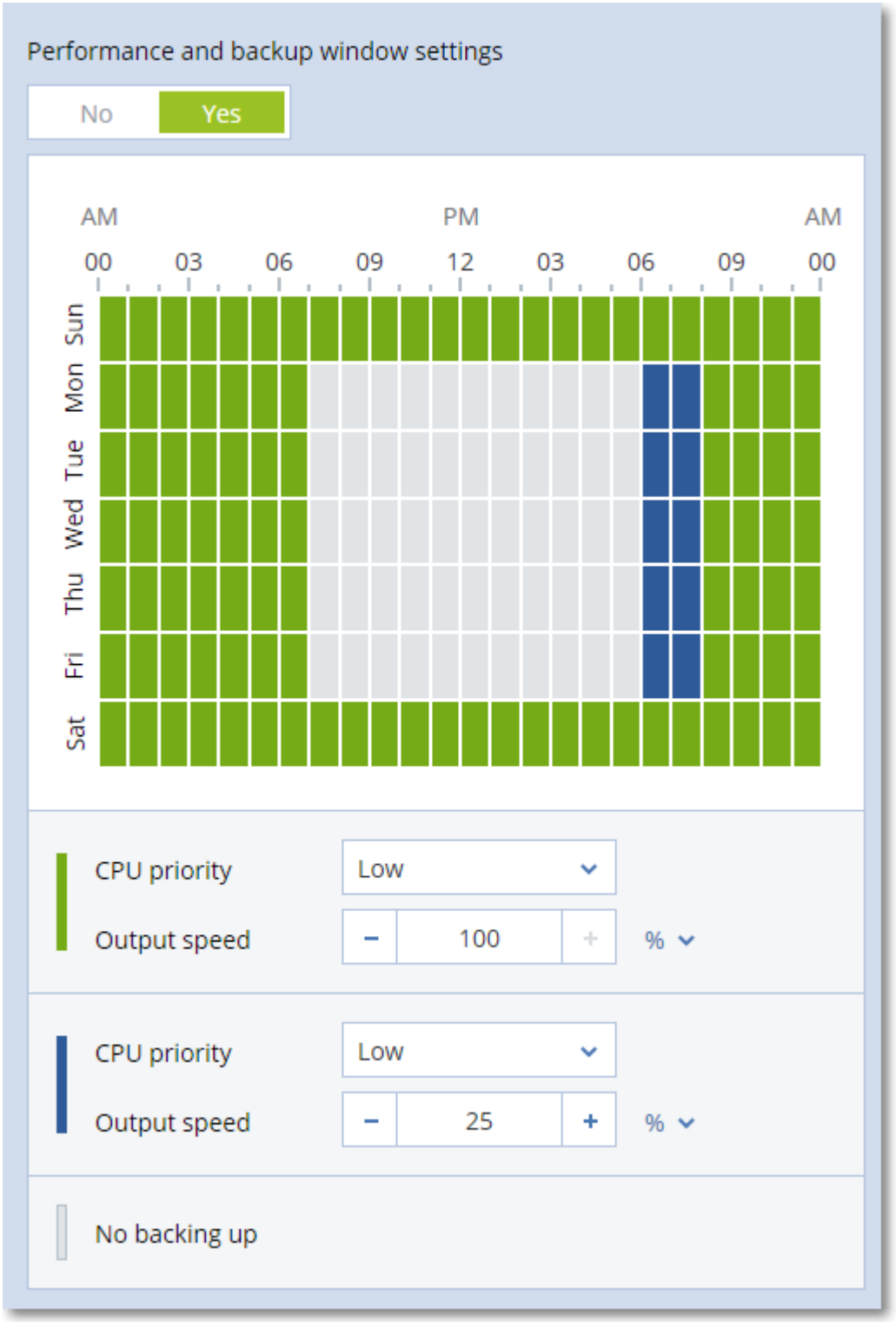
Créneau de sauvegarde

Chaque rectangle représente une heure au cours d'un jour de semaine. Cliquez sur un rectangle pour parcourir les états suivants :

- **Vert :** la sauvegarde est autorisée avec les paramètres spécifiés dans la section verte ci-dessous.
- **Bleu :** la sauvegarde est autorisée avec les paramètres spécifiés dans la section bleue ci-dessous. Cet état est indisponible si le format de sauvegarde est défini sur **Version 11**.
- **Gris :** la sauvegarde est bloquée.

Vous pouvez cliquer et faire glisser pour changer simultanément l'état de plusieurs rectangles.

© Acronis International GmbH, 2003-2026



Priorité de CPU

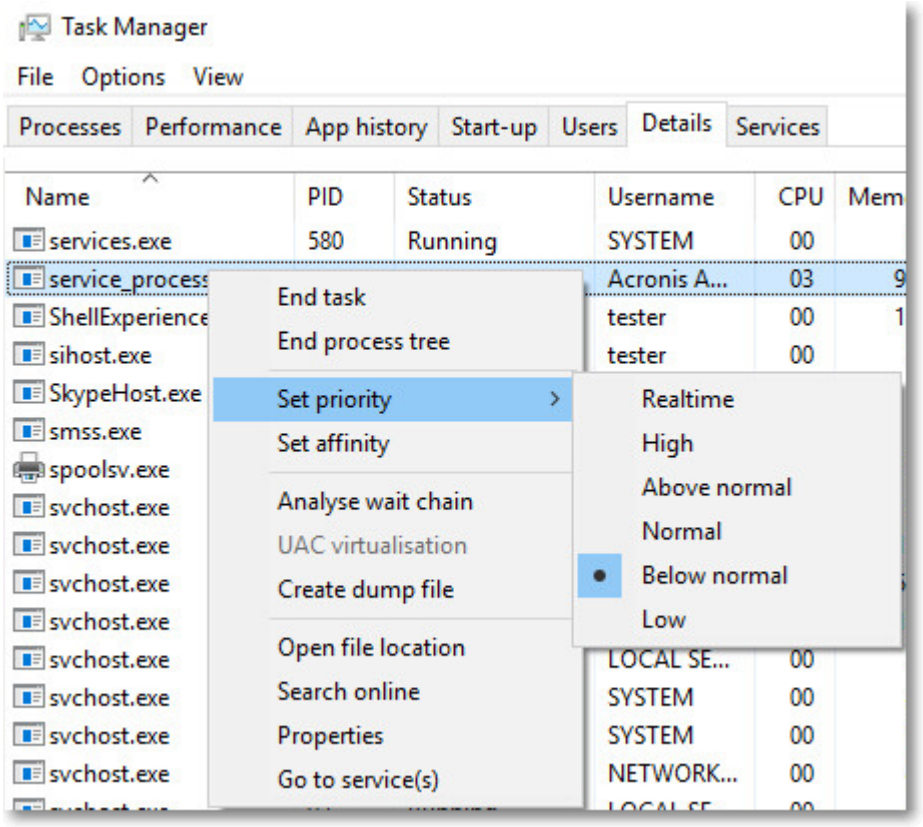
Ce paramètre définit la priorité du processus de sauvegarde dans le système d'exploitation.

Les paramètres disponibles sont les suivants : **Basse**, **Normale**, **Élevé**.

© Acronis International GmbH, 2003-2026

Le degré de priorité des processus exécutés dans un système détermine le niveau d'utilisation du processeur et la quantité de ressources système qui leur sont allouées. Réduire la priorité de sauvegarde libérera davantage de ressources pour les autres applications. Augmenter la priorité de sauvegarde pourrait accélérer le processus de sauvegarde en imposant au système d'exploitation d'allouer plus de ressources, par exemple de processeur, à l'application de sauvegarde. Cependant, l'effet correspondant dépendra de l'utilisation globale du processeur ainsi que d'autres facteurs comme la vitesse d'E/S du disque ou le trafic réseau.

Cette option définit la priorité du processus de sauvegarde (**service_process.exe**) sous Windows et le caractère agréable du processus de sauvegarde (**service_process**) sous Linux et macOS.



Le tableau ci-dessous répertorie le mappage de ce paramètre sous Windows, Linux et macOS.

Priorité Cyber Protection	Priorité Windows	Caractère agréable Linux et macOS
Faible	Inférieure à la normale	10
Normal	Normal	0
Élevée	Élevée	-10

© Acronis International GmbH, 2003-2026

Vitesse de sortie au cours de la sauvegarde

Ce paramètre vous permet de limiter la vitesse d'écriture du disque dur (lors d'une sauvegarde dans un dossier local) ou la vitesse de transfert des données de la sauvegarde via le réseau (lors d'une sauvegarde sur un espace de stockage sur le Cloud ou un partage réseau).

Lorsque cette option est activée, vous pouvez spécifier la vitesse de sortie maximum autorisée :

- En tant que pourcentage de l'estimation de la vitesse d'écriture du disque dur de destination (lors d'une sauvegarde dans un dossier local) ou de l'estimation de la vitesse maximale de la connexion réseau (lors d'une sauvegarde sur un espace de stockage sur le Cloud ou un partage réseau).

  Ce paramètre fonctionne uniquement si l'agent est en cours d'exécution sous Windows.
- En ko/seconde (pour toutes les destinations).

Envoi de données physiques

Cette option est disponible si la destination de la sauvegarde ou de la réplication est le stockage dans le cloud et que le format de sauvegarde est défini sur **Version 12**.

Cette option est effective pour les sauvegardes de lecteur et pour les sauvegardes de fichier créées par l'agent pour Windows, l'agent pour Linux, l'agent pour Mac, l'agent pour VMware, l'agent pour Hyper-V et l'agent pour Virtuozzo.

Utilisez cette option pour envoyer la première sauvegarde complète créée par le plan de protection vers le stockage dans le Cloud ou sur un disque dur à l'aide du service d'envoi de données physiques. Les sauvegardes incrémentielles suivantes seront effectuées via le réseau.

Pour les sauvegardes locales qui sont répliquées vers le Cloud, les sauvegardes incrémentielles se poursuivent et sont enregistrées en local jusqu'à ce que la sauvegarde initiale soit chargée sur le stockage dans le Cloud. Ensuite, toutes les modifications incrémentielles sont répliquées vers le Cloud et la réplication se poursuit conformément à la planification.

Le préréglage est le suivant : **Désactivé.**

À propos du service d'envoi de données physiques

L'interface Web du service d'envoi de données physiques est disponible uniquement pour les administrateurs.

Pour des instructions détaillées concernant l'utilisation du service d'envoi de données physiques et l'outil de création de commandes, consultez le Guide de l'administrateur sur le service d'envoi de données physiques. Pour accéder à ce document dans l'interface Web du service d'envoi de données physiques, cliquez sur l'icône en forme de point d'interrogation.

© Acronis International GmbH, 2003-2026

Présentation du processus d'envoi de données physiques

1. [Pour envoyer des sauvegardes dont l'emplacement de sauvegarde principal est le stockage dans le Cloud]
   a. Créer un nouveau plan de protection avec sauvegarde sur le Cloud.
   b. Sur la ligne **options de sauvegarde**, cliquez sur **Modifier**.
   c. Dans la liste des options disponibles, cliquez sur **Envoi de données physiques**.

   Vous pouvez sauvegarder directement vers un lecteur amovible ou sauvegarder vers un dossier local ou réseau, puis copier/déplacer la (les) sauvegarde(s) vers le lecteur.
2. [Pour envoyer des sauvegardes locales qui sont répliquées vers le Cloud]

   Remarque
   Cette option est prise en charge avec l'agent de protection à partir de la version C21.06.

   a. Créer un nouveau plan de protection avec sauvegarde dans un stockage local ou réseau.
   b. Cliquez sur **Ajouter un emplacement** et sélectionnez **Stockage dans le Cloud**.
   c. Sur la ligne d'emplacement **Stockage dans le Cloud**, cliquez sur la roue d'engrenage et sélectionnez **Envoi de données physiques**.
3. Sous **Utiliser l'envoi de données physiques**, cliquez sur **Oui** puis sur **Terminé**.
   L'option Chiffrement est automatiquement activée dans le plan de protection, car toutes les sauvegardes qui sont envoyées doivent être chiffrées.
4. Sur la ligne **Chiffrement**, cliquez sur **Spécifier un mot de passe** et saisissez un mot de passe pour le chiffrement.
5. Sur la ligne **Envoi de données physiques**, sélectionnez le lecteur amovible sur lequel la sauvegarde initiale sera enregistrées.
6. Cliquez sur **Créer** pour enregistrer le plan de protection.
7. Une fois la première sauvegarde effectuée, utilisez l'interface Web du service d'envoi de données physiques pour télécharger l'outil de création de commandes et créez la commande.
   Pour accéder à cette interface Web, connectez-vous au portail de gestion, cliquez sur **Vue d'ensemble** > **Utilisation**, puis cliquez sur **Gérer le service** ou sur **Envoi de données physiques**.

   Important
   Une fois la sauvegarde complète initiale effectuée, les sauvegardes suivantes doivent être effectuées selon le même plan de protection. Un autre plan de protection, y compris avec des paramètres et une machine identiques, nécessitera un autre cycle d'envoi de données physiques.
8. Emballez les lecteurs et envoyez-les au centre de données.

© Acronis International GmbH, 2003-2026

Important
Assurez-vous de suivre les instructions d'emballage fournies dans le Guide de l'administrateur sur le service d'envoi de données physiques.

9. Suivez le statut de la commande en utilisant l'interface Web du service d'envoi de données physiques. Veuillez noter que les sauvegardes suivantes échoueront jusqu'à ce que la sauvegarde initiale soit téléchargée sur le stockage sur le Cloud.

Commandes Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la procédure de sauvegarde.

Le modèle suivant illustre quand les commandes pre/post sont exécutées.

Commandes avant la sauvegarde	Sauvegarde	Commande après la sauvegarde

Exemples d'utilisation des commandes pre/post :

- Supprimer certains fichiers temporaires du disque avant de démarrer la sauvegarde.
- Configurer un produit antivirus tiers pour qu'il démarre chaque fois avant le début de la sauvegarde.
- Copier sélectivement des sauvegardes vers un autre emplacement. Cette option peut être utile car la réplication configurée dans un plan de protection copie *chaque* sauvegarde vers les emplacements suivants.

L'agent effectue la réplication *après* l'exécution de la commande post-sauvegarde.

Le programme ne prend pas en charge de commandes interactives, c'est-à-dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).

Commandes avant la sauvegarde

Pour spécifier une commande ou un fichier lot à exécuter avant le démarrage de la sauvegarde

1. Activez le commutateur **Exécuter une commande avant la sauvegarde**.
2. Dans le champ **Chemin d'accès de la commande ou du fichier lot sur la machine avec un agent**, saisissez une commande ou parcourez un fichier lot.
   Les commandes qui nécessitent une saisie de l'utilisateur (par exemple, `pause`) ne sont pas prises en charge.
   Si vous utilisez PowerShell, passez la commande comme argument à `powershell.exe`.
   Par exemple, utilisez :

   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```

   au lieu de :

© Acronis International GmbH, 2003-2026

```
New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
```

3. Dans le champ **Répertoire de travail**, spécifiez un chemin vers un répertoire où la commande ou le fichier lot sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments de la commande, si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Terminé**.

Case à cocher	**Sélection**			
Faire échouer la sauvegarde si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas sauvegarder tant que l'exécution de la commande n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
Résultat				
	Préréglage Effectuer la sauvegarde uniquement si la commande a été exécutée avec succès. Faire échouer la sauvegarde si l'exécution de la commande échoue.	Effectuer la sauvegarde après l'exécution de la commande a été exécutée, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Effectuer la sauvegarde en même temps que l'exécution de la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Remarque
Si un script échoue en raison d'un conflit lié à une version de bibliothèque obligatoire dans Linux, excluez les variables d'environnement `LD_LIBRARY_PATH` et `LD_PRELOAD`, en ajoutant les lignes suivantes à votre script :

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```


© Acronis International GmbH, 2003-2026

Commande après la sauvegarde

Pour spécifier une commande ou un fichier lot à exécuter une fois la sauvegarde terminée

1. Activez le commutateur **Exécuter une commande après la sauvegarde**.
2. Dans le champ **Chemin d'accès de la commande ou du fichier lot sur la machine avec un agent**, saisissez une commande ou parcourez un fichier lot.
   Les commandes qui nécessitent une saisie de l'utilisateur (par exemple, `pause`) ne sont pas prises en charge.
   Si vous utilisez PowerShell, passez la commande comme argument à `powershell.exe`.
   Par exemple, utilisez :
   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```
   au lieu de :
   ```
   New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
   ```
3. Dans le champ **Répertoire de travail**, spécifiez un chemin vers un répertoire où la commande ou le fichier lot sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments de la commande, si nécessaire.
5. Si l'exécution réussie de la commande est critique, cochez la case **Faire échouer la sauvegarde si l'exécution de la commande échoue**.
   Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.
   Si l'exécution de la commande échoue, l'état de la sauvegarde est défini sur **Erreur**.
   Si la case à cocher **Faire échouer la sauvegarde si l'exécution de la commande échoue** n'est pas sélectionnée, le résultat de l'exécution de la commande n'affecte pas l'état de la sauvegarde.
   Vous pouvez vérifier le résultat de l'exécution de la commande dans l'onglet **Activités**.
6. Cliquez sur **Terminé**.

Commandes de capture de données Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la capture des données (c'est à dire, la prise de l'instantané des données). La capture des données est exécutée au début de la procédure de sauvegarde.

Le modèle suivant illustre le moment où les commandes avant/après capture de données sont exécutées.

	<---------- **Sauvegarde** ---------->				
Commandes avant la sauvegarde	Commande avant la capture de données	Capture des données	Commande après la capture de données	Écrire des données dans le jeu de sauvegarde	Commande après la sauvegarde

© Acronis International GmbH, 2003-2026

Interaction avec d'autres options de sauvegarde

L'exécution de commandes avant/après capture de données peut être modifiée par d'autres options de sauvegarde.

Si l'option **Instantané Multi-volume** est activée, les commandes avant/après capture de données ne seront exécutées qu'une seule fois, car les instantanés pour tous les volumes sont créés simultanément. Si l'option **Instantané Multi-volume** est désactivée, les commandes avant/après capture de données seront exécutées pour chaque volume sauvegardé, car les instantanés sont créés de manière séquentielle, un instantané après l'autre.

Si l'option **Service de cliché instantané des volumes (VSS)** est activée, les commandes avant/après capture des données et les actions Microsoft VSS seront exécutées comme suit :

Commandes avant capture des données > *Suspension de VSS* > *Capture des données* > *Reprise de VSS* > *Commandes après capture des données*

À l'aide des commandes de capture des données avant/après, vous pouvez suspendre et redémarre une base de données ou une application qui n'est pas compatible avec VSS. La capture des données prenant quelques secondes, le temps durant lequel la base de données ou l'application seront ralenties sera minimal.

Commande avant la capture de données

Pour spécifier une commande ou un fichier lot à exécuter avant la capture des données

1. Activez le commutateur **Exécuter une commande avant la capture des données**.
2. Dans le champ **Chemin d'accès de la commande ou du fichier lot sur la machine avec un agent**, saisissez une commande ou parcourez un fichier lot.
   Les commandes qui nécessitent une saisie de l'utilisateur (par exemple, `pause`) ne sont pas prises en charge.
   Si vous utilisez PowerShell, passez la commande comme argument à `powershell.exe`.
   Par exemple, utilisez :

   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```

   au lieu de :

   ```
   New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
   ```
3. Dans le champ **Répertoire de travail**, spécifiez un chemin vers un répertoire où la commande ou le fichier lot sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments de la commande, si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Case à cocher	Sélection			
Faire échouer la sauvegarde si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas exécuter la saisie des données tant que l'exécution de la commande n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
	Résultat			
	Préréglage Effectuer la capture des données uniquement si la commande a été exécutée avec succès. Faire échouer la sauvegarde si l'exécution de la commande échoue.	Effectuer la sauvegarde après l'exécution de la commande, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Effectuer la capture des données en même temps que la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Remarque
Si un script échoue en raison d'un conflit lié à une version de bibliothèque obligatoire dans Linux, excluez les variables d'environnement `LD_LIBRARY_PATH` et `LD_PRELOAD`, en ajoutant les lignes suivantes à votre script :

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Commande après la capture de données

Pour spécifier une commande ou un fichier lot à exécuter après la capture des données

© Acronis International GmbH, 2003-2026

1. Activez le commutateur **Exécuter une commande après la capture des données**.
2. Dans le champ **Chemin d'accès de la commande ou du fichier lot sur la machine avec un agent**, saisissez une commande ou parcourez un fichier lot.

   Les commandes qui nécessitent une saisie de l'utilisateur (par exemple, `pause`) ne sont pas prises en charge.

   Si vous utilisez PowerShell, passez la commande comme argument à `powershell.exe`.

   Par exemple, utilisez :

   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```

   au lieu de :

   ```
   New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
   ```
3. Dans le champ **Répertoire de travail**, spécifiez un chemin vers un répertoire où la commande ou le fichier lot sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments de la commande, si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Terminé**.

Case à cocher	**Sélection**			
Faire échouer la sauvegarde si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas sauvegarder tant que l'exécution de la commande n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
Résultat				
	Préréglage Continuer la sauvegarde uniquement si la commande a été exécutée avec succès.	Effectuer la sauvegarde après l'exécution de la commande a été exécutée, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Continuer la sauvegarde en même temps que l'exécution de la commande et quel que soit le résultat de l'exécution de la commande.

© Acronis International GmbH, 2003-2026

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Planification

Cette option définit si les sauvegardes commencent exactement telles qu'elles sont planifiées ou en différé, et indique le nombre de machines virtuelles sauvegardées simultanément.

Pour plus d'informations sur la configuration du calendrier de sauvegarde, voir "Exécution d'une sauvegarde à partir d'une planification" (p. 574).

Le préréglage est le suivant : **Répartir les heures de démarrage de sauvegarde dans une fenêtre de temps**. **Retard maximum** : **30 minutes**.

Vous pouvez sélectionner l'une des options suivantes :

- **Démarrer toutes les sauvegardes exactement comme planifié**
  Les sauvegardes des machines virtuelles commenceront exactement comme planifié. Les machines seront sauvegardées une par une.
- **Répartir les heures de démarrage dans une fenêtre de temps**
  La sauvegarde des machines physiques commencera en différé selon l'heure planifiée. La valeur de délai pour chaque machine est sélectionnée de façon aléatoire et comprise entre zéro et la valeur maximale que vous spécifiez. Il se peut que vous souhaitiez utiliser ce paramètre lors de sauvegarde de machines multiples sur un emplacement réseau, pour éviter une charge excessive du réseau. La valeur du délai pour chaque machine est déterminée quand le plan de protection est appliqué à la machine, et reste la même tant que vous n'avez pas modifié le plan de protection et changé la valeur de délai maximal.
  Les machines seront sauvegardées une par une.
- **Limiter le nombre de sauvegardes simultanées par**
  Utilisez cette option pour gérer la sauvegarde parallèle de machines virtuelles sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent).
  Les plans de protection dans lesquels cette option est sélectionnée peuvent s'exécuter simultanément avec d'autres plans de protection gérés par le même agent. Lorsque vous sélectionnez cette option, vous devez indiquer le nombre de sauvegardes parallèles par plan. Le nombre total d'ordinateurs sauvegardés simultanément par tous les plans est limité à 10 par agent. Pour plus d'informations sur la modification de la limite par défaut, voir "Limite le nombre total de machines virtuelles sauvegardées simultanément." (p. 986).
  Les plans de protection dans lesquels cette option n'est pas sélectionnée exécutent les opérations de sauvegarde de manière séquentielle, une machine virtuelle après l'autre.

Sauvegarde secteur par secteur

Cette option est effective uniquement pour une sauvegarde de niveau disque.

Cette option définit si une copie exacte d'un disque ou d'un volume sur un niveau physique doit être créée.

Le préréglage est le suivant : **Désactivé**.

© Acronis International GmbH, 2003-2026

Si cette option est activée, tous les secteurs du disque ou du volume seront sauvegardés, y compris l'espace non alloué et les secteurs qui ne contiennent aucunes données. La sauvegarde obtenue sera de la même taille que le disque en cours de sauvegarde (si l'option Niveau de compression est définie sur **Aucune**). Le logiciel passe automatiquement en mode secteur par secteur lorsque la sauvegarde présente des systèmes de fichiers non reconnus ou non pris en charge.

Remarque
Il sera impossible d'exécuter une restauration des données d'application à partir des sauvegardes créées en mode secteur par secteur.

Fractionnement

Lors de la création d'un plan de protection, vous pouvez sélectionner la méthode de fractionnement des sauvegardes volumineuses en petits fichiers.

Remarque
Le fractionnement n'est pas disponible dans les plans de protection qui utilisent le stockage dans le cloud en tant qu'emplacement de sauvegarde secondaire.

L'option par défaut est :

- Si l'emplacement de sauvegarde est un dossier local ou réseau (SMB), et si le format de sauvegarde est TIBX (Version 12) : **Taille fixe : 200 Go**
  Ce paramètre permet au logiciel de sauvegarde de fonctionner avec des volumes de données importants sur les systèmes de fichiers NTFS, sans que la fragmentation de fichiers ne cause d'effets indésirables.
- Sinon : **Automatique**

Les paramètres suivants sont disponibles :

- **Automatique**
  Une sauvegarde sera fractionnée si elle excède la taille de fichier maximum prise en charge par le système de fichiers.
- **Taille fixe**
  Saisissez la taille de fichier souhaitée ou sélectionnez-la dans la liste déroulante, puis enregistrez le plan.

Remarque
Le changement de l'option de fractionnement dans un plan de sauvegarde n'a pas d'incidence sur les archives déjà créées.

Traitement de l'échec de tâche

Cette option détermine le comportement du programme lorsqu'un plan de protection programmé échoue ou que votre ordinateur redémarre pendant l'exécution d'une sauvegarde. Cette option ne fonctionne pas lorsqu'un plan de protection est démarré manuellement.

© Acronis International GmbH, 2003-2026

Si cette option est activée, le programme essaiera de nouveau d'exécuter le plan de protection. Vous pouvez spécifier le nombre de tentatives et l'intervalle de temps entre ces tentatives. Le programme s'arrête dès qu'une tentative aboutit ou que le nombre spécifié de tentatives est atteint, selon le cas de figure qui se produit en premier.

Si cette option est activée et que votre ordinateur redémarre pendant l'exécution d'une sauvegarde, l'opération de sauvegarde n'échoue pas. Quelques minutes après le redémarrage, l'opération de sauvegarde se poursuit automatiquement et crée le fichier de sauvegarde avec les données manquantes. Dans ce cas d'utilisation, l'option **Intervalle entre les tentatives** n'est pas pertinente.

Le préréglage est le suivant : **Activé**.

Remarque
Cette option n'est pas effective pour les sauvegardes de données d'investigation.

Conditions de démarrage de tâche

Cette option est effective à la fois dans les systèmes d'exploitation Windows et Linux.

Cette option détermine le comportement du programme lorsqu' une tâche est sur le point de démarrer (l'heure planifiée arrive ou l'événement spécifié dans la planification se produit), mais la condition (ou l'une des nombreuses conditions) n'est pas remplie. Pour plus d'informations sur les conditions, consultez la section "Conditions de démarrage" (p. 580).

Le préréglage est le suivant : **Attendre que les conditions de la planification soient remplies.**

Attendre que les conditions de la planification soient remplies

Avec ce paramètre, le planificateur commence à surveiller les conditions et lance la tâche dès que les conditions sont remplies. Si les conditions ne sont jamais remplies, la tâche ne démarrera jamais.

Pour gérer la situation lorsque les conditions ne sont pas remplies pendant trop longtemps et qu'il devient trop risqué de retarder la tâche, vous pouvez définir l'intervalle de temps à l'issue duquel la tâche sera exécutée, quelle que soit la condition. Cochez la case **Exécuter la tâche de toutes façons après**, puis spécifiez l'intervalle de temps. La tâche démarrera dès que les conditions seront remplies OU que le délai maximum sera écoulé, en fonction du cas de figure qui se produira en premier.

Sauter l'exécution de la tâche

Il peut être impossible de retarder une tâche, par exemple, lorsque vous devez impérativement exécuter une tâche au moment spécifié. Il est alors pertinent de passer outre la tâche plutôt que d'attendre que les conditions soient remplies, particulièrement si les tâches sont effectuées relativement fréquemment.

© Acronis International GmbH, 2003-2026

Service de cliché instantané des volumes

Cette option ne s'applique qu'aux systèmes d'exploitation Windows.

Elle définit si une sauvegarde peut réussir si un ou plusieurs enregistreurs VSS (service de cliché instantané des volumes) échouent, et indique également si le fournisseur doit informer les applications compatibles VSS que la sauvegarde va démarrer.

L'utilisation du service VSS (service de cliché instantané des volumes) garantit la cohérence de toutes les données utilisées par les applications, en particulier, l'achèvement de toutes les transactions de la base de données au moment de la prise de l'instantané des données par le logiciel de sauvegarde. La cohérence des données garantit, quant à elle, que l'application sera restaurée dans l'état approprié et deviendra opérationnelle immédiatement après la restauration.

L'instantané est utilisé uniquement pendant l'opération de sauvegarde et il est supprimé automatiquement lorsque cette opération est terminée. Aucun fichier temporaire n'est conservé.

Vous pouvez également utiliser les commandes avant et après la capture de données afin de vous assurer que les données sont sauvegardées de façon cohérente. Par exemple, spécifiez des commandes avant la capture de données, qui suspendront la base de données et videront tous les caches pour garantir que toutes les transactions sont terminées, et des commandes après la capture de-données, qui remettront la base de données en service une fois l'instantané pris.

Remarque
Les fichiers et les dossiers qui sont indiqués dans la clé de la base de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** ne sont pas sauvegardés. En particulier, les fichiers de données Outlook hors connexion (.ost) ne sont pas sauvegardés, car ils sont indiqués dans la valeur **OutlookOST** de cette clé.

Ignorer les enregistreurs VSS échoués

Vous pouvez sélectionner l'une des options suivantes :

- **Ignorer les enregistreurs VSS échoués**
  Grâce à cette option, les sauvegardes sont réussies, même en cas d'échec d'un ou de plusieurs enregistreurs VSS.

  Important
  Les sauvegardes reconnaissant les applications échouent toujours si l'enregistreur propre à l'application échoue. Par exemple, si vous effectuez la sauvegarde reconnaissant les applications de données SQL Server et que l'enregistreur **SqlServerWriter** échoue, l'opération de sauvegarde échoue également.

  Lorsque cette option est activée, trois tentatives consécutives de création d'instantané VSS sont réalisées.

© Acronis International GmbH, 2003-2026

Pour la première tentative, tous les enregistreurs VSS sont nécessaires. En cas d'échec, cette tentative est relancée. Si la deuxième tentative échoue également, les enregistreurs VSS qui ont échoué sont exclus de l'opération de sauvegarde et une troisième tentative est lancée. Si cette troisième tentative réussit, la sauvegarde s'effectue, avec un avertissement concernant les enregistreurs VSS qui ont échoué. En cas d'échec de la troisième tentative, la sauvegarde échoue.

- **Exiger la réussite du traitement de tous les enregistreurs VSS**
  En cas d'échec de l'un des enregistreurs VSS, l'opération de sauvegarde échoue également.

Sélectionner le fournisseur d'instantanés

Vous pouvez sélectionner l'une des options suivantes :

- **Sélection automatique du fournisseur d'instantanés**
  Sélection automatique du fournisseur d'instantanés matériels ou logiciels, ou de Microsoft Software Shadow Copy.

  Remarque
  Nous vous recommandons d'utiliser la sélection automatique d'un fournisseur d'instantanés dès que possible.

- **Utilisation du fournisseur de cliché instantané des logiciels Microsoft**
  Nous vous recommandons de forcer l'utilisation du fournisseur Microsoft Software Shadow Copy si vous avez d'autres fournisseurs VSS tiers que vous ne souhaitez pas utiliser, et lorsque la ressource protégée ne contient pas de volumes partagés de cluster.

  Avertissement !
  Forcez l'utilisation du fournisseur Microsoft Software Shadow Copy uniquement si vous avez besoin de vous en servir. En effet, l'utilisation de ce fournisseur peut provoquer l'échec des sauvegardes dans les environnements comportant des volumes de cluster partagés et d'autres volumes que ce fournisseur ne prend pas en charge.

Activer la sauvegarde complète VSS

Si cette option est activée, les journaux de Microsoft Exchange Server et des autres applications compatibles VSS (sauf Microsoft SQL Server) seront tronqués après chaque sauvegarde de disque complète, incrémentielle ou différentielle réussie.

Le préréglage est le suivant : **Désactivé**.

Laissez cette option désactivée dans les cas suivants :

- Si vous utilisez l'agent pour Exchange ou un logiciel tiers pour sauvegarder les données Exchange Server. La raison est que la troncature du journal interférera avec les sauvegardes des journaux des transactions consécutives.
- Si vous utilisez un logiciel tiers pour sauvegarder les données SQL Server. La raison pour cela est que le logiciel tiers prendra la sauvegarde de niveau disque résultante comme sa « propre »

© Acronis International GmbH, 2003-2026

sauvegarde complète. En conséquence, la sauvegarde différentielle suivante des données SQL Server échouera. Les sauvegardes continueront à échouer jusqu'à ce que le logiciel tiers crée sa prochaine « propre » sauvegarde complète.

- Si d'autres applications compatibles VSS sont en cours d'exécution sur la machine et que vous devez conserver leurs journaux pour une raison quelconque.

Important
L'activation de cette option n'entraîne pas la troncature des journaux Microsoft SQL Server. Pour tronquer le journal SQL Server après une sauvegarde, activez l'option de sauvegarde Troncation de journal.

Service de cliché instantané des volumes (VSS) pour les machines virtuelles

Cette option contrôle la création d'instantanés suspendus pour les machines virtuelles protégées.

Le préréglage est le suivant : **Activé**.

Lorsque cette option est activée, les transactions de toutes les applications compatibles VSS en cours d'exécution sur la machine virtuelle sont terminées avant la prise d'un instantané suspendu.

Si un instantané suspendu ne peut pas être pris pour une raison quelconque, le résultat de l'opération de sauvegarde dépend des paramètres de l'application de sauvegarde comme suit.

- Si la sauvegarde de l'application est définie sur **Activé** et qu'un instantané suspendu ne peut pas être pris après le nombre de nouvelles tentatives spécifié dans l'option Gestion des erreurs, la sauvegarde échoue.
- Si la sauvegarde de l'application est définie sur **Désactivé** et qu'un instantané suspendu ne peut pas être pris après le nombre de tentatives spécifiées dans l'option Gestion des erreurs, une sauvegarde cohérente en cas de plantage est créée.

  Pour faire échouer la sauvegarde au lieu de créer une sauvegarde cohérente après plantage, sélectionnez la case à cocher **Échec de la sauvegarde si la prise d'un instantané suspendu n'est pas possible**.

Lorsque cette option est désactivée, un cliché instantané non suspendu est pris. La machine virtuelle sera sauvegardée dans un état cohérent en cas de panne.

Le tableau suivant résume les paramètres disponibles et leurs résultats.

Paramètres	L'instantané suspendu a été pris avec succès		L'instantané suspendu n'a pas été pris	
	Sauvegarde de l'application activée	Sauvegarde de l'application désactivée	Sauvegarde de l'application activée	Sauvegarde de l'application désactivée
Activation du	L'instantané	L'instantané	La sauvegarde échoue.	Un instantané non

© Acronis International GmbH, 2003-2026

Paramètres	L'instantané suspendu a été pris avec succès		L'instantané suspendu n'a pas été pris	
	Sauvegarde de l'application activée	**Sauvegarde de l'application désactivée**	**Sauvegarde de l'application activée**	**Sauvegarde de l'application désactivée**
service de cliché instantané des volumes (VSS) pour les machines virtuelles **Échec de la sauvegarde si la prise d'un instantané suspendu n'est pas possible** non sélectionné	suspendu est pris. La sauvegarde cohérente de l'application est créée.	suspendu est pris. La sauvegarde cohérente de l'application est créée.		suspendu est pris. Une sauvegarde cohérente de plantage est créée.
Activation du **service de cliché instantané des volumes (VSS) pour les machines virtuelles** **Échec de la sauvegarde si la prise d'un instantané suspendu n'est pas possible** sélectionné	L'instantané suspendu est pris. La sauvegarde cohérente de l'application est créée.	L'instantané suspendu est pris. La sauvegarde cohérente de l'application est créée.	La sauvegarde échoue.	La sauvegarde échoue.
Service de cliché instantané des volumes (VSS) désactivé **pour les machines virtuelles**	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.	Un instantané non suspendu est pris. Une sauvegarde cohérente de plantage est créée.

L'activation du **Service VSS pour machines virtuelles** déclenche également les scripts de pré-gel et de post-dégel éventuellement présents sur la machine virtuelle sauvegardée. Pour plus d'informations sur ces scripts, voir "Exécution automatique de scripts pre-freeze et post-thaw" (p. 974).

© Acronis International GmbH, 2003-2026

Pour prendre un instantané en suspend, le logiciel de sauvegarde exécute un VSS sur une machine virtuelle en utilisant VMware Tools, Hyper-V Integration Services, Virtuozzo Guest Tools, Red Hat Virtualization Guest Tools ou QEMU Guest Tools, respectivement.

Remarque
Pour les machines virtuelles Red Hat Virtualization (oVirt), nous vous recommandons d'installer QEMU Guest Tools plutôt que Red Hat Virtualization Guest Tools. Certaines versions de Red Hat Virtualization Guest Tools ne prennent pas en charge les instantanés cohérents avec les applications.

Cette option n'affecte pas les machines virtuelles Scale Computing HC3. Pour celles-ci, la suspension dépend de l'installation ou non des outils Scale sur la machine virtuelle.

Sauvegarde hebdomadaire

Cette option détermine quelles sauvegardes sont considérées comme « hebdomadaires » dans les règles de rétention et les plans de sauvegarde. Une sauvegarde « hebdomadaire » correspond à la première sauvegarde créée dès qu'une semaine commence.

Le préréglage est le suivant : **Lundi**.

Journal des événements Windows

Cette option est effective uniquement dans les systèmes d'exploitation Windows.

Cette option définit si les agents doivent consigner des événements des opérations de sauvegarde dans journal des événements d'applications Windows (pour voir ce journal, exécutez eventvwr.exe ou sélectionnez **Panneau de configuration** > **Outils administratifs** > **Affichage des événements**). Vous pouvez filtrer les événements à consigner.

Le préréglage est le suivant : **Désactivé**.

Restauration

Restauration de l'aide-mémoire

Le tableau suivant résume les méthodes de restauration disponibles. Utilisez le tableau afin de choisir la méthode de restauration qui correspond le mieux à vos besoins.

Remarque
Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes dans des tenants en mode de conformité. Voir "Restauration de sauvegardes dans les tenants en mode de conformité" (p. 1617).

Quoi restaurer	Méthode de restauration

© Acronis International GmbH, 2003-2026

Machine physique (Windows ou Linux)	Utilisation de la console Cyber Protect Utilisation d'un support de démarrage
Machine physique (Mac)	Utilisation d'un support de démarrage
Machine virtuelle (telle que VMware, Hyper-V, Red Hat Virtualization (oVirt), Scale Computing HC3, Proxmox)	Utilisation de la console Cyber Protect Utilisation d'un support de démarrage
Machine virtuelle (Virtuozzo Hybrid Server, Virtuozzo Hybrid Infrastructure)	Utilisation de la console Cyber Protect
Conteneur (Virtuozzo Hybrid Server, Proxmox)	Utilisation de la console Cyber Protect
Configuration ESXi	Utilisation d'un support de démarrage
Fichiers/Dossiers	Utilisation de la console Cyber Protect Téléchargement de fichiers depuis le Cloud Utilisation d'un support de démarrage Extraction de fichiers à partir de sauvegardes locales
Etat du système	Utilisation de la console Cyber Protect
Bases de données SQL	Utilisation de la console Cyber Protect
Bases de données Exchange	Utilisation de la console Cyber Protect
Boîtes aux lettres Exchange	Utilisation de la console Cyber Protect
Microsoft 365	
Boîtes aux lettres (agent local pour Microsoft 365)	Utilisation de la console Cyber Protect
Boîtes aux lettres (agent Cloud pour Microsoft 365)	Utilisation de la console Cyber Protect
Dossiers publics	Utilisation de la console Cyber Protect
Fichiers OneDrive	Utilisation de la console Cyber Protect

© Acronis International GmbH, 2003-2026

Données SharePoint Online	Utilisation de la console Cyber Protect
Google Workspace	
Boîtes aux lettres	Utilisation de la console Cyber Protect
Fichiers Google Drive	Utilisation de la console Cyber Protect
Fichiers de Drive partagés	Utilisation de la console Cyber Protect

Restauration interplate-forme

La restauration interplate-forme est disponible pour les sauvegardes d'ordinateurs complets et de disques contenant un système d'exploitation.

Une restauration interplate-forme s'effectue dans les cas suivants :

- Une sauvegarde est créée par un type d'agent, mais elle est restaurée par un type d'agent différent.
- Une sauvegarde avec agent est restaurée au niveau de l'hyperviseur (restauration sans agent), ou une sauvegarde sans agent est restaurée par un agent (restauration avec agent).
- Une sauvegarde est restaurée sur un matériel différent (y compris les appliances virtuelles).

Remarque
Certains périphériques tels que les imprimantes risquent de ne pas être restaurés correctement lorsque vous effectuez une restauration interplate-forme.

Pour plus d'informations sur les combinaisons possibles pour la restauration interplate-forme, voir "Restauration interplate-forme" (p. 667).

Remarque pour les utilisateurs Mac

- Depuis la version 10.11 du système d'exploitation El Capitan, certains fichiers système, dossiers et processus sont marqués comme protégés avec l'ajout de l'attribut de fichier com.apple.rootless. Cette fonctionnalité est appelée Protection de l'intégrité du système (System Integrity Protection, SIP). Les fichiers protégés comprennent les applications préinstallées, ainsi que la plupart des dossiers des répertoires /system, /bin, /sbin et /usr.

  Les fichiers et dossiers protégés ne peuvent pas être écrasés lors de la restauration du système d'exploitation. Si vous souhaitez écraser les fichiers protégés, effectuez une restauration à partir d'un support de démarrage.
- Désormais, dans macOS Sierra 10.12, les fichiers rarement utilisés peuvent être déplacés vers iCloud au moyen de la fonctionnalité de stockage dans le Cloud. De petites empreintes de ces fichiers sont conservées sur le système de fichiers. Ces empreintes sont sauvegardées à la place des fichiers d'origine.

  Lorsque vous restaurez une empreinte à l'emplacement d'origine, elle est synchronisée avec iCloud, et le fichier d'origine redevient disponible. Si vous restaurez une empreinte à un

© Acronis International GmbH, 2003-2026

emplacement différent, celle-ci n'est pas synchronisée avec iCloud et le fichier d'origine est indisponible.

Restauration interplate-forme

Vous pouvez restaurer une sauvegarde de niveau disque sur une machine physique ou sur une machine virtuelle. Par exemple, une sauvegarde de niveau disque est une sauvegarde **Machine complète** ou une sauvegarde **Disque/volumes** qui contient le disque système et le disque de démarrage.

Une restauration multiplate-forme (migration d'ordinateur) s'effectue dans les cas suivants :

- Lorsque vous restaurer la sauvegarde d'une machine physique sur une machine virtuelle.
- Lorsque vous restaurez la sauvegarde d'une machine virtuelle sur une machine physique.
- Lorsque vous restaurez la sauvegarde d'une machine virtuelle sur une machine virtuelle sur un autre type d'hyperviseur.

Remarque
Si une machine virtuelle est sauvegardée par un agent de protection installé dans le système d'exploitation invité, la sauvegarde est considérée comme une sauvegarde de machine physique.

Les tableaux suivants résument les options disponibles pour la restauration multiplate-forme selon la ressource sauvegardée.

Machine physique

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

© Acronis International GmbH, 2003-2026

Machine virtuelle Broadcom VMware ESXi

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

Machine virtuelle Microsoft Azure

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

© Acronis International GmbH, 2003-2026

Machine virtuelle Microsoft Hyper-V

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

Machine virtuelle Virtuozzo Hybrid Server

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

© Acronis International GmbH, 2003-2026

Conteneur Virtuozzo Hybrid Server

Ressource cible	Pris en charge
Machine physique	Non
Machine virtuelle Broadcom VMware ESXi	Non
Machine virtuelle Microsoft Azure	Non
Machine virtuelle Microsoft Hyper-V	Non
Machine virtuelle Virtuozzo Hybrid Server	Non
Conteneur Virtuozzo Hybrid Server	Oui
Machine virtuelle Virtuozzo Hybrid Infrastructure	Non
Machine virtuelle Scale Computing HyperCore	Non
Machine virtuelle RHV/oVirt	Non
Machine virtuelle Nutanix	Non
Machine virtuelle Proxmox	Non
Conteneur Proxmox	Non

Machine virtuelle Virtuozzo Hybrid Infrastructure

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

© Acronis International GmbH, 2003-2026

Machine virtuelle Scale Computing HyperCore

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

Machine virtuelle Red Hat Virtualization/oVirt

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

© Acronis International GmbH, 2003-2026

Machine virtuelle Nutanix

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

Machine virtuelle Proxmox

Ressource cible	Pris en charge
Machine physique	Oui
Machine virtuelle Broadcom VMware ESXi	Oui
Machine virtuelle Microsoft Azure	Oui
Machine virtuelle Microsoft Hyper-V	Oui*
Machine virtuelle Virtuozzo Hybrid Server	Oui
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Oui
Machine virtuelle Scale Computing HyperCore	Oui
Machine virtuelle RHV/oVirt	Oui
Machine virtuelle Nutanix	Oui
Machine virtuelle Proxmox	Oui
Conteneur Proxmox	Non

© Acronis International GmbH, 2003-2026

Conteneur Proxmox

Ressource cible	Pris en charge
Machine physique	Non
Machine virtuelle Broadcom VMware ESXi	Non
Machine virtuelle Microsoft Azure	Non
Machine virtuelle Microsoft Hyper-V	Non
Machine virtuelle Virtuozzo Hybrid Server	Non
Conteneur Virtuozzo Hybrid Server	Non
Machine virtuelle Virtuozzo Hybrid Infrastructure	Non
Machine virtuelle Scale Computing HyperCore	Non
Machine virtuelle RHV/oVirt	Non
Machine virtuelle Nutanix	Non
Machine virtuelle Proxmox	Non
Conteneur Proxmox	Oui

Remarque
Le paramètre Démarrage sécurisé n'est pas sauvegardé. Si le démarrage sécurisé est activé sur l'ordinateur d'origine, la machine virtuelle restaurée en tant que nouvelle machine ne démarrera pas. Pour démarrer la machine restaurée, désactivez le démarrage sécurisé dans la console de la MV après la restauration.

Remarque

- * Les ordinateurs EFI sont restaurés en tant que machines virtuelles de génération 2.
- * Vous ne pouvez pas restaurer des machines virtuelles macOS sur des hôtes Hyper-V, car Hyper-V ne prend pas en charge le système macOS. Vous pouvez restaurer des machines virtuelles macOS sur des hôtes VMware installés sur un matériel Mac.

Restauration interplate-forme via un support de démarrage

Vous pouvez effectuer une restauration interplate-forme en utilisant un support de démarrage.

Nous vous recommandons d'utiliser un support de démarrage au lieu de la console Cyber Protect dans les cas suivants :

- Exécution d'une migration non prise en charge de manière native.

© Acronis International GmbH, 2003-2026

Par exemple, utilisez un support de démarrage pour restaurer une machine physique ou une machine virtuelle non Virtuozzo Hybrid Server en tant que machine virtuelle Virtuozzo Hybrid Server sur un hôte Virtuozzo.

- Exécution de la migration d'une machine Linux contenant des volumes logiques.
  Utilisez l'agent pour Linux ou un support de démarrage pour créer la sauvegarde, puis employez un support de démarrage pour restaurer la sauvegarde.
- Fourniture de pilotes pour du matériel spécifique, essentiel pour la capacité de démarrage du système.
  Concevez un support de démarrage pouvant utiliser les pilotes requis. Pour plus d'informations, voir "Bootable Media Builder" (p. 992).

Restauration de machines physiques

Vous pouvez restaurer la sauvegarde de niveau disque d'une machine physique sur une autre machine physique ou sur une machine virtuelle. Par exemple, une sauvegarde de niveau disque est une sauvegarde **Machine complète** ou une sauvegarde **Disque/volumes** qui contient le disque système et le disque de démarrage.

Limites

- Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes de machines enregistrées dans des tenants clients en mode de conformité. Voir "Restauration de sauvegardes dans les tenants en mode de conformité" (p. 1617).
- Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes de machines physiques macOS sur une autre machine physique.
- Vous ne pouvez pas restaurer des sauvegardes de machines physiques macOS sur une machine virtuelle.
- Lors d'une restauration sur une machine virtuelle, Cyber Protect arrête la machine virtuelle cible sans afficher d'invite. Après la restauration, vous devez redémarrer cette machine manuellement. Vous pouvez modifier le comportement par défaut dans **Options de restauration** > **Gestion de l'alimentation des MV**.

Si vous souhaitez restaurer l'un des éléments suivants, utilisez un support de démarrage à la place de la console Cyber Protect :

- Machine physique fonctionnant sous macOS.

  Remarque
  Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.

- Ordinateur dans un tenant client en mode de conformité.
- Tout système d'exploitation sur un ordinateur hors ligne ou sur système nu.

© Acronis International GmbH, 2003-2026

- Structure de volumes logiques, par exemple, volumes créés par Logical Volume Manager dans Linux. Avec le support de démarrage, vous pouvez recréer la structure de volumes logiques automatiquement.

Pour plus d'informations sur la restauration d'ordinateurs à l'aide d'un support de démarrage, voir "Restauration de disques via un support de démarrage" (p. 704).

Restauration d'une machine physique en tant que machine physique

Vous pouvez restaurer la sauvegarde de disque d'un ordinateur physique sur l'ordinateur d'origine ou sur un nouvel ordinateur.

Cette procédure décrit la restauration à partir de la console Cyber Protect. Vous pouvez également utiliser un support de démarrage pour restaurer une sauvegarde (y compris une sauvegarde d'un ordinateur hors ligne) sur une machine physique. Pour plus d'informations, voir la documentation correspondante. Pour plus d'informations, voir "Restauration de disques via un support de démarrage" (p. 704).

Pour restaurer une machine physique en tant que machine physique

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
     - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
     - Sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   Une machine cible est automatiquement sélectionnée.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. Sélectionnez un ordinateur en ligne, puis cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] Configurez le mappage de disques entre l'ordinateur sauvegardé et la machine cible.
   a. [Pour configurer le mappage au niveau du disque]
      i. Cliquez sur **Mappage de disques**.
      ii. Configurez le mappage de disques entre l'ordinateur sauvegardé et la machine cible.
      iii. Cliquez sur **Terminé**.
   b. [Pour configurer le mappage au niveau du volume]
      i. Cliquez sur **Mappage de disques**, puis, dans l'angle supérieur droit, sur **Passer au mappage de volume**.
      ii. Configurez le mappage de volumes entre l'ordinateur sauvegardé et la machine cible.
      iii. Cliquez sur **Terminé**.
7. [Facultatif] [Disponible uniquement pour les ordinateurs Windows] Pour garantir que les données restaurées sont exemptes de malware, activez le bouton **Restauration sécurisée**. Pour plus d'informations, voir "Restauration sûre" (p. 730).
8. Cliquez sur **Démarrer la restauration**.
9. [Facultatif] Si vous préférez redémarrer l'ordinateur manuellement après la restauration, désélectionnez la case **Redémarrer automatiquement l'ordinateur, si nécessaire**. Pour plus d'informations, voir "Restauration avec redémarrage" (p. 716).
10. Pour confirmer que vous souhaitez écraser les disques de la machine cible, cliquez sur **Démarrer la restauration**.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Restauration d'une machine physique en tant que machine virtuelle

Vous pouvez restaurer la sauvegarde de disque d'une machine physique sur une machine virtuelle. Cette opération est appelée restauration interplate-forme (migration d'ordinateur). Pour plus d'informations, voir "Restauration interplate-forme" (p. 667).

Prérequis

- Un agent pour l'hyperviseur pertinent est installé dans votre environnement. Par exemple, la restauration vers une machine virtuelle VMware ESXi nécessite l'installation et l'enregistrement de l'agent pour VMware dans le programme d'installation de la console Cyber Protect.

Restauration d'une machine physique en tant que machine virtuelle

Les procédures sont répertoriées en fonction du type de la machine virtuelle cible.

VMware ESXi

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
     - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
     - Sélectionnez un point de restauration.

     Remarque
     Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Broadcom (VMware) ESXi**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Magasin de données**, puis sélectionnez un magasin de données.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Azure

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
     - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
     - Sélectionnez un point de restauration.

     Remarque
     Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

© Acronis International GmbH, 2003-2026

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Microsoft Azure**.
      a. [Pour effectuer la restauration sur un nouvel ordinateur]
         i. Sélectionnez **Nouvel ordinateur**.
         ii. Sélectionnez un abonnement Azure, une région et un groupe de ressources.
         iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
         iv. Cliquez sur **OK**.
      b. [Pour effectuer la restauration sur l'ordinateur d'origine]
         i. Sélectionnez **Ordinateur d'origine**.
         ii. Cliquez sur **OK**.
6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le type de stockage de chaque disque cible, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Sélectionnez le type de stockage.
      Le stockage redondant au niveau local (LRS) et le stockage redondant par zone (ZRS) sont disponibles.
      iv. Cliquez sur **Terminé**.
   b. Pour modifier le type et la zone de disponibilité, la taille de la mémoire et les connexions réseau (y compris les sous-réseaux et les groupes de sécurité) de la machine virtuelle, cliquez sur **Paramètres de MV**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur l'ordinateur d'origine] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Hyper-V

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
     - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
     - Sélectionnez un point de restauration.

     Remarque
     Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Microsoft Hyper-V**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Chemin**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier le stockage, l'interface ou le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Configurez les paramètres.
      iv. Cliquez sur **Terminé**.
   d. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Virtuozzo Hybrid Infrastructure

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.

© Acronis International GmbH, 2003-2026

- Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
- Sélectionnez un point de restauration.

Remarque
Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Virtuozzo Hybrid Infrastructure**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options supplémentaires.
   a. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   b. Pour modifier la stratégie de stockage du disque cible, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Sélectionnez la stratégie de stockage du disque.
      iv. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

c. Pour modifier les cartes réseau, cliquez sur **Paramètres de MV**.
   i. Configurez les paramètres.
   ii. Cliquez sur **OK**.

8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Scale Computing HC3

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
     - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
     - Sélectionnez un point de restauration.

     Remarque
     Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Scale Computing HC3**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]

© Acronis International GmbH, 2003-2026

i. Sélectionnez **Nouvel ordinateur**.

ii. Sélectionner un hôte.

iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.

iv. Cliquez sur **OK**.

d. [Pour effectuer la restauration sur un ordinateur existant]

i. Sélectionnez **Ordinateur existant**.

ii. Sélectionnez la machine cible.

iii. Cliquez sur **OK**.

6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options supplémentaires.
   a. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   b. Pour changer le conteneur de stockage, l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Configurez les paramètres.
      iv. Cliquez sur **Terminé**.
8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

oVirt

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).

© Acronis International GmbH, 2003-2026

- [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
  - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
  - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
  - Sélectionnez un point de restauration.

Remarque
Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **oVirt**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Domaine de stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Nutanix

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
   - [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
     - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
     - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
     - Sélectionnez un point de restauration.

     Remarque
     Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Nutanix**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

d. [Pour effectuer la restauration sur un ordinateur existant]
   i. Sélectionnez **Ordinateur existant**.
   ii. Sélectionnez la machine cible.
   iii. Cliquez sur **OK**.

6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options supplémentaires.
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Conteneur de stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier le conteneur de stockage ou l'interface, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Configurez les paramètres.
      iv. Cliquez sur **Terminé**.
   d. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Proxmox

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - [Pour les ordinateurs en ligne] Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

     Remarque
     Les points de restauration sont filtrés en fonction du stockage de la sauvegarde.

   - [Pour les ordinateurs en ligne et hors ligne] Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).

© Acronis International GmbH, 2003-2026

- [Pour les ordinateurs hors ligne] [Si l'emplacement de sauvegarde est le stockage dans le cloud ou un stockage partagé et accessible par d'autres agents]
  - Dans l'onglet **Terminaux**, sélectionnez un ordinateur sauvegardé, puis cliquez sur **Restauration**.
  - Cliquez sur **Sélectionner l'ordinateur**, sélectionnez une machine cible en ligne, puis cliquez sur **OK**.
  - Sélectionnez un point de restauration.

Remarque
Vous pouvez également restaurer un ordinateur hors ligne en utilisant un support de démarrage. Voir "Restauration de disques via un support de démarrage" (p. 704).

2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
5. Sélectionnez une machine cible.
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Proxmox**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques, le type de contrôleur de disque, le mode de provisionnement des disques, ou exclure certains disques sauvegardés de la restauration, cliquez sur **Mappage de disque**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Remarque

- Pour restaurer un disque en tant que disque de type VirtIO, dans les options de restauration, sélectionnez NVME.
- Lors d'une restauration sur un nouvelle machine, les disques VMDK sont restaurés en tant que disques QCOW2 ou disques RAW (si vous changez le type de provisionnement en statique).

c. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
   i. Configurez les paramètres.
   ii. Cliquez sur **OK**.

8. Cliquez sur **Démarrer la restauration**
9. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Restauration de machines virtuelles

Vous pouvez restaurer la sauvegarde de niveau disque d'une machine virtuelle sur une machine physique ou une autre machine virtuelle. Par exemple, une sauvegarde de niveau disque est une sauvegarde **Machine complète** ou une sauvegarde **Disque/volumes** qui contient le disque système et le disque de démarrage.

Limites

- Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes de machines enregistrées dans des tenants clients en mode de conformité. Voir "Restauration de sauvegardes dans les tenants en mode de conformité" (p. 1617).
- Lors d'une restauration sur une machine virtuelle, Cyber Protect arrête la machine virtuelle cible sans afficher d'invite. Après la restauration, vous devez redémarrer cette machine manuellement. Vous pouvez modifier le comportement par défaut dans **Options de restauration** > **Gestion de l'alimentation des MV**.
- Vous pouvez restaurer une sauvegarde d'une machine virtuelle sur une machine physique si la configuration des disques de la machine cible correspond exactement à celle de la sauvegarde. Sinon, vous pouvez effectuer une migration virtuelle vers physique à l'aide d'un support de démarrage. Consultez "Restauration de disques via un support de démarrage" (p. 704).
- Vous ne pouvez pas restaurer des machines virtuelles macOS sur des hôtes Hyper-V, car Hyper-V ne prend pas en charge macOS. Vous pouvez restaurer des machines virtuelles macOS sur un hôte VMware installé sur un matériel Mac.

© Acronis International GmbH, 2003-2026

Restauration d'une machine virtuelle en tant que machine physique

Vous pouvez restaurer la sauvegarde de disque d'une machine virtuelle sur une machine physique. Cette opération est appelée restauration interplate-forme (migration d'ordinateur). Pour plus d'informations, voir "Restauration interplate-forme" (p. 667).

La procédure suivante décrit la restauration à partir de la console Cyber Protect. Vous pouvez également utiliser un support de démarrage pour restaurer une sauvegarde d'une machine virtuelle sur une machine physique. Pour plus d'informations, voir "Restauration de disques via un support de démarrage" (p. 704).

Pour restaurer une machine virtuelle en tant que machine physique

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. Dans **Restaurer vers**, sélectionnez **Machine physique**.
   Une machine cible est automatiquement sélectionnée.
5. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. Sélectionnez un ordinateur en ligne, puis cliquez sur **OK**.
6. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
7. [Facultatif] Configurez le mappage de disques entre l'ordinateur sauvegardé et la machine cible.
   a. [Pour configurer le mappage au niveau du disque]
      i. Cliquez sur **Mappage de disques**.
      ii. Configurez le mappage de disques entre l'ordinateur sauvegardé et la machine cible.
      iii. Cliquez sur **Terminé**.
   b. [Pour configurer le mappage au niveau du volume]
      i. Cliquez sur **Mappage de disques**, puis, dans l'angle supérieur droit, sur **Passer au mappage de volume**.
      ii. Configurez le mappage de volumes entre l'ordinateur sauvegardé et la machine cible.
      iii. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Remarque
Vous pouvez sélectionner des disques ou des volumes pour la restauration. Assurez-vous que la configuration des disques ou des volumes de l'ordinateur sauvegardé correspond exactement à celle de la machine cible.

8. [Facultatif] [Disponible uniquement pour les ordinateurs Windows] Pour garantir que les données restaurées sont exemptes de malware, activez le bouton **Restauration sécurisée**. Pour plus d'informations, voir "Restauration sûre" (p. 730).
9. Cliquez sur **Démarrer la restauration**
10. [Facultatif] Si vous préférez redémarrer l'ordinateur manuellement après la restauration, désélectionnez la case **Redémarrer automatiquement l'ordinateur, si nécessaire**. Pour plus d'informations, voir "Restauration avec redémarrage" (p. 716).
11. Pour confirmer que vous souhaitez écraser les disques de la machine cible, cliquez sur **Démarrer la restauration**.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Restauration d'une machine virtuelle en tant que machine virtuelle

Vous pouvez restaurer la sauvegarde d'une machine virtuelle sur l'hyperviseur d'origine ou sur un autre type d'hyperviseur. La restauration sur un autre type d'hyperviseur est appelée restauration interplate-forme (migration d'ordinateur). Pour plus d'informations, voir "Restauration interplate-forme" (p. 667).

La restauration sur une machine virtuelle sur laquelle aucun agent de protection n'est installé est effectuée au niveau de l'hyperviseur. Il s'agit d'une restauration sans agent.

La restauration vers une machine virtuelle sur laquelle un agent de protection est installé est une restauration avec agent. Ce type de restauration est identique à la restauration vers une machine physique.

Prérequis

- Un agent pour l'hyperviseur pertinent est installé dans votre environnement. Par exemple, la restauration vers une machine virtuelle VMware ESXi nécessite l'installation et l'enregistrement de l'agent pour VMware dans le programme d'installation de la console Cyber Protect.

Pour restaurer une machine virtuelle en tant que machine physique

Les procédures sont répertoriées en fonction du type de la machine virtuelle cible.

VMware ESXi

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).

© Acronis International GmbH, 2003-2026

- Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).

2. Cliquez sur **Restaurer** > **Toute la machine**.

   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **VMware ESXi**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Magasin de données**, puis sélectionnez un magasin de données.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Azure

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.

   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Microsoft Azure**.
      a. [Pour effectuer la restauration sur un nouvel ordinateur]
         i. Sélectionnez **Nouvel ordinateur**.
         ii. Sélectionnez un abonnement Azure, une région et un groupe de ressources.
         iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
         iv. Cliquez sur **OK**.
      b. [Pour effectuer la restauration sur l'ordinateur d'origine]
         i. Sélectionnez **Ordinateur d'origine**.
         ii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le type de stockage de chaque disque cible, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Sélectionnez le type de stockage.

      Le stockage redondant au niveau local (LRS) et le stockage redondant par zone (ZRS) sont disponibles.
      iv. Cliquez sur **Terminé**.
   b. Pour modifier le type et la zone de disponibilité, la taille de la mémoire et les connexions réseau (y compris les sous-réseaux et les groupes de sécurité) de la machine virtuelle, cliquez sur **Paramètres de MV**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
7. Cliquez sur **Démarrer la restauration**

© Acronis International GmbH, 2003-2026

8. [Lors de la restauration sur l'ordinateur d'origine] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Hyper-V

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Microsoft Hyper-V**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Chemin**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier le stockage, l'interface ou le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disques**.

© Acronis International GmbH, 2003-2026

i. Dans la section Disque cible, cliquez sur **Modifier**.

ii. Cliquez sur l'icône en forme d'engrenage.

iii. Configurez les paramètres.

iv. Cliquez sur **Terminé**.

d. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.

i. Configurez les paramètres.

ii. Cliquez sur **OK**.

7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Virtuozzo

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Virtuzzo**.

   Remarque
   Seule une machine virtuelle Virtuozzo peut être restaurée sur une machine virtuelle Virtuozzo.

   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.

© Acronis International GmbH, 2003-2026

   ii. Sélectionnez la machine cible.
   iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Chemin**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier le stockage, l'interface ou le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Configurez les paramètres.
      iv. Cliquez sur **Terminé**.
   d. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Virtuozzo Hybrid Infrastructure

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :

© Acronis International GmbH, 2003-2026

a. Cliquez sur **Machine cible**.

b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Virtuozzo Hybrid Infrastructure**.

c. [Pour effectuer la restauration sur un nouvel ordinateur]

i. Sélectionnez **Nouvel ordinateur**.

ii. Sélectionner un hôte.

iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.

iv. Cliquez sur **OK**.

d. [Pour effectuer la restauration sur un ordinateur existant]

i. Sélectionnez **Ordinateur existant**.

ii. Sélectionnez la machine cible.

iii. Cliquez sur **OK**.

5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options supplémentaires.

a. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.

i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.

ii. Cliquez sur **Terminé**.

b. Pour modifier la stratégie de stockage du disque cible, cliquez sur **Mappage de disques**.

i. Dans la section Disque cible, cliquez sur **Modifier**.

ii. Cliquez sur l'icône en forme d'engrenage.

iii. Sélectionnez la stratégie de stockage du disque.

iv. Cliquez sur **Terminé**.

c. Pour modifier les cartes réseau, cliquez sur **Paramètres de MV**.

i. Configurez les paramètres.

ii. Cliquez sur **OK**.

7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Scale Computing HC3

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).

© Acronis International GmbH, 2003-2026

2. Cliquez sur **Restaurer** > **Toute la machine**.
   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Scale Computing HC3**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options supplémentaires.
   a. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   b. Pour changer le conteneur de stockage, l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l'icône en forme d'engrenage.
      iii. Configurez les paramètres.
      iv. Cliquez sur **Terminé**.
7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

oVirt

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.

   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **oVirt**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Domaine de stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Nutanix

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.

   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Nutanix**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options supplémentaires.
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Conteneur de stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier le conteneur de stockage ou l'interface, cliquez sur **Mappage de disques**.
      i. Dans la section Disque cible, cliquez sur **Modifier**.
      ii. Cliquez sur l’icône en forme d’engrenage.
      iii. Configurez les paramètres.
      iv. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

d. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.
   i. Configurez les paramètres.
   ii. Cliquez sur **OK**.

7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Proxmox

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   La machine virtuelle d'origine est sélectionnée comme machine cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier la machine cible :
   a. Cliquez sur **Machine cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Proxmox**.
   c. [Pour effectuer la restauration sur un nouvel ordinateur]
      i. Sélectionnez **Nouvel ordinateur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom de l'ordinateur**, spécifiez un nom pour le nouvel ordinateur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un ordinateur existant]
      i. Sélectionnez **Ordinateur existant**.
      ii. Sélectionnez la machine cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez ces options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques, le type de contrôleur de disque, le mode de provisionnement des disques, ou exclure certains disques sauvegardés de la restauration,

© Acronis International GmbH, 2003-2026

cliquez sur **Mappage de disque**.

i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.

ii. Cliquez sur **Terminé**.

Remarque

- Pour restaurer un disque en tant que disque de type VirtIO, dans les options de restauration, sélectionnez NVME.
- Lors d'une restauration sur un nouvelle machine, les disques VMDK sont restaurés en tant que disques QCOW2 ou disques RAW (si vous changez le type de provisionnement en statique).

c. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres de la machine virtuelle**.

i. Configurez les paramètres.

ii. Cliquez sur **OK**.

7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un ordinateur existant] Pour confirmer que vous souhaitez écraser la machine cible, cliquez sur **Démarrer la restauration**.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Restauration de conteneurs

Vous pouvez restaurer un conteneur sauvegardé dans le conteneur d'origine ou dans un nouveau conteneur sur le même hyperviseur.

La restauration multiplate-forme n'est pas prise en charge pour les conteneurs.

Pour restaurer un conteneur

Conteneur Virtuozzo

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez un conteneur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   Le conteneur d'origine est sélectionné comme conteneur cible.
3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier le conteneur cible :

© Acronis International GmbH, 2003-2026

a. Cliquez sur **Conteneur cible**.

b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Virtuozzo**.

c. [Pour effectuer la restauration sur un nouveau conteneur]

   i. Sélectionnez **Nouveau conteneur**.

   ii. Sélectionner un hôte.

   iii. Dans **Nom du conteneur**, spécifiez un nom pour le nouveau conteneur.

   iv. Cliquez sur **OK**.

d. [Pour effectuer la restauration sur un conteneur existant]

   i. Sélectionnez **Conteneur existant**.

   ii. Sélectionnez le conteneur cible.

   iii. Cliquez sur **OK**.

5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouveau conteneur] Configurez les options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres du conteneur**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un conteneur existant] Pour confirmer que vous souhaitez écraser le conteneur cible, cliquez sur **Démarrer la restauration**.

Conteneur Proxmox

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Terminaux**, sélectionnez un conteneur sauvegardé, cliquez sur **Restauration**, puis sélectionnez une sauvegarde (point de restauration).
   - Dans l'onglet **Stockage de sauvegarde**, sélectionnez une archive de sauvegarde, puis sélectionnez une sauvegarde (point de restauration).
2. Cliquez sur **Restaurer** > **Toute la machine**.
   Le conteneur d'origine est sélectionné comme conteneur cible.

© Acronis International GmbH, 2003-2026

3. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
4. [Facultatif] Pour modifier le conteneur cible :
   a. Cliquez sur **Conteneur cible**.
   b. [Si plusieurs hyperviseurs sont disponibles] Sélectionnez **Proxmox**.
   c. [Pour effectuer la restauration sur un nouveau conteneur]
      i. Sélectionnez **Nouveau conteneur**.
      ii. Sélectionner un hôte.
      iii. Dans **Nom du conteneur**, spécifiez un nom pour le nouveau conteneur.
      iv. Cliquez sur **OK**.
   d. [Pour effectuer la restauration sur un conteneur existant]
      i. Sélectionnez **Conteneur existant**.
      ii. Sélectionnez le conteneur cible.
      iii. Cliquez sur **OK**.
5. [Si vous y êtes invité] Spécifiez les identifiants nécessaires pour accéder au stockage des sauvegardes, puis cliquez sur **OK**.
6. [Facultatif] [Lors de la restauration sur un nouveau conteneur] Configurez les options supplémentaires :
   a. Pour modifier le stockage de la machine virtuelle, cliquez sur **Stockage**, puis sélectionnez un stockage.
   b. Pour modifier le mappage des disques ou exclure certains des disques sauvegardés de la restauration, cliquez sur **Mappage de disques**.
      i. Configurez le mappage des disques ou sélectionnez les disques à restaurer.
      ii. Cliquez sur **Terminé**.
   c. Pour modifier la taille de la mémoire, le nombre de processeurs virtuels ou les connexions réseau de la machine cible, cliquez sur **Paramètres du conteneur**.
      i. Configurez les paramètres.
      ii. Cliquez sur **OK**.
7. Cliquez sur **Démarrer la restauration**
8. [Lors de la restauration sur un conteneur existant] Pour confirmer que vous souhaitez écraser le conteneur cible, cliquez sur **Démarrer la restauration**.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Restauration de disques via un support de démarrage

L’exécution du support de démarrage nécessite 1,5 Go de RAM.

© Acronis International GmbH, 2003-2026

Pour plus d'informations sur la création d'un support de démarrage, voir "Création d'un support de démarrage physique" (p. 991).

Remarque
Vous ne pouvez pas restaurer les sauvegarde de disque d'ordinateurs Mac Intel sur des Mac utilisant des puces silicone Apple, et inversement. Vous pouvez restaurer des fichiers et des dossiers.

Pour restaurer des disques via un support de démarrage

1. Démarrez la machine cible par le biais d'un support de démarrage.
2. [Uniquement lors de la restauration d'un Mac] Si vous restaurez des disques/volumes formatés APFS vers une machine non d'origine ou à froid, recréez la configuration du disque d'origine manuellement :
   a. Cliquez sur **Utilitaire de disque**.
   b. Effacer et formater le disque de destination dans APFS. Pour obtenir des instructions, consultez l'article https://support.apple.com/en-us/HT208496#erasedisk.
   c. Recréez la configuration du disque d'origine. Pour obtenir des instructions, consultez l'article https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.
   d. Cliquez sur **Utilitaire de disque** > **Quitter l'utilitaire de disque**.
3. Cliquez sur **Gérer cette machine localement** ou double-cliquez sur **Support de Secours Bootable**, en fonction du type de support que vous utilisez.
4. Si un serveur proxy est activé dans votre réseau, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez l'adresse IP/nom de l'hôte, le port et les informations d'identification du serveur proxy. Sinon, ignorez cette étape.
5. [Facultatif] Lors d'une restauration depuis Windows ou Linux, cliquez sur **Outils** > **Enregistrer le support au sein du service Cyber Protection**, puis spécifiez le jeton d'enregistrement que vous avez obtenu lorsque vous avez téléchargé le support. Si vous faites cela, vous n'aurez pas besoin de saisir d'informations d'identification ni de code d'inscription pour accéder au stockage Cloud, comme décrit à l'étape 8.
6. Sur l'écran d'accueil, cliquez sur **Restaurer**.
7. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
8. Indiquez l'emplacement de la sauvegarde :
   - Pour restaurer des informations depuis le Cloud, sélectionnez **Stockage dans le Cloud**. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.

     Lors d'une restauration Windows ou Linux, vous avez la possibilité de demander un code d'inscription et de l'utiliser à la place de vos informations d'identification. Cliquez sur **Utiliser le code d'inscription** > **Demander le code**. Le logiciel affiche le lien et le code d'inscription.

© Acronis International GmbH, 2003-2026

Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Le code d'enregistrement n'est valable qu'une heure.

- Pour effectuer une restauration depuis un dossier local ou réseau, rendez-vous dans **Dossiers locaux** ou **Dossiers réseau**.
- Pour restaurer à partir d'emplacements de sauvegarde sur un stockage cloud public tel que Microsoft Azure, Amazon S3 ou un stockage compatible S3, cliquez d'abord sur **Enregistrer le support dans le service Cyber Protection**, puis configurez la restauration à l'aide de l'interface Web. Pour plus d'informations sur la gestion des supports à distance via l'interface Web, consultez "Opérations à distance avec un support de démarrage" (p. 1009).

Cliquez sur **OK** pour confirmer votre sélection.

9. Sélectionnez la sauvegarde à partir de laquelle vous voulez restaurer les données. Si vous y êtes invité, saisissez le mot de passe pour la sauvegarde.
10. Dans **Contenu des sauvegardes**, sélectionnez les disques que vous souhaitez restaurer. Cliquez sur **OK** pour confirmer votre sélection.
11. Sous **Où restaurer**, le logiciel mappe automatiquement les disques sélectionnés vers les disques cibles.

    Si le mappage échoue, ou si vous n'êtes pas satisfait du résultat, vous pouvez remapper les disques manuellement.

    Remarque
    Modifier la disposition du disque peut affecter la capacité de démarrage du système d'exploitation. Veuillez utiliser la disposition originale du disque de la machine à moins que vous ne soyez certain de votre succès.

12. [Lors de la restauration de Linux] Si la machine sauvegardée possédait des volumes logiques (LVM) et que vous voulez en reproduire la structure initiale :
    a. Assurez-vous que le nombre de disques sur la machine cible et que leur capacité sont équivalents ou supérieurs à ceux de la machine d'origine, puis cliquez sur **Appliquer RAID/LVM**.
    b. Revoyez la structure des volumes et cliquez ensuite sur **Appliquer RAID/LVM** pour la créer.
13. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
14. Cliquez sur **OK** pour démarrer la restauration.

© Acronis International GmbH, 2003-2026

Restauration des fichiers

Restauration de fichiers dans la console Cyber Protect

Remarque
Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes dans des tenants en mode de conformité. Voir "Restauration de sauvegardes dans les tenants en mode de conformité" (p. 1617).

1. Sélectionnez la machine sur laquelle les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez le point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine sélectionnée est physique et hors ligne, les points de restauration ne sont pas affichés. Effectuez l'une des actions suivantes :

   - [Recommandé] Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine cible qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde.
   - Téléchargement de fichiers depuis le Cloud
   - Utilisation d'un support de démarrage
4. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
5. Accédez au dossier requis ou servez-vous de la barre de recherche pour obtenir la liste des fichiers et dossiers requis.

   La recherche ne dépend pas de la langue.

   Vous pouvez utiliser un ou plusieurs caractères génériques (* et ?). Pour plus de détails sur l'utilisation de caractères génériques, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 620).

   Remarque
   La recherche n'est pas disponible pour les sauvegardes de lecteur qui sont stockées dans le Cloud.
6. Sélectionnez les fichiers que vous voulez restaurer.
7. Si vous souhaitez enregistrer les fichiers au format .zip, cliquez sur **Télécharger**, sélectionnez l'emplacement où enregistrer les données et cliquez sur **Enregistrer**. Sinon, ignorez cette étape.

   Le téléchargement n'est pas disponible si votre sélection contient des dossiers ou si la taille totale des fichiers sélectionnés dépasse 100 Mo. Pour récupérer de plus grandes quantités de

© Acronis International GmbH, 2003-2026

données depuis le cloud, suivez la procédure "Téléchargement de fichiers dans la console Web Restore" (p. 709).

8. Cliquez sur **Restaurer**.

   Dans **Restaurer vers**, cliquez pour sélectionner la cible de l'opération de restauration ou conservez la cible par défaut. La cible par défaut varie en fonction de la source de la sauvegarde.

   Les cibles suivantes sont disponibles :

   - Machine source (si un agent de protection y est installé).

     Il s'agit de l'ordinateur qui contenait à l'origine les fichiers que vous souhaitez restaurer.
   - Autres ordinateurs sur lesquelles un agent de protection est installé : machines physiques, machines virtuelles et hôtes de virtualisation sur lesquels un agent de protection est installé, ou appliances virtuelles.

     Vous pouvez restaurer des fichiers sur des machines physiques, des machines virtuelles et des hôtes de virtualisation sur lesquels un agent de protection est installé. Vous ne pouvez pas restaurer des fichiers sur des machines virtuelles sur lesquelles aucun agent de protection n'est installé (à l'exception des machines virtuelles Virtuozzo).
   - Conteneurs ou machines virtuelles Virtuozzo.

     Vous pouvez restaurer des fichiers sur des conteneurs et des machines virtuelles Virtuozzo, avec toutefois quelques restrictions. Pour plus d'informations, voir "Limites de la restauration des fichiers dans la console Cyber Protect" (p. 713).
9. Dans **Chemin d'accès**, sélectionnez la destination de la restauration. Vous pouvez sélectionner l'une des options suivantes :

   - [Lors d'une restauration vers l'ordinateur d'origine] Emplacement d'origine.
   - Dossier local ou stockage attaché localement sur la machine cible.

     Remarque
     Les liens symboliques ne sont pas pris en charge.

   - un dossier réseau accessible depuis la machine cible

     Par exemple, lors de la restauration de fichiers à partir d'une machine virtuelle Microsoft Azure, le dossier réseau doit être accessible à l'agent pour Azure déployé sur la machine virtuelle.
10. Cliquez sur **Démarrer la restauration**.
11. Sélectionnez l'une des options d'écrasement de fichier :

    - **Écraser les fichiers existants**
    - **Écraser un fichier existant s'il est plus ancien**
    - **Ne pas écraser les fichiers existants**

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

© Acronis International GmbH, 2003-2026

Téléchargement de fichiers dans la console Web Restore

Dans la console Web de restauration, vous pouvez parcourir le stockage dans le cloud, voir le contenu des sauvegardes et télécharger des fichiers et des dossiers sauvegardés.

La console Web Restore est uniquement accessible aux comptes utilisateur de niveau client avec les rôles suivants :

- Administrateur d'entreprise
- Administrateur de Protection
- Utilisateur de Protection

Tous les comptes ne peuvent accéder qu'à leurs propres sauvegardes.

Les comptes utilisateur de niveau partenaire ne peuvent pas accéder à la console Web Restore.

Limites

- Vous ne pouvez pas télécharger des disques, des volumes ou des points de restauration complets sauvegardés.
- Lorsque vous parcourez les sauvegardes de niveau disque, les volumes logiques (tels que LVM et LDM) ne sont pas affichés.
- Vous ne pouvez pas parcourir les sauvegardes de l'état du système, des bases de données SQL et des bases de données Exchange.

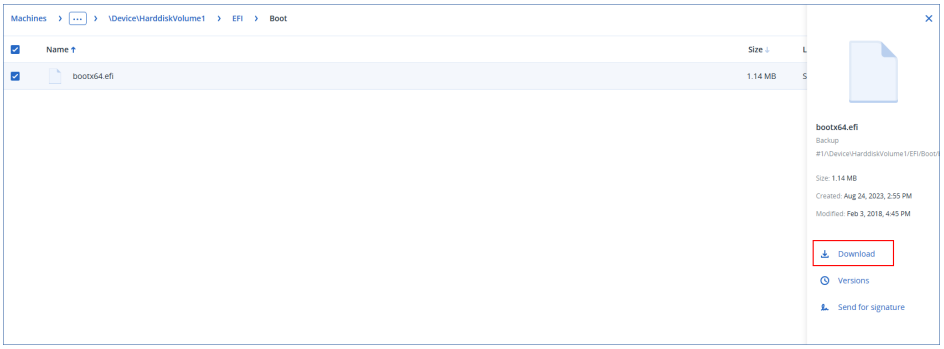
Pour télécharger des fichiers et des dossiers du stockage dans le cloud

1. Dans la console Cyber Protection, sélectionnez la ressource requise, puis cliquez sur **Restauration**.
2. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde, puis cliquez sur **Autres méthodes de restauration**.
3. Cliquez sur **Télécharger les fichiers**.
4. Sous **Ordinateurs**, cliquez sur le nom de la ressource, puis sur l'archive de sauvegarde.
   Une archive de sauvegarde contient une ou plusieurs sauvegardes (points de restauration).
5. Cliquez sur le numéro de sauvegarde (point de restauration) à partir duquel vous souhaitez télécharger des fichiers ou des dossiers, puis accédez aux éléments requis.
6. Cochez les cases situées à côté des éléments à télécharger.

Remarque
Si vous sélectionnez plusieurs éléments, ils sont téléchargés sous forme de fichier ZIP.

© Acronis International GmbH, 2003-2026

7. Cliquez sur **Télécharger**.



Vérification de l'authenticité d'un fichier grâce à Notary Service

Si la notarisation a été activée lors de la sauvegarde, vous pouvez vérifier l'authenticité d'un fichier sauvegardé.

Pour vérifier l'authenticité d'un fichier

1. Sélectionnez le fichier tel que décrit dans les étapes 1 à 6 de la section « Restauration de fichiers via l'interface Web », ou les étapes 1 à 5 de la section « Téléchargement de fichiers depuis le Cloud ».
2. Assurez-vous que le fichier sélectionné possède l'icône suivante :  . Cela signifie que le fichier est notarié.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Vérifier**.
     Le logiciel vérifie l'authenticité du fichier et affiche le résultat.
   - Cliquez sur **Obtenir certificat**.
     Un certificat confirmant la notarisation du fichier est ouvert dans une fenêtre de navigateur Web. La fenêtre contient également les instructions qui vous permettent de vérifier l'authenticité d'un fichier manuellement.

Signer un fichier avec ASign

ASign est un service permettant à plusieurs personnes de signer électroniquement un fichier sauvegardé. Cette fonctionnalité est accessible uniquement pour les sauvegardes de niveau fichier stockées dans le stockage dans le Cloud.

Une seule version de fichier peut être signée à la fois. Si le fichier a été sauvegardé à plusieurs reprises, vous devez choisir la version à signer, et seule cette version sera signée.

ASign peut par exemple être utilisé pour la signature électronique des fichiers suivants :

- Contrats de location ou baux
- Contrats de vente
- Conventions d'achat de biens

© Acronis International GmbH, 2003-2026

- Contrats de prêt
- Feuilles de permission
- Documents financiers
- Documents d'assurance
- Décharges de responsabilité
- Documents médicaux
- Documents de recherche
- Certificats d'authenticité
- Accords de non-divulgation
- Lettres de proposition
- Accords de confidentialité
- Contrats de prestataires indépendants

Pour signer une version de fichier

1. Sélectionnez le fichier tel que décrit dans les étapes 1 à 6 de la section « Restauration de fichiers via l'interface Web », ou les étapes 1 à 5 de la section « Téléchargement de fichiers depuis le Cloud ».
2. Assurez-vous que la bonne date et la bonne heure sont sélectionnées dans le volet de gauche.
3. Cliquez sur **Signer cette version de fichier**.
4. Indiquez le mot de passe pour le compte de stockage dans le Cloud sous lequel la sauvegarde est stockée. L'identifiant de connexion du compte est affiché dans votre fenêtre d'invite.
   L'interface du service ASign est ouverte dans une fenêtre de navigateur Web.
5. Ajoutez d'autres signataires en indiquant leur adresse e-mail. Il n'est pas possible d'ajouter ou supprimer des signataires après avoir envoyé les invitations, assurez-vous donc que la liste contient chaque personne dont la signature est nécessaire.
6. Cliquez sur **Inviter à signer** pour envoyer l'invitation aux signataires.
   Chaque signataire reçoit un e-mail contenant la demande de signature. Lorsque tous les signataires auxquels vous l'aurez demandé auront signé le fichier, ce dernier sera notarié et signé via le service de notarisation.
   Vous recevrez une notification à la signature de chaque signataire, et lorsque le processus sera entièrement terminé. Vous pouvez accéder à la page Web ASign en cliquant sur **Afficher les détails** dans l'un des e-mails que vous recevez.
7. Une fois le processus terminé, rendez-vous sur la page Web ASign et cliquez sur **Obtenir le document** pour télécharger un document .pdf contenant :
   - La page du certificat de signature avec toutes les signatures récoltées.
   - La page du journal d'audit contenant l'historique des activités : date/heure à laquelle l'invitation a été envoyée aux signataires, date/heure à laquelle chaque signataire a signé le fichier, etc.

© Acronis International GmbH, 2003-2026

Restauration de fichiers via un support de démarrage

L'exécution du support de démarrage nécessite 1,5 Go de RAM.

Pour plus d'informations sur la création d'un support de démarrage, voir "Création d'un support de démarrage physique" (p. 991).

Pour restaurer des fichiers via un support de démarrage

1. Démarrez la machine cible à l'aide du support de démarrage.
2. Cliquez sur **Gérer cette machine localement** ou double-cliquez sur **Support de Secours Bootable**, en fonction du type de support que vous utilisez.
3. Si un serveur proxy est activé dans votre réseau, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez l'adresse IP/nom de l'hôte, le port et les informations d'identification du serveur proxy. Sinon, ignorez cette étape.
4. [Facultatif] Lors d'une restauration depuis Windows ou Linux, cliquez sur **Outils** > **Enregistrer le support au sein du service Cyber Protection**, puis spécifiez le jeton d'enregistrement que vous avez obtenu lorsque vous avez téléchargé le support. Si vous faites cela, vous n'aurez pas besoin de saisir d'informations d'identification ni de code d'inscription pour accéder au stockage Cloud, comme décrit à l'étape 7.
5. Sur l'écran d'accueil, cliquez sur **Restaurer**.
6. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
7. Indiquez l'emplacement de la sauvegarde :
   - Pour restaurer des informations depuis le Cloud, sélectionnez **Stockage dans le Cloud**. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.

     Lors d'une restauration Windows ou Linux, vous avez la possibilité de demander un code d'inscription et de l'utiliser à la place de vos informations d'identification. Cliquez sur **Utiliser le code d'inscription** > **Demander le code**. Le logiciel affiche le lien et le code d'inscription. Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Le code d'enregistrement n'est valable qu'une heure.
   - Pour effectuer une restauration depuis un dossier local ou réseau, rendez-vous dans **Dossiers locaux** ou **Dossiers réseau**.
   - Pour restaurer à partir d'emplacements de sauvegarde sur un stockage cloud public tel que Microsoft Azure, Amazon S3 ou un stockage compatible S3, cliquez d'abord sur **Enregistrer le support dans le service Cyber Protection**, puis configurez la restauration à l'aide de l'interface Web. Pour plus d'informations sur la gestion des supports à distance via l'interface Web, consultez "Opérations à distance avec un support de démarrage" (p. 1009).

   Cliquez sur **OK** pour confirmer votre sélection.
8. Sélectionnez la sauvegarde à partir de laquelle vous voulez restaurer les données. Si vous y êtes invité, saisissez le mot de passe pour la sauvegarde.

© Acronis International GmbH, 2003-2026

9. Dans **Contenu des sauvegardes**, sélectionnez **Dossiers/fichiers**.
10. Sélectionnez les données que vous voulez restaurer. Cliquez sur **OK** pour confirmer votre sélection.
11. Dans **Où restaurer**, indiquez un dossier. Vous pouvez également empêcher l'écrasement des versions plus récentes des fichiers ou exclure certains fichiers de la restauration.
12. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
13. Cliquez sur **OK** pour démarrer la restauration.

Extraction de fichiers à partir de sauvegardes locales

Vous pouvez explorer les contenus de sauvegardes et extraire les fichiers dont vous avez besoin.

Configuration requise

- Cette fonctionnalité est uniquement disponible sous Windows à l'aide de l'Explorateur de fichiers.
- Le système du fichier sauvegardé doit être l'un des suivants : FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS ou HFS+.

Prérequis

- Un agent de protection doit être installé sur la machine utilisée pour explorer la sauvegarde.
- La sauvegarde doit être stockée dans un dossier local ou sur un partage réseau (SMB/CIFS).

Extraction de fichiers à partir d'une sauvegarde

1. Accédez à l'emplacement de la sauvegarde à l'aide de l'Explorateur de fichiers.
2. Double-cliquez sur le fichier de sauvegarde. Les noms des fichiers reposent sur l'exemple suivant :
   `<machine name> - <protection plan GUID>`
3. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement. Sinon, ignorez cette étape.
   L'Explorateur de fichiers affiche les points de restauration.
4. Double-cliquez sur le point de restauration.
   L'Explorateur de fichiers affiche les données sauvegardées.
5. Accédez au dossier requis.
6. Copiez les fichiers requis vers n'importe quel dossier du système de fichiers.

Limites de la restauration des fichiers dans la console Cyber Protect

Tenants en mode de Conformité

Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes dans des tenants en mode de conformité. Voir "Restauration de sauvegardes dans les tenants en mode de conformité" (p. 1617).

© Acronis International GmbH, 2003-2026

Restauration sur des conteneurs ou machines virtuelles Virtuozzo

- L'agent client QEMU doit être installé sur la machine virtuelle cible.
- [S'applique uniquement lors de la restauration dans des conteneurs] Les points de montage dans les conteneurs ne peuvent pas être utilisés comme cible de restauration. Par exemple, vous ne pouvez pas restaurer des fichiers sur un second disque dur ou sur un partage NFS monté dans un conteneur.
- Lors de la restauration de fichiers dans une machine virtuelle Windows et si l'option de restauration "Sécurité de niveau fichier" (p. 726) est activée, l'attribut de bit d'archive est défini sur les fichiers restaurés.
- Les fichiers comportant dans leur nom des caractères non-ANSI sont restaurés avec des noms incorrects sur les ordinateurs exécutant Windows Server 2012 ou une version antérieure, et Windows 7 ou une version antérieure.
- Pour restaurer des fichiers sur des machines virtuelles CentOS ou Red Hat Enterprise Linux qui s'exécutent sur Virtuozzo Hybrid Server, vous devez modifier le fichier `qemu-ga` comme suit :
  - Sur la machine virtuelle cible, accédez à `/etc/sysconfig/`, puis ouvrez le fichier `qemu-ga` pour le modifier.
  - Accédez à la ligne suivante, puis supprimez tout ce qui suit le signe égal (=) :

    ```
    BLACKLIST_RPC=
    ```

  - Redémarrez l'agent client QEMU en exécutant la commande suivante :

    ```
    systemctl restart qemu-guest-agent
    ```

Restauration de l'état du système

Remarque
Dans la console Cyber Protect, vous ne pouvez pas restaurer des sauvegardes dans des tenants en mode de conformité. Voir "Restauration de sauvegardes dans les tenants en mode de conformité" (p. 1617).

1. Sélectionnez la machine pour laquelle vous voulez restaurer l'état du système.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration de l'état du système. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer l'état du système**.
5. Confirmez que vous souhaitez écraser l'état du système avec sa version sauvegardée.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

© Acronis International GmbH, 2003-2026

Restauration d'une configuration ESXi

Pour restaurer une configuration ESXi, vous avez besoin d'un support de démarrage basé sur Linux. Pour en savoir plus sur la manière de créer un support de démarrage, consultez la section "Création d'un support de démarrage physique" (p. 991).

Si vous restaurez une configuration ESXi sur un hôte non d'origine et que l'hôte ESXi d'origine est toujours connecté au vCenter Server, déconnectez et supprimez cet hôte du vCenter Server pour éviter des problèmes inattendus au cours de la restauration. Si vous souhaitez conserver l'hôte d'origine ainsi que l'hôte restauré, vous pouvez de nouveau l'ajouter une fois la restauration terminée.

Les machines virtuelles s'exécutant sur l'hôte ne sont pas incluses dans la sauvegarde de la configuration ESXi. Elles peuvent être sauvegardées et restaurées séparément.

Pour restaurer une configuration ESXi

1. Démarrez la machine cible à l'aide du support de démarrage.
2. Cliquez sur **Gérer cette machine localement**.
3. Sur l'écran d'accueil, cliquez sur **Restaurer**.
4. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
5. Indiquez l'emplacement de la sauvegarde :
   - Accédez au dossier sous **Dossiers locaux** ou **Dossiers réseau**.

   Cliquez sur **OK** pour confirmer votre sélection.
6. Dans **Afficher**, sélectionnez **Configurations ESXi**.
7. Sélectionnez la sauvegarde à partir de laquelle vous voulez restaurer les données. Si vous y êtes invité, saisissez le mot de passe pour la sauvegarde.
8. Cliquez sur **OK**.
9. Dans **Disques à utiliser pour les nouveaux magasins de données**, procédez comme suit :
   - Sous **Restaurer ESXi sur**, sélectionnez le disque de restauration de la configuration de l'hôte. Si vous restaurez la configuration sur l'hôte d'origine, le disque d'origine est sélectionné par défaut.
   - [Facultatif] Sous **Utiliser pour les nouveaux magasins de données**, sélectionnez les disques où les nouveaux magasins de données seront créés. Soyez vigilant car toutes les données sur les disques sélectionnés seront perdues. Si vous souhaitez conserver les machines virtuelles dans les magasins de données existants, ne sélectionnez aucun disque.
10. Si aucun disque pour les nouveaux magasins de données n'est sélectionné, sélectionnez la méthode de création de magasins de données dans **Comment créer de nouveaux magasins de données** : **Créer un magasin de données par disque** ou **Créer un magasin de données sur tous les disques durs sélectionnés**.
11. [Facultatif] Dans **Mappage de réseau**, changez le résultat du mappage automatique des commutateurs virtuels présents dans la sauvegarde pour les adaptateurs réseau physiques.

© Acronis International GmbH, 2003-2026

12. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
13. Cliquez sur **OK** pour démarrer la restauration.

Restauration avec redémarrage

Un redémarrage est nécessaire lorsque vous restaurez les éléments suivants :

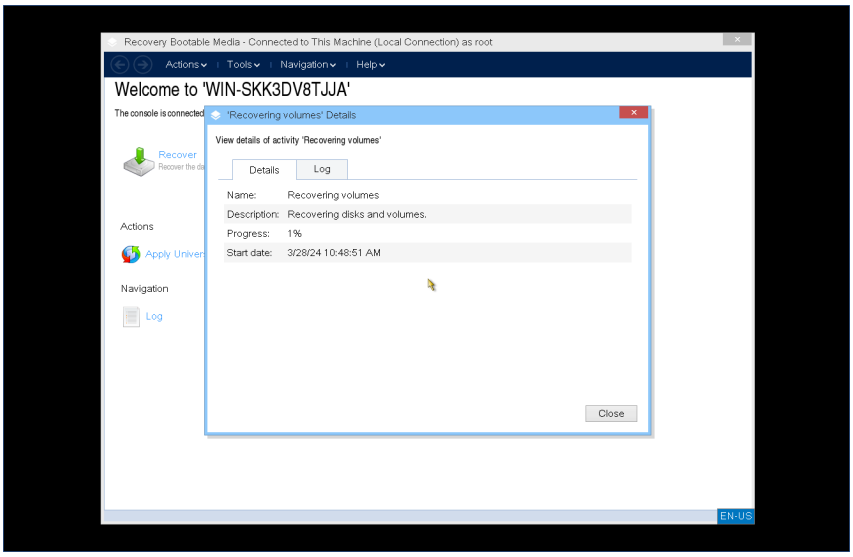
- Un système d'exploitation

  Par exemple, lorsque vous restaurez un ordinateur complet ou le volume système d'un ordinateur.
- Volumes chiffrés

  Par exemple, lorsque vous restaurez des volumes chiffrés par BitLocker ou CheckPoint.

Important
Les volumes chiffrés et sauvegardés sont restaurés comme volumes non chiffrés.

Un environnement de restauration est automatiquement préparé sur l'ordinateur restauré. Lorsque l'environnement est prêt, l'ordinateur redémarre, puis l'environnement de restauration s'ouvre. Lorsque la restauration est terminée, le système d'exploitation démarre.



Remarque
La préparation de l'environnement de restauration WinRE peut prendre jusqu'à trois minutes.

Pour plus d'informations sur les environnements de restauration disponibles, voir "Environnements de restauration" (p. 716).

Environnements de restauration

Vous pouvez utiliser WinRE ou l'environnement de restauration Linux.

Le tableau ci-dessous résume les options disponibles.

© Acronis International GmbH, 2003-2026

Ordinateur restauré	Environnement de restauration	
	WinRE	Linux
Windows	Oui (par défaut)*	Oui
Linux	Sans Objet	Oui

Remarque

* Si l'environnement de restauration WinRE par défaut ne peut pas démarrer, l'opération de restauration basculera automatiquement vers l'environnement Linux. Si vous définissez explicitement l'environnement de restauration sur WinRE ou Linux, seul l'environnement sélectionné sera utilisé. Pour plus d'informations, voir "Modification de l'environnement de restauration" (p. 718).

La préparation de l'environnement de restauration WinRE peut prendre jusqu'à trois minutes.

Espace disque nécessaire

L'environnement de restauration nécessite de l'espace disque pour les fichiers temporaires. La configuration requise varie en fonction de l'ordinateur restauré.

Le tableau ci-dessous résume les options disponibles.

Mode de démarrage	Ordinateur avec volume système non chiffré	Ordinateur avec volume système chiffré
BIOS	1 Go dans le dossier `Windows\Temp`	1 Go dans le dossier `Windows\Temp`
UEFI	1 Go dans le dossier `Windows\Temp`	1 Go dans le dossier `Windows\Temp`
BIOS	200 Mo sur le volume système	400 Mo sur un volume non chiffré
UEFI	200 Mo sur la partition système EFI (ESP)	L'un des éléments suivants : • 400 Mo sur la partition système EFI (ESP) • 200 Mo sur la partition système EFI (ESP) et 200 Mo sur une partition non chiffrée accessible pendant le processus de démarrage.

* La restauration d'un ordinateur avec un volume système chiffré nécessite au moins un volume non chiffré sur le même ordinateur.

Limites

- Avant la restauration, vous devez verrouiller tous les volumes non système chiffrés. Vous pouvez verrouiller un volume en ouvrant un fichier qui y réside. Si le volume n'est pas verrouillé, la restauration se poursuivra sans redémarrage et le volume risque de ne pas être reconnu par le

© Acronis International GmbH, 2003-2026

système d'exploitation.

Il n'est pas nécessaire de verrouiller un volume système chiffré.

Dépannage

Si la restauration échoue et que l'erreur `Impossible d'obtenir le fichier de la partition` s'affiche après le redémarrage, désactivez Secure Boot. Pour plus d'informations, voir Désactivation de Secure Boot dans la documentation Microsoft.

Modification de l'environnement de restauration

Vous pouvez modifier l'environnement de restauration par défaut dans les ressources Windows.

Pour les ressources Linux, seul l'environnement de restauration Linux est disponible.

Pour définir WinRE

1. Sous Windows, ouvrez **Regedit**.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Créez une nouvelle valeur de chaîne, puis nommez-la **RebootEnvironmentType**.
4. Ouvrez la valeur de chaîne pour la modifier.
5. Dans **Données de la valeur**, spécifiez `Windows`.
6. Cliquez sur **OK**.

Pour définir Linux

1. Sous Windows, ouvrez **Regedit**.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Créez une nouvelle valeur de chaîne, puis nommez-la **RebootEnvironmentType**.
4. Ouvrez la valeur de chaîne pour la modifier.
5. Dans **Données de la valeur**, spécifiez `Linux`.
6. Cliquez sur **OK**.

Pour réinitialiser les paramètres par défaut

1. Sous Windows, ouvrez **Regedit**.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Supprimez la valeur de chaîne **RebootEnvironmentType**.
4. Pour confirmer votre choix, cliquez sur **Oui**.

En utilisant Universal Restore

Les systèmes d'exploitation les plus récents peuvent être démarrés lorsqu'ils sont restaurés sur un matériel différent, notamment sur les plates-formes VMware ou Hyper-V. Si un système

© Acronis International GmbH, 2003-2026

d'exploitation restauré ne démarre pas, utilisez l'outil Universal Restore pour mettre à jour les pilotes et les modules essentiels au démarrage du système d'exploitation.

Universal Restore peut s'appliquer à Windows et Linux.

Pour appliquer Universal Restore

1. Démarrez la machine à partir du support de démarrage.
2. Cliquez sur **Appliquer Universal Restore**.
3. S'il existe plusieurs systèmes d'exploitation sur la machine, choisissez celui sur lequel appliquer Universal Restore.
4. [Pour Windows uniquement] Configurez les paramètres supplémentaires.
5. Cliquez sur **OK**.

Universal Restore sous Windows

Préparation

Préparez les pilotes

Avant d'appliquer Universal Restore à un système d'exploitation Windows, assurez-vous que vous avez les pilotes pour le nouveau contrôleur de disque dur et pour le jeu de puces. Ces pilotes sont cruciaux pour lancer le système d'exploitation. Utilisez le CD ou le DVD fourni par le fabricant du matériel ou téléchargez les pilotes depuis le site Web du fabricant. Les fichiers pilotes doivent avoir l'extension *.inf. Si vous téléchargez les pilotes au format *.exe, *.cab ou *.zip, veuillez les extraire en utilisant une application tierce.

La meilleure pratique consiste à stocker les pilotes pour tout le matériel utilisé dans votre organisation dans un seul dépôt trié par type de terminal ou par configuration matérielle. Vous pouvez conserver une copie du dépôt sur un DVD ou sur un lecteur flash ; choisissez des pilotes et ajoutez-les au support de démarrage ; créez le support de démarrage personnalisé avec les pilotes nécessaires (et les configurations réseau nécessaires) pour chacun de vos serveurs. Vous pouvez aussi simplement spécifier le chemin vers le répertoire chaque fois que Universal Restore est utilisé.

Vérifiez l'accès aux pilotes dans l'environnement de démarrage

Assurez-vous que vous avez accès au terminal contenant les pilotes quand vous travaillez en utilisant un support de démarrage. Utilisez un support basé sur WinPE si le terminal est disponible sous Windows mais que le support basé sur Linux ne le détecte pas.

Paramètres de Universal Restore

Recherche de pilote automatique

Spécifiez où le programme recherchera les pilotes de la couche d'abstraction matérielle (HAL - Hardware Abstraction Layer), du contrôleur de disque dur et de l'adaptateur réseau :

© Acronis International GmbH, 2003-2026

- Si les pilotes se trouvent sur le disque d'un fournisseur ou sur un autre support amovible, activez **Rechercher dans le support amovible**.
- Si les pilotes sont situés dans un dossier en réseau ou sur le support de démarrage, spécifiez le chemin d'accès au dossier en cliquant sur **Ajouter un dossier**.

En outre, Universal Restore recherche dans le dossier Windows de stockage des pilotes par défaut. Son emplacement est indiqué dans la valeur de registre **DevicePath**, laquelle se trouve dans la clé de la base de registre **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Ce dossier de stockage est généralement WINDOWS / inf.

Universal Restore exécute une recherche récursive dans tous les sous-dossiers du dossier spécifié, trouve les pilotes HAL et de contrôleur de disque dur les plus appropriés de tous ceux qui sont disponibles, et les installe sur le système restauré. Universal Restore recherche également le pilote de la carte réseau ; le chemin vers le pilote trouvé est alors transmis par Universal Restore au système d'exploitation. Si le matériel possède plusieurs cartes d'interface réseau, Universal Restore tentera de configurer les pilotes de toutes les cartes.

Pilotes de stockage de masse à installer de toutes façons

Vous avez besoin de ce paramètre si :

- Le matériel a un contrôleur de stockage de masse spécifique tel que RAID (particulièrement NVIDIA RAID) ou un adaptateur fibre channel.
- Vous avez effectué la migration d'un système sur une machine virtuelle qui utilise un contrôleur de disque dur SCSI. Utilisez les pilotes SCSI fournis avec le logiciel de virtualisation ou téléchargez les versions les plus récentes des pilotes à partir du site Web du fabricant du logiciel.
- La recherche de pilotes automatiques n'aide pas a démarrer le système.

Spécifiez les pilotes appropriés en cliquant sur **Ajouter le pilote**. Les pilotes définis ici sont installés, avec un avertissement approprié, même si le programme trouve un meilleur pilote.

Processus Universal Restore

Après avoir spécifié les paramètres requis, cliquez sur **OK**.

Si Universal Restore ne peut pas trouver un pilote compatible dans les emplacements spécifiés, il affiche une invite sur le terminal problématique. Effectuez l'une des actions suivantes :

- Ajoutez le pilote dans n'importe quel emplacement spécifié précédemment et cliquez sur **Réessayer**.
- Si vous ne vous souvenez pas de l'emplacement, cliquez sur **Ignorer** pour continuer le processus. Si le résultat n'est pas satisfaisant, appliquez Universal Restore à nouveau. Lorsque vous configurez l'opération, spécifiez le pilote nécessaire.

Lorsque Windows démarre, la procédure courante pour l'installation de nouveaux matériels sera initialisée. Le pilote de l'adaptateur réseau est installé silencieusement si le pilote a la signature Microsoft Windows. Sinon, Windows demandera de confirmer l'installation du pilote ne possédant pas la signature.

© Acronis International GmbH, 2003-2026

Après cela, vous pouvez configurer la connexion réseau et spécifier les pilotes pour les adaptateurs graphique, USB et autres périphériques.

Universal Restore sous Linux

Universal Restore peut être appliqué aux systèmes opérationnels de version Linux 2.6.8 ou supérieure.

Quand Universal Restore est appliqué à un système d'exploitation Linux, il met à jour un système de fichiers temporaire connu comme le disque RAM initial (initrd). Cela garantit que le système d'exploitation peut démarrer sur le nouveau matériel.

Universal Restore ajoute des modules pour le nouveau matériel (y compris les pilotes de périphériques) pour le disque RAM initial. En règle générale, il trouve les modules nécessaires dans le répertoire **/lib/modules**. Si Universal Restore ne peut pas trouver un module dont il a besoin, il enregistre le nom de fichier du module dans le journal.

Universal Restore peut modifier la configuration du chargeur de démarrage GRUB. Cela peut être nécessaire, par exemple, pour assurer la capacité de démarrage du système lorsque la nouvelle machine possède une structure de volume différente de la machine d'origine.

Universal Restore ne modifie jamais le noyau Linux.

Pour rétablir le disque RAM initial d'origine

Vous pouvez rétablir le disque RAM initial d'origine si nécessaire.

Le disque RAM initial est stocké sur la machine dans un fichier. Avant de mettre à jour le disque RAM initial pour la première fois, Universal Restore en enregistre une copie dans le même répertoire. Le nom de la copie est le nom du fichier, suivi par le suffixe **_acronis_backup.img**. Cette copie ne sera pas écrasée si vous exécutez Universal Restore plusieurs fois (par exemple, après avoir ajouté des pilotes manquants).

Pour rétablir le disque RAM initial d'origine, exécutez l'une des actions suivantes :

- Renommez la copie en conséquence. Par exemple, exécutez une commande semblable à celle-ci :

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
```

- Spécifiez la copie dans la ligne **initrd** de la configuration du chargeur de démarrage GRUB.

Options de restauration

Pour modifier les options de restauration, cliquez sur **Options de restauration** lors de la configuration de la restauration.

Disponibilité des options de restauration

L'ensemble des options de restauration disponibles dépendent de :

© Acronis International GmbH, 2003-2026

- L'environnement dans lequel fonctionne l'agent effectuant la restauration (Windows, Linux, macOS ou support de démarrage).
- le type de données en cours de restauration (disques, fichiers, machines virtuelles, données d'application).

Le tableau suivant résume la disponibilité des options de restauration.

	Disques			Fichiers				Machines virtuelles		SQL et Exchange
	Windows	Linux	Support de démarrage	Windows	Linux	macOS	Support de démarrage	ESXi, Hyper-V, Scale Computing, oVirt et Virtuozzo	Azure	Windows
Validation de la sauvegarde	+	+	+	+	+	+	+	+	-	+
Mode de démarrage	+	-	-	-	-	-	-	+	-	-
Date et heure des fichiers	-	-	-	+	+	+	+	-	-	-
Gestion erreurs	+	+	+	+	+	+	+	+	+	+
Exclusions de fichiers	-	-	-	+	+	+	+	-	-	-
Sécurité de niveau fichier	-	-	-	+	-	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-	-
Restauration de chemin d'accès complet	-	-	-	+	+	+	+	-	-	-
Points de montage	-	-	-	+	-	-	-	-	-	-

© Acronis International GmbH, 2003-2026

Performance	+	+	-	+	+	+	-	+	-	+
Commandes Pré/Post	+	+	-	+	+	+	-	+	-	+
Modification de SID	+	-	-	-	-	-	-	-	-	-
Gestion de l'alimentation des MV	-	-	-	-	-	-	-	+	+	-
Journal des événements Windows	+	-	-	+	-	-	-	Hyper-V uniquement	-	+

Validation de la sauvegarde

Cette option définit si la sauvegarde doit être validée avant la restauration des données afin de garantir qu'elle n'est pas corrompue. Cette opération est effectuée par l'agent de protection.

Le préréglage est le suivant : **Désactivé**.

Pour en savoir plus sur la validation par vérification de somme de contrôle, reportez-vous à "Vérification de la somme de contrôle" (p. 261).

Remarque
Selon les paramètres choisis par votre fournisseur de services, il se peut que la validation ne soit pas disponible lors d'une sauvegarde sur le stockage dans le Cloud.

Mode de démarrage

Cette option est effective lors de la restauration d'une machine physique ou virtuelle depuis une sauvegarde de lecteur contenant un système d'exploitation Windows.

Cette option vous permet de sélectionner le mode de démarrage (BIOS ou UEFI) que Windows utilisera après la restauration. Si le mode de démarrage de la machine d'origine diffère du mode de démarrage sélectionné, le logiciel :

- Initialisera le disque vers lequel vous restaurez le volume système, en fonction du mode de démarrage sélectionné (MBR pour BIOS, GPT pour UEFI).

© Acronis International GmbH, 2003-2026

- Ajustera le système d'exploitation Windows afin qu'il puisse démarrer en utilisant le mode de démarrage sélectionné.

Le préréglage est le suivant : **Comme sur la machine cible.**

Vous pouvez choisir l'une des options suivantes:

- **Comme sur la machine cible**

  L'agent qui s'exécute sur la machine cible détecte le mode de démarrage actuellement utilisé par Windows et procède aux ajustements en fonction du mode de démarrage sélectionné.

  C'est la valeur la plus sûre qui entraîne un système bootable, sauf si les restrictions répertoriées ci-dessous s'appliquent. Étant donné que l'option **Mode de démarrage** est absente sous le support de démarrage, l'agent sur le support se comporte toujours comme si la valeur était choisie.
- **Comme sur la machine sauvegardée**

  L'agent qui s'exécute sur la machine cible lit le mode de démarrage depuis la sauvegarde et procède aux ajustements en fonction de ce mode de démarrage. Ceci vous aide à restaurer un système sur une machine différente, même si cette machine utilise un autre mode de démarrage, puis remplace le disque dans la machine sauvegardée.
- **BIOS**

  L'agent qui s'exécute sur la machine cible procède aux ajustements nécessaires à l'utilisation de BIOS.
- **UEFI**

  L'agent qui s'exécute sur la machine cible procède aux ajustements nécessaires à l'utilisation d'UEFI.

Une fois qu'un paramètre sera modifié, la procédure de mappage de disque sera répétée. Cela peut prendre un certain temps.

Recommandations

Si vous devez transférer Windows entre UEFI et BIOS :

- Restaurez le disque à l'emplacement du volume système. Si vous restaurez uniquement le volume système au-dessus d'un volume existant, l'agent ne pourra pas initialiser correctement le disque de destination.
- N'oubliez pas que le BIOS ne permet pas l'utilisation de plus de 2 To d'espace disque.

Limites

- Le transfert entre UEFI et BIOS est compatible avec :
  - Les systèmes d'exploitation Windows 64 bits à partir de Windows 7
  - Les systèmes d'exploitation Windows Server 64 bits à partir de Windows Server 2008 SP1

Lorsque le transfert d'un système entre UEFI et BIOS n'est pas pris en charge, l'agent se comporte comme si le paramètre **Comme sur la machine sauvegardée** était choisi. Si la machine cible

© Acronis International GmbH, 2003-2026

prend en charge à la fois UEFI et BIOS, vous devez activer manuellement le mode de démarrage correspondant à la machine d'origine. Sinon, le système ne démarrera pas.

Date et heure des fichiers

Cette option est effective uniquement lors de la restauration de fichiers.

Cette option définit si la date et l'heure des fichiers doivent être restaurées depuis la sauvegarde ou assignées selon les valeurs actuelles.

Si cette option est activée, les fichiers présenteront la date et l'heure actuelles.

Le préréglage est le suivant : **Activé**.

Gestion erreurs

Ces options vous permettent de spécifier comment traiter des erreurs qui peuvent se produire pendant la restauration.

Réessayer si une erreur se produit

Le préréglage est le suivant : **Activé. Nombre de tentatives : 30. Intervalle entre les tentatives : 30 secondes.**

Lorsqu'une erreur récupérable se produit, le programme essaie à nouveau d'effectuer l'opération qui a échoué. Vous pouvez définir l'intervalle de temps ainsi que le nombre de tentatives. Les tentatives s'arrêteront dès que l'opération réussira OU que le nombre de tentatives sera atteint, le premier de ces deux cas prévalant.

Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux)

Le préréglage est le suivant : **Désactivé**.

Avec le mode silencieux activé, le programme gérera automatiquement les situations nécessitant une intervention de l'utilisateur dans la mesure du possible. Si une opération ne peut pas se poursuivre sans l'intervention de l'utilisateur, elle échouera. Les détails de l'opération, y compris les erreurs, le cas échéant, apparaissent dans le journal des opérations.

Ignorer les erreurs

Cette option est effective uniquement pour une sauvegarde de niveau fichier.

Le préréglage est le suivant : **Activé**.

Lorsque cette option est activée et que la restauration d'un fichier échoue, l'opération de restauration se poursuit pour les autres fichiers. Un avertissement s'affiche sur l'écran **Activités**. L'option **Réessayer si une erreur se produit** n'est pas déclenchée, car aucune erreur n'est consignée.

Lorsque cette option est désactivée et que la restauration d'un fichier échoue, l'opération de restauration échoue. Une erreur s'affiche dans l'écran **Activités**.

© Acronis International GmbH, 2003-2026

Enregistrer des informations système au cas où une restauration avec un redémarrage échouerait

Cette option est effective pour une restauration de disque ou volume sur une machine physique sous Windows ou Linux.

Le préréglage est le suivant : **Désactivé**.

Quand cette option est activée, vous pouvez indiquer un dossier sur le disque local (y compris des lecteurs flash ou des disques durs connectés à la machine cible) ou sur un partage réseau où seront enregistrés le journal, les informations système et les fichiers de vidage mémoire après plantage. Ce fichier aidera le personnel du support technique à identifier le problème.

Exclusions de fichiers

Cette option est effective uniquement lors de la restauration de fichiers.

Cette option définit les fichiers et dossiers à ignorer pendant le processus de restauration et à exclure ainsi de la liste des éléments restaurés.

Remarque
Les exclusions remplacent la sélection des éléments de données à restaurer. Par exemple, si vous sélectionnez cette option pour restaurer le fichier MonFichier.tmp en excluant tous les fichiers .tmp, le fichier MonFichier.tmp ne sera pas restauré.

Sécurité de niveau fichier

Cette option est effective lors de la restauration de fichiers sur disque et au niveau des fichiers pour des volumes formatés NTFS.

Cette option définit s'il faut restaurer les permissions NTFS pour les fichiers avec les fichiers eux-mêmes.

Le préréglage est le suivant : **Activé**.

Vous pouvez choisir de restaurer les permissions ou de laisser les fichiers hériter des permissions NTFS du dossier vers lequel ils sont restaurés.

Flashback

Cette option est efficace lors de la restauration des disques et volumes sur des machines physiques et virtuelles, excepté pour Mac.

Cette option fonctionne uniquement si la disposition du volume du disque en cours de restauration correspond exactement à celui du disque de destination.

Si l'option est activée, seules les différences entre les données de la sauvegarde et le disque de destination sont restaurées. Cela accélère la restauration des machines physiques et virtuelles. Les données sont comparées au niveau des blocs.

© Acronis International GmbH, 2003-2026

Lors de la restauration d'une machine physique, le préréglage est : **Désactivé**.

Lors de la restauration d'une machine virtuelle, le préréglage est : **Activé**.

Restauration de chemin d'accès complet

Cette option est effective seulement lors de la restauration de données d'une sauvegarde de niveau fichier.

Si cette option est activée, le chemin d'accès complet au fichier est recréé dans l'emplacement cible

Le préréglage est le suivant : **Désactivé**.

Points de montage

Cette option est efficace seulement sous Windows pour restaurer des données d'une sauvegarde de niveau fichier.

Activez cette option pour restaurer des fichiers et dossiers qui ont été stockés sur des volumes montés et qui ont été sauvegardés avec l'option Points de montage activée.

Le préréglage est le suivant : **Désactivé**.

Cette option est efficace seulement lorsque vous sélectionnez un dossier à restaurer qui est supérieur au point de montage dans l'arborescence des dossiers. Si vous sélectionnez des dossiers à restaurer qui sont dans le point de montage ou le point de montage lui-même, les éléments sélectionnés seront restaurés peu importe la valeur de l'option **Points de montage**.

Remarque
Veuillez être conscients que si le volume n'est pas monté au moment de la restauration, les données seront restaurées directement dans le dossier était le point de montage au moment de la sauvegarde.

Performance

Cette option définit la priorité du processus de restauration dans le système d'exploitation.

Les paramètres disponibles sont les suivants : **Basse**, **Normale**, **Élevé**.

Le préréglage est le suivant : **Normale**.

Le degré de priorité des processus exécutés dans un système détermine le niveau d'utilisation du processeur et la quantité de ressources système qui leur sont allouées. Réduire la priorité de restauration libérera davantage de ressources pour les autres applications. Augmenter la priorité de restauration pourrait accélérer le processus de restauration en imposant au système d'exploitation d'allouer plus de ressources à l'application qui effectuera la restauration Cependant, l'effet en résultant dépendra de l'utilisation globale du processeur ainsi que d'autres facteurs comme la vitesse d'E/S du disque ou le trafic réseau.

© Acronis International GmbH, 2003-2026

Commandes Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la restauration des données.

Exemple de possibilités d'utilisation des commandes avant/après :

- Lancez la commande **Checkdisk** afin de détecter et réparer les erreurs de systèmes de fichiers logiques, les erreurs physiques ou les secteurs défectueux à démarrer avant le début de la restauration ou après la fin de la restauration.

Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).

Une commande post-restauration ne sera pas exécutée si la restauration exécute un redémarrage.

Commande avant la restauration

Pour spécifier une commande / un fichier de traitement par lots à exécuter avant le début du processus de restauration

1. Activez le commutateur **Exécuter une commande avant la restauration**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots. Le programme ne prend pas en charge de commandes interactives, c'est à dire des commandes qui impliquent une saisie de l'utilisateur (par exemple, « pause »).
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, indiquez les arguments d'exécution de commande si nécessaire.
5. En fonction du résultat que vous voulez obtenir, sélectionnez les options appropriées comme décrit dans le tableau ci-dessous.
6. Cliquez sur **Terminé**.

Case à cocher	Sélection			
Faire échouer la restauration si l'exécution de la commande échoue*	Sélectionné	Effacé	Sélectionné	Effacé
Ne pas récupérer tant que l'exécution de la commande	Sélectionné	Sélectionné	Effacé	Effacé

© Acronis International GmbH, 2003-2026

n'est pas achevée				
Résultat				
	Préréglage Effectuer la restauration uniquement si la commande a été exécutée avec succès. Faire échouer la restauration si l'exécution de la commande échoue.	Effectuer la restauration après l'exécution de la commande, indépendamment de l'échec ou du succès de l'exécution.	Sans Objet	Effectuer la restauration en même temps que l'exécution de la commande et quel que soit le résultat de l'exécution de la commande.

* Une commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro.

Commande après la restauration

Pour spécifier une commande / un fichier exécutable à exécuter une fois la restauration terminée

1. Activez le commutateur **Exécuter une commande après la restauration**.
2. Dans le champ **Commande...**, saisissez une commande ou naviguez jusqu'à un fichier de traitement par lots.
3. Dans le champ **Répertoire de travail**, indiquez un chemin vers un répertoire où la commande/le fichier de traitement par lots sera exécuté.
4. Dans le champ **Arguments**, spécifiez les arguments d'exécution de commande si nécessaire.
5. Sélectionnez la case à cocher **Faire échouer la restauration si l'exécution de la commande échoue** si la réussite de l'exécution de la commande est cruciale pour vous. La commande est considérée comme ayant échoué si son code de sortie n'est pas égal à zéro. Si l'exécution de la commande échoue, l'état de la restauration sera défini sur **Erreur**.
   Lorsque la case n'est pas cochée, le résultat d'exécution de commande n'a pas d'incidence sur l'échec ou la réussite de la restauration. Vous pouvez retrouver le résultat de l'exécution de la commande en explorant l'onglet **Activités**.
6. Cliquez sur **Terminé**.

Remarque
Une commande post-restauration ne sera pas exécutée si la restauration exécute un redémarrage.

Modification de SID

Cette option est effective lors de la restauration de Windows 8.1/Windows Server 2012 R2 ou versions précédentes.

Cette option n'est pas effective lorsque la restauration vers une machine virtuelle est exécutée par l'agent pour VMware, l'agent pour Hyper-V, l'agent pour Scale Computing HC3 ou l'agent pour oVirt.

© Acronis International GmbH, 2003-2026

Le préréglage est le suivant : **Désactivé**.

Le logiciel peut générer un identificateur de sécurité unique (SID d'ordinateur) pour le système d'exploitation restauré. Vous avez uniquement besoin de cette option pour assurer le fonctionnement de logiciels tiers qui dépendent du SID d'ordinateur.

Microsoft ne prend pas officiellement en charge la modification de SID sur un système déployé ou restauré. Par conséquent, vous utilisez cette option à vos propres risques.

Gestion de l'alimentation des MV

Ces options sont effectives lorsque la restauration vers une machine virtuelle est exécutée par l'agent pour VMware, l'agent pour Azure, l'agent pour Hyper-V, l'agent pour Virtuozzo, l'agent pour Scale Computing HC3 ou l'agent pour oVirt.

Éteindre les machines virtuelles cibles lors du démarrage de la restauration

Le préréglage est le suivant : **Activé**.

Il n'est pas possible d'effectuer une restauration sur une machine virtuelle existante si la machine est en ligne ; la machine est donc éteinte automatiquement dès que la restauration démarre. Les utilisateurs seront déconnectés de la machine et toutes les données non enregistrées seront perdues.

Décochez la case correspondant à cette option si vous préférez éteindre les machines virtuelles manuellement avant la restauration.

Démarrer la machine virtuelle cible lorsque la restauration est complétée

Le préréglage est le suivant : **Désactivé**.

Après qu'une machine ait été restaurée à partir d'une sauvegarde sur une autre machine, il est possible que la réplique de la machine existante apparaisse sur le réseau. Par prudence, allumez manuellement la machine virtuelle restaurée, après avoir pris les précautions nécessaires.

Journal des événements Windows

Cette option est effective uniquement dans les systèmes d'exploitation Windows.

Cette option définit si les agents doivent consigner des événements des opérations de restauration dans journal des événements d'applications Windows (pour voir ce journal, exécutez eventvwr.exe ou sélectionnez **Panneau de configuration** > **Outils administratifs** > **Affichage des événements**). Vous pouvez filtrer les événements à consigner.

Le préréglage est le suivant : **Désactivé**.

Restauration sûre

Utilisez une restauration complète avec des sauvegardes de type **Machine complète** ou **Disques/volumes** de ressources Windows afin de ne restaurer que des données exemptes de

© Acronis International GmbH, 2003-2026

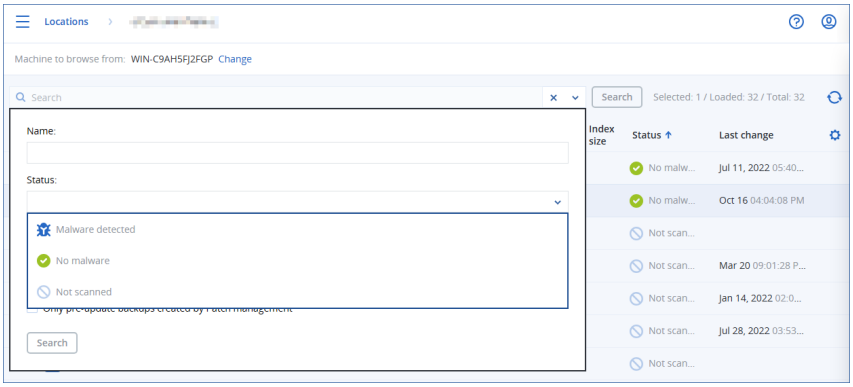
malware, même si la sauvegarde contient des fichiers infectés.

Pendant une opération de restauration sécurisée, la sauvegarde fait l'objet d'une recherche automatique de malware. L'agent de protection restaure ensuite la sauvegarde sur la ressource cible et supprime les fichiers infectés. En conséquence, la sauvegarde restaurée est exempte de malware.

Par ailleurs, l'un des états suivants est attribué à la sauvegarde :

- Malware détecté
- Aucun malware
- Non analysé

Vous pouvez utiliser l'état pour filtrer les archives de sauvegarde.



Limites

- La restauration sécurisée est prise en charge pour les machines physiques et virtuelles Windows sur lesquelles un agent de protection est installé.
- La restauration sécurisée est prise en charge pour les sauvegardes **Machine complète** ou **Disques/volumes**.
- La recherche de malware ne porte que sur les volumes NTFS. Les volumes non-NTFS sont restaurés sans analyse antimalware.
- La restauration sécurisée n'est pas prise en charge pour les sauvegardes de type protection continue des données de l'archive. Pour restaurer les données de la sauvegarde de type protection continue des données, exécutez une autre opération de restauration de **Fichiers/dossiers**. Pour plus d'instructions sur les sauvegardes de type protection continue des données, consultez "Protection continue des données (CDP)" (p. 566).

Opérations avec des sauvegardes

Stockage de sauvegarde

L'onglet **Stockage de sauvegarde** offre un accès à toutes les sauvegardes, y compris celles des ressources hors ligne, des ressources qui ne sont plus enregistrées dans la console Cyber Protect,

© Acronis International GmbH, 2003-2026

ainsi que des sauvegardes vers des clouds publics tels que Microsoft Azure.

Les sauvegardes sont organisées en archives de sauvegarde. Les archives sont nommées selon le modèle suivant :

```
<workload name> - <protection plan name>
```

Les archives suivantes sont orphelines :

- Archives qui ne sont plus associées à un plan de protection ou à un plan de sauvegarde dans le cloud.
- Archives qui ne sont plus associées à une ressource enregistrée.

Remarque
Les sauvegardes orphelines utilisent de l'espace de stockage et sont facturées en conséquence.

Les sauvegardes stockées dans un emplacement partagé (tel qu'un partage SMB ou NFS) sont visibles par tous les utilisateurs qui ont des autorisations de lecture pour cet emplacement. Nous vous recommandons de restreindre les autorisations de lecture pour les emplacements dans lesquels vous stockez des sauvegardes.

Remarque
Nous vous recommandons d'utiliser la réplication de sauvegarde plutôt que de déplacer manuellement les fichiers de sauvegarde.

Avertissement !
N'éditer pas manuellement les fichiers de sauvegarde. Cela pourrait entraîner une corruption des fichiers et rendre les sauvegardes inutilisables. Dans la console Cyber Protect, les sauvegardes corrompues sont marquées comme **Inconnue**, et vous ne pouvez que les supprimer. La restauration de données à partir de celles-ci pourrait ne pas être possible. Pour toute assistance concernant les sauvegardes corrompues, contactez l'équipe de support.

Dans le stockage dans le cloud, l'accès aux sauvegardes dépend du rôle de l'utilisateur :

- Les comptes avec le rôle d'administrateur peuvent accéder à toutes les sauvegardes dans leur tenant ou leur unité.
- Les comptes avec le rôle d'utilisateur ne peuvent accéder qu'à leurs propres sauvegardes.

Les emplacements de sauvegarde utilisés dans les plans de protection sont ajoutés automatiquement à l'onglet **Stockage de sauvegarde**. Les sauvegardes cloud à cloud sont affichées dans **Stockage de sauvegarde** > **Sauvegardes d'applications cloud**.

Un emplacement de sauvegarde (sauf pour le stockage dans le cloud) disparaît de l'onglet **Stockage de sauvegarde** si toutes les ressources qui sont sauvegardées dans cet emplacement sont supprimées de la console Cyber Protect. Si une nouvelle sauvegarde dans cet emplacement se produit, l'emplacement est à nouveau ajouté avec toutes les sauvegardes qui y sont stockées.

© Acronis International GmbH, 2003-2026

Vous pouvez ajouter manuellement un emplacement de sauvegarde. Par exemple, une mémoire USB ou un disque dur externe.

Pour ajouter manuellement un emplacement de sauvegarde

Remarque
Cette opération est disponible uniquement si vous avez un agent en ligne.

1. Connectez-vous à la console Cyber Protect.
2. Accédez à l'onglet **Stockage de sauvegarde**, puis cliquez sur **Ajouter un emplacement**.
3. Sélectionnez le type d'emplacement :
   - Dossier local
   - Dossier réseau
   - Secure Zone
   - Dossier NFS
   - Cloud public
4. Configurez l'emplacement, puis cliquez sur **Terminé**.

Pour actualiser les emplacements de sauvegarde

Si vous avez ajouté ou supprimé des sauvegardes manuellement, vous devez actualiser l'emplacement pour synchroniser la modification avec la console Cyber Protect.

1. Connectez-vous à la console Cyber Protect.
2. Accédez à l'onglet **Stockage de sauvegarde**, puis sélectionnez un emplacement de sauvegarde.
3. [Non applicable aux **sauvegardes d'applications cloud**] Dans **Ordinateur à parcourir depuis**, sélectionnez un ordinateur en ligne.
4. Dans le volet **Actions**, cliquez sur **Actualiser**.

Pour filtrer les archives de sauvegarde

1. Connectez-vous à la console Cyber Protect.
2. Accédez à l'onglet **Stockage de sauvegarde**, puis sélectionnez un emplacement de sauvegarde.
3. Dans la grille principale, cliquez sur l'icône d'engrenage et activez les colonnes que vous souhaitez voir.
4. Pour filtrer les sauvegardes, cliquez sur le nom de la colonne.

Sélectionnez une sauvegarde (point de restauration)

1. Connectez-vous à la console Cyber Protect.
2. Accédez à l'onglet **Stockage de sauvegarde**, puis sélectionnez un emplacement de sauvegarde. Seules les sauvegardes accessibles sont affichées.

© Acronis International GmbH, 2003-2026

3. [Non applicable aux sauvegardes d'applications Cloud] Dans **Ordinateur à parcourir depuis**, sélectionnez un ordinateur en ligne.

   L'accès à certaines sauvegardes nécessite un agent spécifique. Par exemple, pour parcourir les sauvegardes de bases de données SQL, vous devez sélectionner un ordinateur exécutant l'agent pour SQL.

   Important
   La machine avec l'agent de protection (**Machine à partir de laquelle parcourir**) est la destination de restauration par défaut pour les sauvegardes de machines physiques. Si vous souhaitez restaurer une telle sauvegarde sur un autre ordinateur, sélectionnez cet ordinateur dans **Machine à partir de laquelle parcourir**.

4. Sélectionnez l'archive à partir de laquelle vous voulez restaurer les données.
5. Cliquez sur **Afficher les sauvegardes**.
6. Sélectionnez la sauvegarde (point de restauration).

Montage de volumes à partir d'une sauvegarde

Monter des volumes à partir d'une sauvegarde de niveau disque vous permet d'accéder aux volumes comme s'il s'agissait de disques physiques.

Monter des volumes en mode lecture/écriture vous permet de modifier le contenu de la sauvegarde, c'est-à-dire enregistrer, déplacer, créer, supprimer des fichiers ou des dossiers, et lancer des fichiers exécutables consistant d'un seul fichier. Dans ce mode, le logiciel crée une sauvegarde incrémentielle contenant les modifications apportées au contenu de la sauvegarde. Veuillez noter qu'aucune des sauvegardes suivantes ne comprendra ces modifications.

Configuration requise

- Cette fonctionnalité est uniquement disponible sous Windows à l'aide de l'Explorateur de fichiers.
- L'agent pour Windows doit être installé sur la machine qui effectue l'opération de montage.
- Le système de fichiers de la sauvegarde doit être pris en charge par la version de Windows sous laquelle fonctionne la machine.
- La sauvegarde doit être stockée dans un dossier local, sur un partage réseau (SMB/CIFS) ou dans Secure Zone.

Scénarios d'utilisation

- Partage de données

  Les volumes montés peuvent facilement être partagés sur le réseau.
- Solution « sparadrap » de restauration de bases de données

  Montez un volume qui contient une base de données SQL d'une machine récemment tombée en panne. Cela donnera accès à la base de données jusqu'à ce que la machine qui a planté soit

© Acronis International GmbH, 2003-2026

récupérée. Cette approche peut également être utilisée pour la restauration granulaire de données Microsoft SharePoint à l'aide de l'Explorateur SharePoint.

- Nettoyage des virus hors ligne

  Si une machine est infectée, montez sa sauvegarde, nettoyez-la avec un logiciel antivirus (ou retrouvez la dernière sauvegarde qui n'est pas infectée), puis restaurez la machine à partir de cette sauvegarde.
- Vérification des erreurs

  L'échec d'une restauration avec redimensionnement du volume peut provenir d'une erreur dans le système de fichiers de la sauvegarde. Montez la sauvegarde en mode lecture/écriture. Vérifiez ensuite le volume monté en utilisant la commande `chkdsk /r`. Une fois que les erreurs sont corrigées et qu'une nouvelle sauvegarde incrémentielle est créée, restaurez le système à partir de cette sauvegarde.

Pour monter un volume à partir d'une sauvegarde

1. Accédez à l'emplacement de la sauvegarde à l'aide de l'Explorateur de fichiers.
2. Double-cliquez sur le fichier de sauvegarde. Les noms des fichiers reposent sur l'exemple suivant :

   `<machine name> - <protection plan GUID>`
3. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement. Sinon, ignorez cette étape.

   L'Explorateur de fichiers affiche les points de restauration.
4. Double-cliquez sur le point de restauration.

   L'Explorateur de fichiers affiche les volumes sauvegardés.

   Remarque
   Double-cliquez sur un volume pour parcourir son contenu. Vous pouvez copier des fichiers et des dossiers à partir de la sauvegarde vers n'importe quel dossier du système de fichiers.
5. Effectuez un clic droit sur un volume pour le monter, puis cliquez sur une des options suivantes :
   a. **Monter**

      Remarque
      Seule la dernière sauvegarde de l'archive (chaîne de sauvegarde) peut être montée en mode lecture/écriture.

   b. **Monter en mode lecture seule**.
6. Si la sauvegarde est stockée sur un partage réseau, fournissez les informations d'identification. Sinon, ignorez cette étape.

   Le logiciel monte le volume sélectionné. La première lettre non utilisée est attribuée au volume.

Démontage d'un volume

1. Accédez à **Ordinateur** (**Ce PC** sous Windows 8.1 et versions ultérieures) à l'aide de l'Explorateur de fichiers.

© Acronis International GmbH, 2003-2026

2. Effectuez un clic droit sur le volume monté.
3. Cliquez sur **Démonter**.
4. [Facultatif] Si le volume était monté en mode lecture/écriture et que son contenu a été modifié, indiquez si vous souhaitez créer une sauvegarde incrémentielle avec les modifications. Sinon, ignorez cette étape.

Le logiciel démonte le volume sélectionné.

Validation des sauvegardes

Vous pouvez valider une sauvegarde pour vérifier que vous pouvez restaurer les données. Pour en savoir plus sur cette opération, reportez-vous à "Validation" (p. 259).

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

Pour valider une sauvegarde

1. Sélectionnez la ressource sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
   Si la ressource est hors ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner la machine**, sélectionnez une ressource cible qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde. Pour en savoir plus sur ce type de sauvegarde, reportez-vous à "Stockage de sauvegarde" (p. 731).
4. Cliquez sur l'icône en forme d'engrenage, puis sur **Terminé**.
5. Sélectionnez l'agent qui exécutera la validation.
6. Sélectionnez la méthode de validation.
7. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement.
8. Cliquez sur **Démarrer**.

Exportation de sauvegardes

L'opération d'exportation crée une copie auto-suffisante d'une sauvegarde à l'emplacement spécifié par vos soins. La sauvegarde originale demeure intacte. L'exportation de sauvegardes vous permet de séparer une sauvegarde spécifique d'une chaîne de sauvegardes incrémentielles et différentielles pour une restauration rapide, une écriture sur support amovible ou détachable, ou pour d'autres raisons.

© Acronis International GmbH, 2003-2026

Remarque
Cette fonctionnalité est disponible dans les tenants clients pour lesquels le quota **Serveurs** est activé dans le cadre de la fonctionnalité de Protection Standard.

Le résultat d'une opération d'exportation est toujours une sauvegarde complète. If vous souhaitez répliquer toute la chaîne de sauvegarde vers un autre emplacement et préserver de multiples points de restauration, utilisez un plan de réplication de sauvegarde. Pour en savoir plus sur ce plan, reportez-vous à "Réplication de sauvegarde" (p. 255).

Le nom du fichier de sauvegarde de la sauvegarde exportée est identique à celui de la sauvegarde d'origine, à l'exception du numéro séquentiel. Si de multiples sauvegardes issues de la même chaîne de sauvegarde sont exportées vers le même emplacement, un numéro de séquence à quatre chiffres est attaché aux noms de fichier de toutes les sauvegardes, sauf au premier.

La sauvegarde exportée hérite des paramètres de chiffrement et du mot de passe de la sauvegarde originale. Vous devez indiquer le mot de passe lorsque vous exportez une sauvegarde chiffrée.

Pour exporter une sauvegarde

1. Sélectionnez la ressource sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
   Si la ressource est hors ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner la machine**, sélectionnez une ressource cible qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde. Pour en savoir plus sur ce type de sauvegarde, reportez-vous à "Stockage de sauvegarde" (p. 731).
4. Cliquez sur l'icône en forme d'engrenage, puis sur **Exporter**.
5. Sélectionnez l'agent qui exécutera l'exportation.
6. Si la sauvegarde est chiffrée, saisissez le mot de passe de chiffrement. Sinon, ignorez cette étape.
7. Spécifiez la destination de l'exportation.
8. Cliquez sur **Démarrer**.

Suppression de sauvegardes

Une archive de sauvegarde contient une ou plusieurs sauvegardes. Vous pouvez supprimer des sauvegardes spécifiques (points de restauration) dans une archive ou toute l'archive.

© Acronis International GmbH, 2003-2026

La suppression de l'archive de sauvegarde supprime toutes les sauvegardes qu'elle contient. La suppression de toutes les sauvegardes d'une ressource supprime les archives de sauvegarde qui contiennent ces sauvegardes.

Remarque
La protection continue des données empêche la suppression des archives de sauvegarde. Si vous souhaitez supprimer manuellement une sauvegarde créée avec la protection continue des données (CDP) activée, vous devez révoquer ou supprimer le plan de protection correspondant.

Vous pouvez supprimer des sauvegardes en utilisant la console Cyber Protect, dans les onglets **Terminaux** et **Stock. de sauvegarde**. Vous pouvez également supprimer des sauvegardes du stockage dans le cloud à l'aide de la console Web Restore.

Avertissement !
Si le stockage immuable est désactivé, les données sauvegardées sont définitivement supprimées et ne peuvent pas être récupérées.

Pour supprimer des sauvegardes ou des archives de sauvegarde

Dans l'onglet Terminaux

Cette procédure ne s'applique qu'aux ressources en ligne.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les sauvegardes de ressources que vous souhaitez supprimer.
3. Cliquez sur **Restauration**.
4. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde.
5. [Pour supprimer toutes les sauvegardes de ressources] Cliquez sur **Supprimer tout**.
   La suppression de toutes les sauvegardes supprime également les archives de sauvegarde qui contiennent ces sauvegardes.
6. [Pour supprimer une sauvegarde spécifique] Sélectionnez la sauvegarde (point de restauration) que vous souhaitez supprimer, puis cliquez sur **Actions** > **Supprimer**.
7. [Lors de la suppression de toutes les sauvegardes] Cochez la case, puis cliquez sur **Supprimer** pour confirmer votre décision.
8. [Lors de la suppression d'une sauvegarde spécifique] Cliquez sur **Supprimer** pour confirmer votre décision.

Dans l'onglet Stockage de sauvegarde

Cette procédure s'applique aux ressources en ligne et hors ligne.

1. Sur la console Cyber Protect, accédez à **Stock. de sauvegarde**.
2. Sélectionnez l'emplacement à partir duquel vous souhaitez supprimer les sauvegardes.

© Acronis International GmbH, 2003-2026

3. Sélectionnez l'archive de sauvegarde à partir de laquelle vous souhaitez supprimer les sauvegardes.
   Le nom de l'archive utilise le modèle suivant :
   - Archives de sauvegarde non-cloud à cloud : <workload name> - <protection plan name>
   - Archives de sauvegarde cloud à cloud : <user name> ou <drive name> ou <team name> - <cloud service> - <protection plan name>
4. [Pour supprimer l'ensemble de l'archive de sauvegardes] Cliquez sur **Supprimer**.
   La suppression d'une archive de sauvegardes supprime toutes les sauvegardes de cette archive.
5. [Pour supprimer une sauvegarde spécifique dans l'archive de sauvegardes] Cliquez sur **Afficher les sauvegardes**.
   a. Sélectionnez la sauvegarde (point de restauration) que vous souhaitez supprimer.
   b. Cliquez sur **Actions** > **Supprimer**.
6. [Lors de la suppression d'une archive de sauvegardes] Cochez la case, puis cliquez sur **Supprimer** pour confirmer votre décision.
7. [Lors de la suppression d'une sauvegarde spécifique] Cliquez sur **Supprimer** pour confirmer votre décision.

Dans la console Web Restore

Cette procédure s'applique uniquement aux archives de sauvegardes dans le stockage dans le cloud.

1. Dans la console Cyber Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les sauvegardes de ressource que vous souhaitez supprimer, puis cliquez sur **Restauration**.
3. [Si plusieurs emplacements de sauvegarde sont disponibles] Sélectionnez l'emplacement de sauvegarde, puis cliquez sur **Autres méthodes de restauration**.
4. Cliquez sur **Télécharger les fichiers**.
   Vous êtes redirigé vers la console Web Restore.
5. Dans la console Web Restore, sous **Machines**, cliquez sur le nom de la ressource.
6. Sous **Dernière version**, cliquez sur la date, puis sur **Supprimer**.
   Cette action n'est disponible qu'au niveau de l'archive de sauvegardes. Vous ne pouvez pas explorer l'archive et supprimer des sauvegardes spécifiques.
7. Cliquez sur **Supprimer** pour confirmer votre décision.

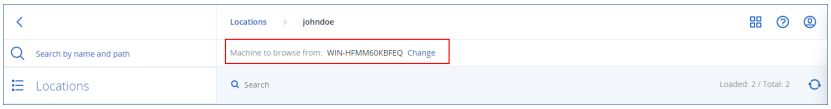
Suppression des sauvegardes en dehors de la console Cyber Protect

Nous vous recommandons de supprimer les sauvegardes à l'aide de la console Cyber Protect. Si vous supprimez des sauvegardes du stockage dans le cloud à l'aide de la console Web Restore ou si vous supprimez des sauvegardes locales à l'aide d'un gestionnaire de fichiers, vous devez actualiser l'emplacement de la sauvegarde pour synchroniser les modifications avec la console Cyber Protect.

Prérequis

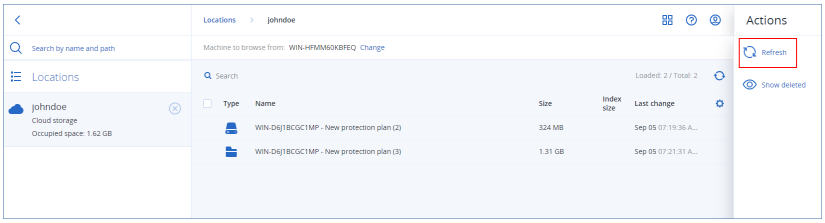
© Acronis International GmbH, 2003-2026

- Un agent en ligne qui peut accéder à l'emplacement de la sauvegarde doit être sélectionné comme **Machine à parcourir** dans la console Cyber Protect.



Pour actualiser un emplacement de sauvegarde

1. Sur la console Cyber Protect, accédez à **Stock. de sauvegarde**.
2. Sélectionnez l'emplacement de sauvegarde dans lequel les sauvegardes supprimées ont été stockées.
3. Dans le volet **Actions**, cliquez sur **Actualiser**.



Compréhension de la détection des goulots d'étranglement

La fonctionnalité de détection de goulots d'étranglement vous permet d'identifier l'endroit où vous pouvez améliorer les performances, car elle met en évidence le composant de votre système qui a été le plus lent pendant une sauvegarde ou une restauration.

Étant donné que les goulots d'étranglement se produisent *toujours* pendant un événement de transmission, ils ne doivent pas nécessairement être résolus. Vos sauvegardes sont peut-être déjà suffisamment rapides, s'intègrent déjà parfaitement dans vos créneaux de sauvegarde et sont conformes à vos accords de niveau de service (SLA) : il n'y a donc généralement pas de problème particulier à résoudre.

Vous pouvez afficher et suivre facilement les goulots d'étranglement dans l'onglet **Détails de l'activité**. Pour ce faire, accédez depuis la console Cyber Protect à **Surveillance > Activités**, puis cliquez sur l'activité pertinente. Pour plus d'informations sur l'affichage des goulots d'étranglement, voir "Affichage des détails d'un goulot d'étranglement" (p. 742) et "Sur quels agents, ressources et emplacements de sauvegarde les goulots d'étranglement sont-ils affichés ?" (p. 744).

Qu'est-ce qu'un goulot d'étranglement ?

Les goulots d'étranglement sont généralement provoqués par la lenteur d'un composant de la chaîne de traitement, ce qui implique que d'autres composants attendent ce composant.

La fonctionnalité de détection des goulots d'étranglement vous permet de suivre des composants présentant des lenteurs pendant la sauvegarde et la restauration, et d'identifier parmi les types de composants suivants ceux qui sont les plus lents :

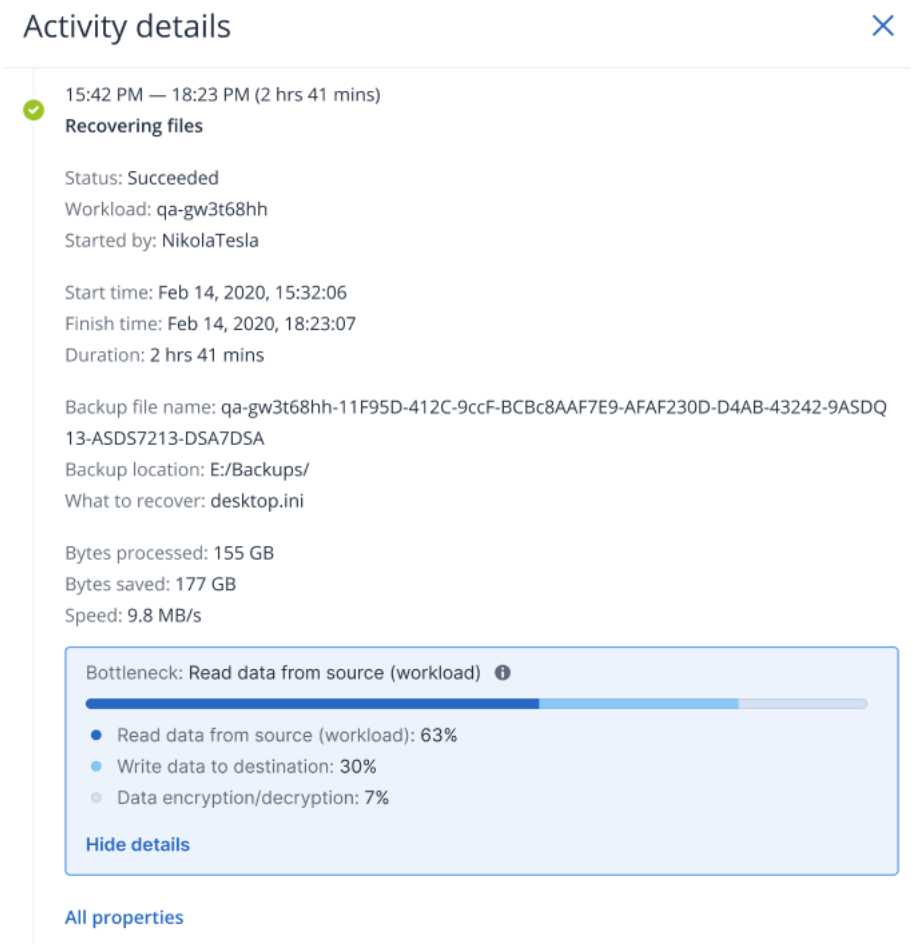
- **Source** : En un coup d'œil, vous pouvez déterminer si la vitesse de lecture à partir de la source de sauvegarde/restauration provoque un goulot d'étranglement.

© Acronis International GmbH, 2003-2026

- **Destination** : Compréhension des incidences sur les performances de la vitesse d'écriture sur la destination de sauvegarde/restauration.
- **Agent** : Examen de la vitesse de traitement des données par l'agent et détermination si elle est suffisante.

Le type de goulot d'étranglement, qu'il provienne de la source, de la destination ou de l'agent, peut évoluer selon les heures pendant la sauvegarde/restauration. Les pourcentages indiqués dans la section **Goulot d'étranglement** de l'onglet **Détails de l'activité** ci-dessous (par exemple, **Lire les données à partir de la source (ressource) : 63 %**) représentent le pourcentage de durée en cas de détection de ce type de goulot d'étranglement. Dans ce cas, pendant 63 % du temps d'activité de la restauration, le type de goulot d'étranglement concernait la lenteur de lecture des données depuis l'archive de sauvegarde par l'agent.

De la même manière, pendant 30 % du temps, le goulot d'étranglement était lié à la lenteur d'écriture des données dans la destination de la restauration (**Écrire les données sur la destination : 30 %**).



Remarque
Les statistiques sur le goulot d'étranglement sont disponibles dans l'onglet **Détails de l'activité**. Ces statistiques sont disponibles uniquement pour les tâches de plus d'une minute.

© Acronis International GmbH, 2003-2026

Comment réduire les goulots d'étranglement ?

Comme indiqué ci-dessus, la fonctionnalité de détection des goulots d'étranglement met en évidence le flux de données *en lecture* et *en écriture* entre les composants de sauvegarde. Les statistiques de *lecture* font référence au flux de données depuis la source de données vers l'agent qui effectue la sauvegarde/restauration. Quant aux statistiques d'*écriture*, elles font référence au flux de données entre l'agent et l'archive de sauvegarde (la destination).

Pour réduire les goulots d'étranglement et améliorer les performances des flux de données en lecture/écriture, vous devez analyser le canal entre l'agent et la source de données/l'archive de sauvegarde. Par exemple, vous pouvez essayer de réaliser un banc d'essai de vos disques durs si l'agent sauvegarde des fichiers locaux.

Affichage des détails d'un goulot d'étranglement

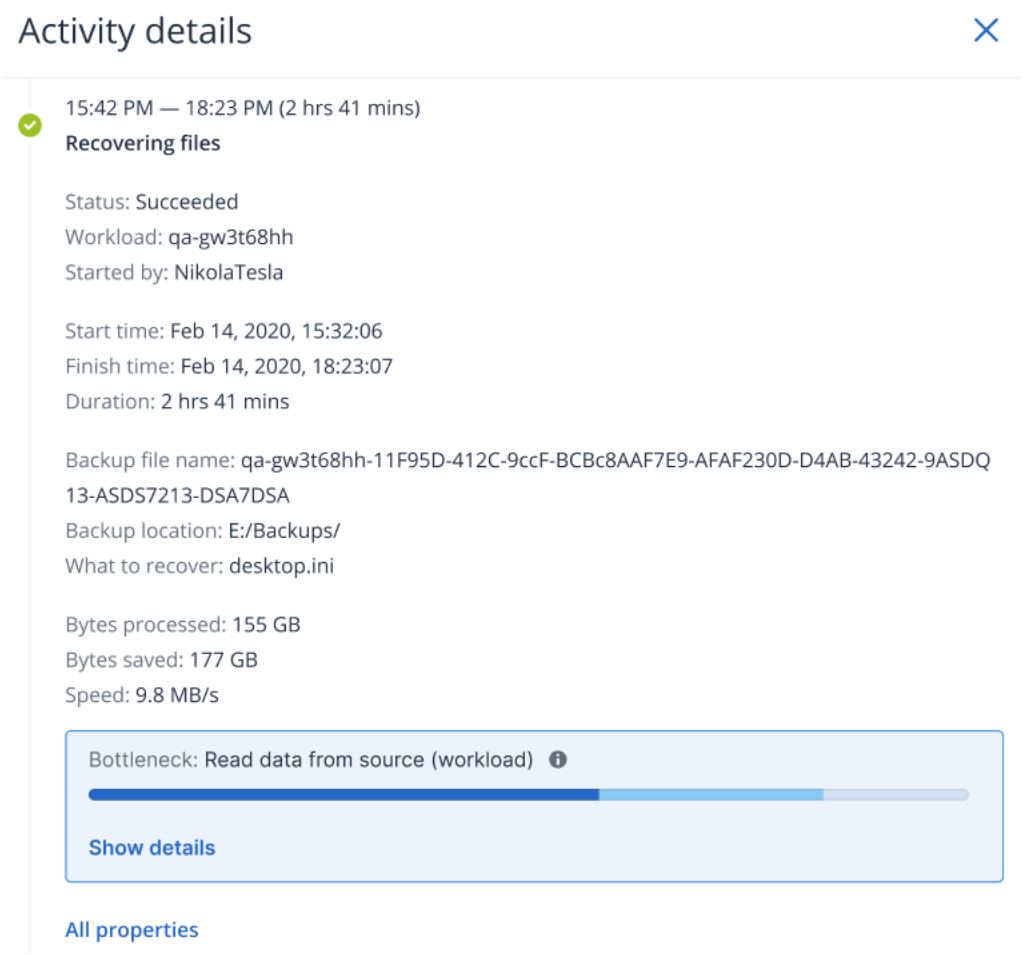
Vous pouvez visualiser les goulots d'étranglement détectés pour tout type de sauvegarde, réplication de sauvegarde ou restauration (vers un autre type de dossier ou d'emplacement de destination), y compris les sauvegardes de machine virtuelle, d'ordinateur et de fichiers/dossiers. Vous pouvez également afficher les goulots d'étranglement des réplications et restaurations automatiques de machines virtuelles.

Pour plus d'informations sur la définition et les concepts essentiels des types de goulots d'étranglement, voir "Compréhension de la détection des goulots d'étranglement" (p. 740).

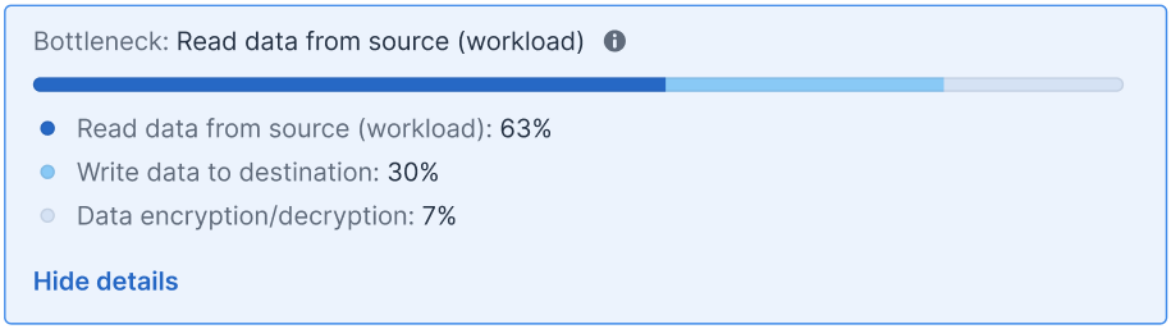
Pour afficher les détails d'un goulot d'étranglement

1. Dans la console Cyber Protect, accédez à **Surveillance > Activités**.
2. Cliquez sur l'activité pertinente.
   Dans l'onglet **Détails de l'activité**, la section **Goulot d'étranglement** apparaît en bleu.

© Acronis International GmbH, 2003-2026



3. Cliquez sur **Afficher les détails** pour afficher le goulot d'étranglement rencontré le plus fréquemment pendant la sauvegarde/restauration.
   La section **Goulot d'étranglement** se développe pour afficher la synthèse des types de goulot d'étranglement pertinents.



   Dans l'exemple ci-dessus, le goulot d'étranglement qui représentait 63 % de la durée totale de l'opération a été provoqué par l'opération de *lecture* (effectuée par l'agent).

Remarque
Les valeurs de goulot d'étranglement se mettent à jour dynamiquement toutes les minutes pendant l'exécution de l'activité correspondante.

© Acronis International GmbH, 2003-2026

Sur quels agents, ressources et emplacements de sauvegarde les goulots d'étranglement sont-ils affichés ?

La détection des goulots d'étranglement est disponible pour les types suivants de ressources, agents et emplacements de sauvegarde :

- Sauvegardes de disque/d'image effectuées par :
  - Agent pour Azure
  - Agent pour Windows
  - Agent pour Linux
  - Agent pour Mac
  - Agent pour VMware (appliance virtuelle et Windows, y compris la réplication et la restauration automatique de VM à partir d'un réplica (activités de restauration à partir de réplicas))
  - Agent pour Hyper-V
  - Agent pour Scale Computing HC3
  - Agent pour oVirt (KVM)
  - Plate-forme d'infrastructure de l'agent pour Virtuozzo
  - Agent pour Virtuozzo
  - Agent pour VMware Cloud Director (vCD-BA)
- Sauvegardes de niveau fichier
  - Agent pour Windows
  - Agent pour Linux
  - Agent pour Mac
- Sauvegardes de niveau application
  - Agent pour SQL
  - Agent pour Exchange
  - Agent pour MySQL/MariaDB
  - Agent pour Oracle
  - Agent pour SAP HANA
- Emplacements de sauvegardes
  - Stockage Acronis Cloud (y compris le stockage hébergé par un partenaire)
  - Stockage dans le cloud public
  - Partages réseau (SMB + NFS)
  - Dossiers locaux
  - Emplacements définis par script
  - Acronis Secure Zone

© Acronis International GmbH, 2003-2026

Sauvegarde de ressources dans des clouds publics

Remarque
Cette fonctionnalité nécessite que la fonctionnalité **Direct Backup to Public Cloud** soit activée pour votre tenant. Notez que lorsque vous ajoutez cette fonctionnalité à un plan de protection, vous pouvez être soumis à des frais supplémentaires.

Important
La sauvegarde de ressources vers l'un des services cloud publics pris en charge est possible uniquement pour les agents de protection s'exécutant sur Windows 7 ou une version ultérieure, et Windows Server 2008 R2 SP1 ou une version ultérieure. Par ailleurs, les agents exécutant des plans de protection des données hors hôte tout en s'exécutant sur un système d'exploitation obsolète (tel que Windows Vista, ou Windows Server 2008 ou une version antérieure) ne peuvent pas fonctionner avec des emplacements dans des clouds publics.

Vous pouvez sélectionner des services de cloud public, tels que Microsoft Azure, Amazon S3 (Simple Storage Service) et un stockage cloud public compatible S3, comme destinations de sauvegarde dans la console Cyber Protect.

Remarque
Le stockage dans le cloud public n'est pas pris en charge comme destination pour les sauvegardes Microsoft 365 et Google Workspace.

Pour configurer des emplacements de sauvegarde dans les clouds publics, vous devez être administrateur d'entreprise ou d'unité, ou disposer de l'un des rôles suivants définis dans le service de cyberprotection : cyberadministrateur, administrateur ou utilisateur.

Définition d'un emplacement de sauvegarde dans Microsoft Azure

Remarque
Pour configurer les emplacements de sauvegarde dans Microsoft Azure, vous devez avoir l'un des rôles suivants définis dans le service de cyberprotection : administrateur d'entreprise, utilisateur, cyberadministrateur.

Vous pouvez définir des emplacements de sauvegarde dans le service Microsoft Azure Blob Storage, dans l'un des types de compte de stockage Microsoft Azure suivants :

- Usage général standard v2 (StorageV2)
- Blobs de bloc Premium

Pour en savoir plus sur les types de compte de stockage Microsoft Azure, consultez la documentation Microsoft.

© Acronis International GmbH, 2003-2026

Pour sauvegarder une ressource dans Microsoft Azure, vous devez définir l'emplacement de sauvegarde Microsoft Azure dans la console Cyber Protect, puis vous connecter à l'abonnement Microsoft Azure pertinent. Cette opération peut être effectuée selon les méthodes suivantes :

- Lors de la création ou de la modification d'un plan de protection.
- Lors de la définition et de la gestion d'emplacements de stockage des sauvegardes.

Important
Les administrateurs et les utilisateurs non-administrateurs peuvent sauvegarder les ressources dans Microsoft Azure.

Les utilisateurs non-administrateurs peuvent ajouter l'accès à un abonnement Microsoft Azure (voir "Gestion de l'accès aux abonnements Microsoft Azure" (p. 761)), mais peuvent appliquer des plans de protection uniquement lorsque l'emplacement de sauvegarde est connecté à l'abonnement Microsoft Azure qu'ils ont eux-mêmes ajouté et pour la ressource enregistrée dans la console Cyber Protect sous leur nom.

Les administrateurs peuvent appliquer des plans de protection lorsque l'emplacement de sauvegarde est connecté aux abonnements Microsoft Azure qu'ils ont eux-mêmes ajoutés ou aux abonnements ajoutés par un autre administrateur, et pour les ressources enregistrées dans la console Cyber Protect sous le nom d'un utilisateur.

Pour définir un emplacement de sauvegarde dans Microsoft Azure

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Si vous créez ou modifiez un plan de protection, accédez à **Terminaux** et sélectionnez la ressource que vous souhaitez sauvegarder dans Microsoft Azure. Dans la section **Sauvegarde** du plan de protection de la ressource sélectionnée, cliquez sur le lien dans la ligne **Où sauvegarder**.
     Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 243).
   - S vous gérez vos emplacements de stockage des sauvegardes et souhaitez ajouter Microsoft Azure en tant que nouvel emplacement, accédez à **Stockage de sauvegarde**.
     Pour plus d'informations sur la gestion de vos emplacements de stockage des sauvegardes, reportez-vous à "Stockage de sauvegarde" (p. 731).
2. Cliquez sur **Ajouter un emplacement**.
3. Dans la liste déroulante **Clouds publics**, sélectionnez **Microsoft Azure**.
4. Si l'abonnement Microsoft Azure pertinent est déjà enregistré dans la console Cyber Protect, sélectionnez-le dans la liste des abonnements.
   Si l'abonnement pertinent n'est pas enregistré dans la console Cyber Protect, cliquez sur **Ajouter** cliquez sur **Connexion** dans la boîte de dialogue qui s'affiche. Vous êtes redirigé vers la page de connexion Microsoft. Pour plus d'informations sur l'ajout et la définition de l'accès à un abonnement Microsoft Azure, voir "Ajout de l'accès à un abonnement Microsoft Azure" (p. 762).

© Acronis International GmbH, 2003-2026

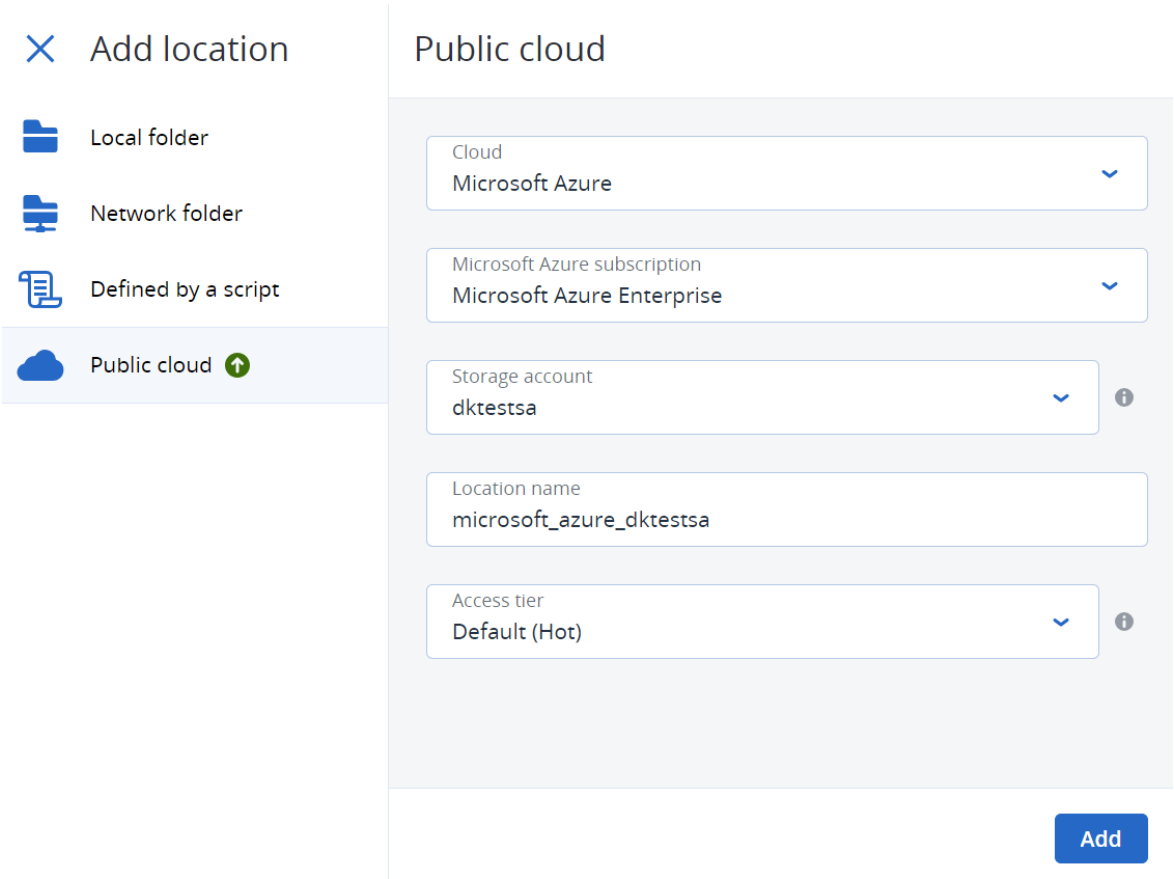
5. Dans le champ **Compte de stockage**, sélectionnez le compte souhaité.

Remarque
Seuls les comptes de stockage Microsoft Azure avec suffixes de terminaux classiques contenant `core.windows.net` sont pris en charge actuellement.

Par défaut, les champs **Nom de l'emplacement** et **Niveau d'accès** sont renseignés automatiquement en fonction du compte de stockage sélectionné. Le nom de l'emplacement affiché est `microsoft_azure_[storage account]` et le niveau d'accès sélectionné est **Par défaut (chaud)**. Les deux champs peuvent être modifiés si nécessaire.

Remarque
Seuls les niveaux d'accès chaud et froid sont pris en charge actuellement (pour plus d'informations sur les niveaux d'accès, voir la documentation Microsoft).

Remarque
Lorsque vous changez le nom de l'emplacement, saisissez un nom d'emplacement unique (ce nom doit être unique pour le tenant client). Si le nom que vous ajoutez existe déjà dans le compte de stockage, Acronis lui ajoute un numéro en suffixe. Par exemple, si le nom **Stockage Microsoft Azure** existe déjà, le nom est automatiquement mis à jour en **Stockage Microsoft Azure_01**.



6. Cliquez sur **Ajouter**.

© Acronis International GmbH, 2003-2026

Si vous créez ou modifiez un plan de protection, l'emplacement de sauvegarde Microsoft Azure est défini comme étant l'emplacement sur la ligne **Où sauvegarder**. Lors de l'exécution de la sauvegarde (manuelle ou en fonction d'une planification), la sauvegarde est enregistrée dans l'emplacement défini.

Si vous gérez vos emplacements de stockage de sauvegarde, vous pouvez afficher et mettre à jour les détails de l'emplacement si nécessaire. L'emplacement Microsoft Azure est également disponible lors de la définition d'un emplacement de sauvegarde pour les ressources. Pour plus d'informations, voir "Affichage et mise à jour des emplacements de sauvegarde dans le cloud public" (p. 756).

Définir un emplacement de sauvegarde dans Amazon S3

Remarque
Pour configurer les emplacements de sauvegarde dans Amazon S3, vous devez avoir l'un des rôles suivants définis dans le service de cyberprotection : administrateur d'entreprise, utilisateur, cyberadministrateur.

Pour sauvegarder une ressource dans Amazon S3, vous devez définir l'emplacement de sauvegarde Amazon S3 dans la console Cyber Protect, puis vous connecter à la connexion Amazon S3 correspondante. Vous pouvez procéder de la manière suivante :

- Lors de la création ou de la modification d'un plan de protection.
- Lors de la définition et de la gestion d'emplacements de stockage des sauvegardes.

Important
Les administrateurs et les utilisateurs non-administrateurs peuvent sauvegarder des ressources dans Amazon S3.

Les utilisateurs non-administrateurs peuvent ajouter un accès à une connexion Amazon S3 (voir "Gestion de l'accès à d'autres services de stockage dans le cloud public" (p. 765)), mais ils ne peuvent appliquer des plans de protection que lorsque l'emplacement de sauvegarde est connecté à la connexion Amazon S3 qu'ils ont eux-mêmes ajoutée, et pour les ressources enregistrées dans la console Cyber Protect sous leur nom.

Les administrateurs peuvent appliquer des plans de protection lorsque l'emplacement de sauvegarde est connecté aux connexions Amazon S3 qu'ils ont eux-mêmes ajoutées ou aux abonnements ajoutés par tout autre administrateur, et pour les ressources enregistrées dans la console Cyber Protect sous n'importe quel utilisateur.

Pour définir un emplacement de sauvegarde dans Amazon S3

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Si vous créez ou modifiez un plan de protection, accédez à **Terminaux** et sélectionnez la ressource que vous souhaitez sauvegarder dans Amazon S3. Dans la section **Sauvegarde** du

© Acronis International GmbH, 2003-2026

plan de protection de la ressource sélectionnée, cliquez sur le lien dans la ligne **Où sauvegarder**.

Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 243).

- Si vous gérez vos emplacements de stockage des sauvegardes et souhaitez ajouter Amazon S3 en tant que nouvel emplacement, accédez à **Stock. de sauvegarde**.

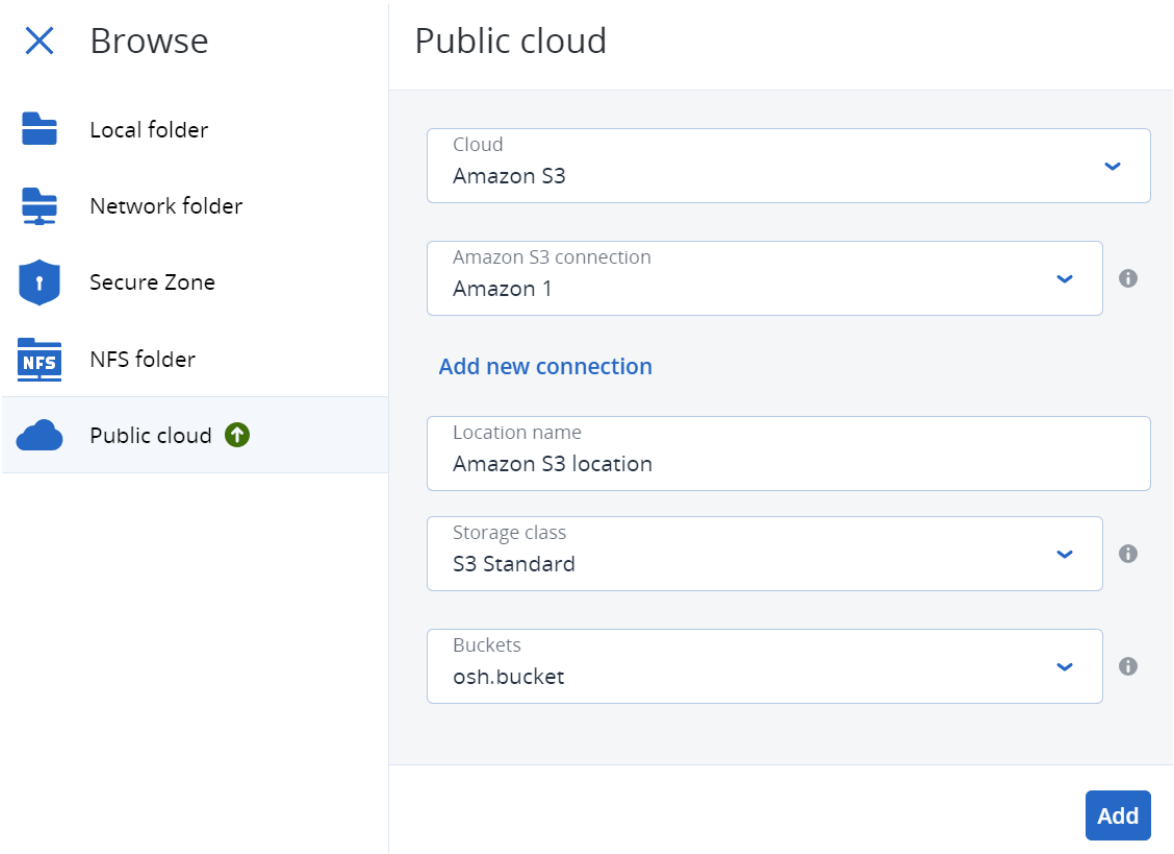
  Pour plus d'informations sur la gestion de vos emplacements de stockage des sauvegardes, reportez-vous à "Stockage de sauvegarde" (p. 731).

2. Cliquez sur **Ajouter un emplacement**.
3. Dans la liste déroulante **Clouds publics**, sélectionnez **Amazon S3**.

Remarque
Les compartiments dans des régions spéciales du Government Cloud (par exemple, `us-gov-west-1`) ne sont pas pris en charge comme emplacements de sauvegarde.

4. Si la connexion Amazon S3 concernée est déjà enregistrée dans la console Cyber Protect, sélectionnez-la dans la liste.

   Si la connexion concernée n'est pas enregistrée dans la console Cyber Protect, cliquez sur **Ajouter une nouvelle connexion**. Pour plus d'informations sur l'ajout et la définition de l'accès à une connexion Amazon S3, voir "Ajout d'un accès à une connexion au cloud public" (p. 766).
   Lorsque la connexion est ajoutée, passez à l'étape suivante.



5. Définissez ce qui suit :

© Acronis International GmbH, 2003-2026

- Dans le champ **Nom de l'emplacement**, saisissez le nom de l'emplacement de sauvegarde.

  Remarque
  Le nom de l'emplacement doit être unique pour le tenant client. Si le nom que vous ajoutez existe déjà dans la connexion, Acronis ajoute un numéro de suffixe au nom. Par exemple, si **Stockage Amazon S3** existe déjà, le nom sera automatiquement mis à jour en **Stockage Amazon S3 1**.

- Dans le champ **Classe de stockage**, sélectionnez l'une des classes de stockage prises en charge suivantes :
  - S3 Standard
  - Standard - Accès peu fréquent (S3 Standard-IA)
  - Une zone - Accès peu fréquent (S3 Une zone-IA)
  - S3 Hiérarchisation intelligente

  Remarque
  Lorsque vous utilisez la classe de stockage S3 Intelligent-Tiering, les anciens objets de sauvegarde peuvent être déplacés automatiquement vers les niveaux d'accès Archive ou Archive approfondie (pour plus d'informations sur ces niveaux, consultez la documentation Amazon S3). Les objets de ces niveaux ne sont pas accessibles instantanément et nécessitent une « réhydratation ». Cela signifie que, si vous essayez d'effectuer une restauration à partir de ces anciennes sauvegardes, cette restauration échoue. Pour effectuer une restauration à partir de ces sauvegardes, récupérez d'abord les anciens objets des niveaux d'accessibilité pertinents. Pour plus d'informations sur la récupération de données à partir de niveaux d'accessibilité, consultez la documentation Amazon S3.

- Dans le champ **Compartiment**, sélectionnez le compartiment Amazon S3 approprié.
  Si le compartiment sélectionné est activé avec les fonctionnalités Verrouillage d'objet et Gestion des versions (qui sont activées dans la console de gestion AWS), la case **Période d'immuabilité de la sauvegarde (jours)** est cochée. Vous pouvez ensuite définir le nombre de jours de la période d'immuabilité, qui garantit que les données sauvegardées ne sont pas supprimées pendant cette période, et qui est appliquée à tous les objets de sauvegarde créés par Acronis.
  Notez que lorsque vous définissez la période d'immuabilité comme propriété de l'emplacement de sauvegarde, la période de rétention par défaut définie pour le compartiment est ignorée. Pour plus d'informations sur la fonctionnalité Verrouillage d'objet et les périodes de rétention, consultez la documentation Amazon S3.

© Acronis International GmbH, 2003-2026

Remarque
Il est recommandé de configurer la stratégie de cycle de vie pour le compartiment si vous avez défini l'option d'immuabilité lors de la création de l'emplacement de sauvegarde. Les compartiments avec les fonctionnalités de versionnement d'objet et de verrouillage d'objet activées stockeront les versions d'objet indéfiniment, ce qui entraînera une consommation de stockage croissante indéfiniment, à moins qu'une stratégie de cycle de vie ne soit configurée.

Cependant, l'activation des fonctionnalités de versionnement d'objet et de verrouillage d'objet n'est pas recommandée pour les compartiments utilisés par les emplacements de sauvegarde et qui sont configurés sans l'option d'immuabilité. Si des stratégies de cycle de vie sont appliquées à ces compartiments, elles peuvent supprimer accidentellement des objets liés à la chaîne d'archives de sauvegarde, ce qui entraîne une corruption de l'archive.

Avec l'option d'immuabilité configurée, le problème est résolu en ajustant la période d'immuabilité pour les anciens objets, dont les nouveaux objets de sauvegarde ont encore des dépendances. Cela se produit automatiquement avec chaque sauvegarde planifiée, où la période d'immuabilité de chaque objet appartenant à la chaîne de sauvegarde est prolongée par l'agent de sauvegarde communiquant avec le stockage dans le cloud. Cette période d'immuabilité n'est jamais inférieure à la valeur de jours de période d'immuabilité définie lors de la création de l'emplacement de sauvegarde. Pour plus d'informations sur la façon de configurer la stratégie de cycle de vie, reportez-vous à la documentation Amazon S3.

Remarque
Les agents antérieurs à la version 24.05 peuvent effectuer des sauvegardes vers Amazon S3, mais seuls les agents de la version 24.05 ou ultérieure appliqueront le verrouillage d'objet aux objets créés dans le stockage Amazon S3. En d'autres termes, seuls les agents récents peuvent reconnaître la période d'immuabilité définie en tant que propriété de l'emplacement de sauvegarde, et gérer cette période pour toutes les sauvegardes créées. Les agents antérieurs à la version 24.05 ignoreront ce paramètre et les propriétés de verrouillage d'objet par défaut (définies dans la console de gestion AWS ou via l'API) seront appliquées aux objets créés dans Amazon S3.

6. Cliquez sur **Ajouter**.

   Si vous créez ou modifiez un plan de protection, l'emplacement de sauvegarde Amazon S3 est défini comme emplacement dans la ligne **Où sauvegarder**. Lorsque la sauvegarde est exécutée (manuellement ou automatiquement par planification), elle est enregistrée dans l'emplacement défini.

   Si vous gérez vos emplacements de stockage de sauvegarde, vous pouvez afficher et mettre à jour les détails de l'emplacement si nécessaire. L'emplacement Amazon S3 est également disponible lors de la définition d'un emplacement de sauvegarde pour les ressources. Pour plus d'informations, voir "Affichage et mise à jour des emplacements de sauvegarde dans le cloud public" (p. 756).

© Acronis International GmbH, 2003-2026

Définir un emplacement de sauvegarde dans IONOS Cloud, Impossible Cloud ou un stockage compatible S3

Remarque

- Pour configurer des emplacements de sauvegarde dans IONOS Cloud, Impossible Cloud ou un stockage compatible S3, vous devez disposer de l'un des rôles suivants définis dans le service Cyber Protect : administrateur de l'entreprise, utilisateur ou administrateur Cyber.
- Les compartiments dans des régions spéciales GovCloud (par exemple, `https://aws.amazon.com/govcloud-us/`, `https://learn.microsoft.com/en-us/azure/azure-government/regions`, ou d'autres URL de terminal provenant de fournisseurs de stockage soutenant le concept GovCloud) ne sont pas pris en charge comme emplacements de sauvegarde.

Pour sauvegarder une ressource vers IONOS Cloud, Impossible Cloud, ou un stockage compatible S3, vous devez définir l'emplacement de sauvegarde dans la console Cyber Protect. Vous pouvez le faire de la manière suivante :

- Lors de la création ou de la modification d'un plan de protection.
- Lors de la définition et de la gestion d'emplacements de stockage des sauvegardes.

Important

Tant les administrateurs que les utilisateurs non-administrateurs peuvent sauvegarder des ressources vers IONOS Cloud, Impossible Cloud, ou un stockage compatible S3.

Les utilisateurs non-administrateurs peuvent également appliquer des plans de protection qui utilisent les emplacements de sauvegarde sur Impossible Cloud, IONOS Cloud, ou le stockage compatible S3 créés par eux-mêmes, et pour les ressources enregistrées dans la console Cyber Protect sous leur nom.

Les administrateurs peuvent appliquer des plans de protection qui utilisent l'emplacement de sauvegarde connecté à IONOS Cloud, Impossible Cloud, ou les connexions de stockage compatible S3 qu'ils ont ajoutées eux-mêmes ou par tout autre administrateur, et pour les ressources enregistrées dans la console Cyber Protect sous n'importe quel utilisateur.

Pour définir un emplacement de sauvegarde dans IONOS Cloud, Impossible Cloud ou tout stockage compatible S3

1. Dans la console Cyber Protect, effectuez l'une des opérations suivantes :
   - Si vous créez ou modifiez un plan de protection, allez dans **Terminaux**, puis sélectionnez la ressource que vous souhaitez sauvegarder dans IONOS Cloud, Impossible Cloud ou tout stockage compatible S3. Dans la section **Sauvegarde** du plan de protection de la ressource sélectionnée, cliquez sur le lien de la ligne **Où sauvegarder**.

     Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 243).

© Acronis International GmbH, 2003-2026

- Si vous gérez vos emplacements de stockage de sauvegarde et souhaitez ajouter IONOS Cloud, Impossible Cloud ou tout stockage compatible S3 en tant que nouvel emplacement, accédez à **Stockage de sauvegarde**.

  Pour plus d'informations sur la gestion de vos emplacements de stockage des sauvegardes, reportez-vous à "Stockage de sauvegarde" (p. 731).

2. Cliquez sur **Ajouter un emplacement**.
3. Dans la liste déroulante **Clouds publics**, sélectionnez l'une des options suivantes :
   - **Compatible S3**
   - **Impossible Cloud**
   - **IONOS Cloud Object Storage**
4. Définissez ce qui suit :
   - [Pour S3 compatible, IONOS Cloud ou Impossible Cloud] Dans le champ **Agent de gestion**, cliquez sur **Parcourir** pour sélectionner l'agent de gestion dans une liste d'agents appropriés. Cet agent établira la communication initiale avec le stockage compatible S3 / IONOS Cloud / Impossible Cloud. Vous pouvez modifier les paramètres de l'emplacement de sauvegarde ultérieurement, si nécessaire.

     Cet agent de gestion, qui peut être sélectionné parmi n'importe quel type pris en charge (y compris l'agent pour Windows/Linux/VMware [appliance virtuelle]/Hyper-V/oVirt [mais pas l'agent pour Azure]), est utilisé uniquement lors de la création ou de la modification de l'emplacement de sauvegarde. L'état hors ligne/en ligne de l'agent n'aura pas d'impact sur les sauvegardes effectuées par d'autres agents standard.
   - Dans le champ **Nom de l'emplacement**, saisissez le nom de l'emplacement de sauvegarde.

     Remarque
     Le nom de l'emplacement doit être unique dans le tenant client. Si le nom que vous ajoutez existe déjà dans la connexion, Cyber Protect Cloud ajoutera un suffixe numérique au nom. Par exemple, si « IONOS Cloud Object Storage » existe déjà, le nom sera automatiquement mis à jour en « IONOS Cloud Object Storage 1 ».

   - Dans le champ **Compartiment**, sélectionnez le compartiment de stockage IONOS Cloud, Impossible Cloud ou compatible S3 pertinent.

     Si le compartiment sélectionné est activé avec les fonctionnalités Verrouillage d'objet et Contrôle de version, la case à cocher **Période d'immuabilité de la sauvegarde (jours)** est activée. Vous pouvez ensuite définir le nombre de jours pour la période d'immuabilité, ce qui garantit que les données sauvegardées ne sont pas supprimées pendant cette période, et cette règle s'applique à tous les objets de sauvegarde créés par Cyber Protect Cloud.

© Acronis International GmbH, 2003-2026

Remarque
La période d'immuabilité peut être définie pour les types compatibles S3, Impossible Cloud, IONOS Cloud, et Amazon S3. Voir "Définir un emplacement de sauvegarde dans Amazon S3" (p. 748).

Notez que lorsque vous définissez la période d'immuabilité comme propriété de l'emplacement de sauvegarde, la période de rétention par défaut définie pour le compartiment est ignorée. Pour plus d'informations sur la fonctionnalité Verrouillage d'objet et les périodes de rétention, consultez la documentation pertinente. Par exemple, consultez la documentation Impossible Cloud.

Remarque
Nous vous recommandons de configurer la stratégie de cycle de vie pour le compartiment si vous avez défini l'option d'immuabilité lors de la création de l'emplacement de sauvegarde. Les compartiments avec les fonctionnalités de versionnage d'objet et de verrouillage d'objet activées stockeront les versions d'objet indéfiniment. En conséquence, la consommation de stockage augmentera indéfiniment, à moins qu'une stratégie de cycle de vie ne soit configurée.

Cependant, nous ne vous recommandons pas d'activer les fonctionnalités de versionnage d'objet et de verrouillage d'objet pour les compartiments utilisés par les emplacements de sauvegarde et qui sont configurés sans l'option d'immuabilité. Si des stratégies de cycle de vie sont appliquées à ces compartiments, elles peuvent accidentellement supprimer des objets liés à la chaîne de sauvegarde d'archive, ce qui entraînera une corruption de l'archive.

Avec l'option d'immutabilité configurée, le problème est résolu en ajustant la période d'immuabilité pour les anciens objets, sur lesquels les nouveaux objets de sauvegarde ont encore des dépendances. Cela se produit automatiquement à chaque sauvegarde planifiée : la période d'immuabilité de chaque objet appartenant à la chaîne de sauvegarde est prolongée par l'agent de sauvegarde qui communique avec le stockage dans le cloud. Cette période d'immuabilité n'est jamais inférieure à la valeur de jours d'immuabilité définie lors de la création de l'emplacement de sauvegarde. Pour plus d'informations sur la configuration de la stratégie de cycle de vie, consultez la documentation Wasabi (applicable lorsque le stockage cloud public Wasabi est ajouté comme type d'emplacement de sauvegarde « compatible S3 »).

Remarque
Les agents antérieurs à la version 24.06 peuvent effectuer des sauvegardes vers Impossible Cloud ou un stockage compatible S3, mais seuls les agents à partir de la version 24.06 appliqueront le verrouillage d'objet aux objets créés dans Impossible Cloud ou un stockage compatible S3. Cela signifie que seuls les agents plus récents peuvent reconnaître la période d'immuabilité définie comme propriété de l'emplacement de sauvegarde et gérer cette période pour toutes les sauvegardes créées. Les agents antérieurs à la version 24.06 ignoreront ce paramètre et les propriétés de verrouillage d'objet par défaut du compartiment seront appliquées aux objets créés dans Impossible Cloud ou un stockage compatible S3.

© Acronis International GmbH, 2003-2026

[Pour Impossible Cloud uniquement] La liste des compartiments est toujours récupérée à partir de l'URL du terminal principal (`https://eu-central-2.storage.impossibleapi.net/`), qui répertorie les compartiments dans toutes les régions. L'URL du terminal utilisée pour lire et écrire des données dans le compartiment est calculée à partir de la région détectée du compartiment et suit le format suivant : `https://[REGION_NAME].storage.impossibleapi.net`. Par exemple, si vous sélectionnez le compartiment **eu-central-1**, l'URL du terminal sera `https://eu-central-1.storage.impossibleapi.net/`.

[Pour IONOS Cloud uniquement] La liste des compartiments est toujours récupérée à partir de l'URL du terminal principal (`https://s3.eu-central-4.ionoscloud.com`), qui répertorie les compartiments dans toutes les régions. L'URL du terminal utilisée pour lire et écrire des données dans le compartiment est calculée à partir de la région détectée du compartiment et suit le format suivant : `https://s3.[REGION_NAME].ionoscloud.com`. Par exemple, si vous sélectionnez le compartiment **eu-central-2**, l'URL du terminal sera `https://s3.eu-central-2.ionoscloud.com/`.

Remarque
Les compartiments appartenant à l'utilisateur dans IONOS Cloud ne seront pas répertoriés, car ils nécessitent une URL de terminal unique pour l'accès. Pour utiliser les compartiments appartenant à l'utilisateur comme emplacements de sauvegarde, vous devez configurer un emplacement de sauvegarde de type **Compatible S3**, au lieu de **IONOS Cloud Object Storage**.

- [Pour le stockage Compatible S3 uniquement] Sélectionnez la case à cocher **Autoriser l'utilisation d'un certificat autosigné du terminal (vulnérable aux attaques MITM, non recommandé)** afin d'ignorer la validation de la chaîne de certificats et d'accepter les certificats autosignés pour l'URL du terminal S3.

  Notez que cette option est uniquement disponible lors de la création de l'emplacement de sauvegarde compatible S3 et qu'elle ne peut pas être modifiée lors de la modification de l'emplacement de sauvegarde.

5. Cliquez sur **Ajouter**.

   Si vous créez ou modifiez un plan de protection, l'emplacement de sauvegarde dans Impossible Cloud, IONOS Cloud ou un stockage compatible S3 est défini comme emplacement dans la ligne **Où sauvegarder**. Lorsque la sauvegarde est exécutée (manuellement ou selon la planification), elle est enregistrée dans l'emplacement défini.

   Si vous gérez vos emplacements de stockage des sauvegardes, vous pouvez afficher et mettre à jour les détails des emplacements selon vos besoins. L'emplacement Impossible Cloud, IONOS Cloud ou stockage compatible S3 est également disponible lors de la définition d'un emplacement de sauvegarde pour les ressources. Pour plus d'informations, voir "Affichage et mise à jour des emplacements de sauvegarde dans le cloud public" (p. 756).

© Acronis International GmbH, 2003-2026

Affichage et mise à jour des emplacements de sauvegarde dans le cloud public

Vous pouvez afficher et mettre à jour les emplacements de sauvegarde Microsoft Azure, Amazon S3 et cloud compatible S3 que vous avez définis dans le module **Stockage de sauvegarde**, ou lors de la création ou de la modification d'un plan de protection.

Pour plus d'informations sur la suppression de l'accès à un abonnement Microsoft Azure à partir de la console Cyber Protect, voir "Suppression de l'accès à un abonnement Microsoft Azure" (p. 764). Pour plus d'informations sur la suppression de l'accès à d'autres connexions au cloud public, voir "Gestion de l'accès à d'autres services de stockage dans le cloud public" (p. 765).

Remarque
Vous ne pouvez ni actualiser ni supprimer manuellement un emplacement de sauvegarde dans le cloud public dans le module **Stockage de sauvegarde**. Le contenu de l'emplacement de sauvegarde est mis à jour automatiquement après chaque opération de sauvegarde ou de restauration.

Pour afficher les emplacements de sauvegarde dans le cloud public

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
   La liste des emplacements de sauvegarde s'affiche, avec des détails sur la capacité de stockage et le nombre de sauvegardes attribuées à chaque emplacement.
   Pour plus d'informations sur l'utilisation des emplacements de sauvegarde répertoriés, voir "Stockage de sauvegarde" (p. 731).
2. Sélectionnez l'emplacement souhaité.
   Les sauvegardes en cours de l'emplacement sélectionné sont répertoriées.
3. (Facultatif) Cliquez sur une sauvegarde pour afficher d'autres informations la concernant.

Pour mettre à jour un emplacement de sauvegarde dans le cloud public dans un plan de protection

1. Accédez au plan de protection pertinent et sélectionnez **Modifier**.
2. Cliquez sur le lien dans la ligne **Où sauvegarder**.
3. Sélectionnez un emplacement de sauvegarde dans la liste ou cliquez sur **Ajouter un emplacement** pour ajouter un nouvel emplacement.
   Si l'abonnement Microsoft Azure ou la connexion au cloud public concernés sont déjà enregistrés dans la console Cyber Protect, sélectionnez-les dans la liste affichée.
   Si vous ajoutez un nouvel abonnement Microsoft Azure, vous êtes invité à authentifier les détails de votre compte Microsoft (voir "Ajout de l'accès à un abonnement Microsoft Azure" (p. 762)).
   Pour plus d'informations sur les autorisations requises lors de la connexion à Microsoft Azure, voir l'article Sécurité de la connexion à Microsoft Azure et audit (72684).

© Acronis International GmbH, 2003-2026

Gestion de l'accès du compte dans le cloud public

Pour activer les services Acronis Cyber Protection sur les plate-formes de cloud public, l'accès aux comptes Microsoft Azure, Amazon S3 ou cloud public compatible S3 concernés doit être configuré.

Par exemple, lorsque vous utilisez Microsoft Azure, l'accès à votre abonnement Microsoft Azure est requis. Une fois ajouté dans la console Cyber Protect, l'abonnement peut être sélectionné lorsque vous configurez une sauvegarde directe vers Microsoft Azure. De la même manière, pour Amazon S3, les clés d'accès associées à des stratégies de sauvegarde spécifiques sont requises.

L'accès aux clouds publics est géré par l'intermédiaire du menu **Infrastructure** de la console Cyber Protect.

Important
La validation de sauvegarde est désactivée pour les sauvegardes sur le stockage dans le cloud public, afin d'éviter des coûts de transfert de données vers des emplacements externes. De plus, vous ne pouvez actuellement pas « rattacher » un emplacement de sauvegarde sur un cloud public au même tenant client ou à un tenant client différent si l'emplacement a été précédemment supprimé.

Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public

Lors de la sauvegarde directe dans des services de stockage dans le cloud public, vous devez prendre en compte un certain nombre de conditions d'accès pour chaque plate-forme :

- Microsoft Azure
- Amazon S3
- Stockage compatible S3 (inclut Wasabi, IONOS Cloud et Impossible Cloud)

Sauvegarde dans Microsoft Azure

Pour vous connecter à un abonnement Microsoft Azure, vous devez disposer de plusieurs autorisations. Pour plus d'informations à ce sujet, voir l'article Sécurité et audit des connexions Microsoft Azure (72684).

Remarque
Pour établir la connexion à l'abonnement, vous devez disposer de l'un des rôles suivants dans Microsoft Azure AD : Administrateur d'applications dans le cloud, administrateur d'applications ou administrateur global. Vous devez également recevoir le rôle de propriétaire pour chaque abonnement sélectionné.

Sauvegarde dans Amazon S3

Lorsque vous effectuez des sauvegardes dans Amazon S3, plusieurs conditions doivent être remplies pour que vous puissiez définir les emplacements de sauvegarde dans Amazon S3 :

© Acronis International GmbH, 2003-2026

- Classes de stockage prises en charge
- Autorisations de politiques
- Clés d'accès
- Paramètres de compartiment

Classes de stockage prises en charge

Les classes de stockage Amazon S3 prises en charge actuellement sont les suivantes :

- S3 Standard
- Standard - Accès peu fréquent (S3 Standard-IA)
- Une zone - Accès peu fréquent (S3 Une zone-IA)
- S3 Hiérarchisation intelligente

Autorisations de stratégies

Lors de la sauvegarde vers Amazon S3, votre compte Amazon doit disposer des autorisations minimales appliquées pour garantir que Cyber Protect Cloud puisse sauvegarder les ressources concernées vers Amazon S3. Cela signifie que les utilisateurs concernés doivent avoir accès à la console de gestion AWS et que la stratégie appropriée doit être appliquée au(x) groupe(s) auquel ils sont affectés.

Remarque
Les autorisations de stratégie spécifiées pour Amazon S3 peuvent être réutilisées par d'autres services de stockage compatibles S3. Pour plus d'informations, voir "Sauvegarde vers un stockage compatible S3 (inclut Wasabi, IONOS Cloud et Impossible Cloud)" (p. 759).

Exemples

L'exemple de stratégie suivant montre l'ensemble minimal d'autorisations pour un large champ d'application de ressources, lors de la sauvegarde et de la restauration vers/depuis un compartiment spécifique (indiqué par [BUCKETNAME]). Notez que * indique toutes les ressources.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

L'exemple de stratégie suivant indique les autorisations minimales d'un compartiment quelconque du compte. Notez que `[BUCKETNAME]` doit être remplacé par le nom du compartiment.

© Acronis International GmbH, 2003-2026

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::*" }, { "Effect": "Allow",
"Action": "sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::*" } ] }
```

Clés d'accès

Acronis exige les clés d'accès à chaque connexion à Amazon S3 et les utilise lors de la définition de la connexion à Amazon S3. Pour plus d'informations sur la génération de clés d'accès et de leurs identifiants, consultez la documentation d'Amazon S3.

Paramètres de compartiment

Lorsque vous utilisez les compartiments Amazon S3 comme emplacement de sauvegarde, assurez-vous que le compartiment est configuré avec les paramètres par défaut, y compris le blocage de tous les accès publics (par défaut, ce paramètre est **activé**). Pour plus d'informations sur l'utilisation des compartiments, consultez la documentation d'Amazon S3.

Remarque
Les exemples dans Autorisations de stratégie incluent un ensemble complet d'autorisations. Si vous n'avez pas besoin d'immuabilité sur un compartiment, vous pouvez exclure les autorisations associées telles que `s3:GetBucketObjectLockConfiguration` (pour créer et modifier l'emplacement de sauvegarde) et `s3:GetObjectRetention` (pour détecter la nécessité de mettre à jour le verrouillage d'objet pour une période réduite).

Sauvegarde vers un stockage compatible S3 (inclut Wasabi, IONOS Cloud et Impossible Cloud)

Lorsque vous effectuez des sauvegardes dans un stockage compatible S3, vous devez tenir compte d'un certain nombre d'exigences lors de la définition des emplacements de sauvegarde :

- Autorisations de politiques
- Clés d'accès
- Paramètres de compartiment

Autorisations de politiques

Lorsque vous définissez un emplacement de sauvegarde dans un stockage compatible S3, assurez-vous que les stratégies adéquates sont appliquées aux groupes et utilisateurs pertinents.

© Acronis International GmbH, 2003-2026

Remarque
Les autorisations de stratégie spécifiées pour Amazon S3 (voir ci-dessus) peuvent être réutilisées pour d'autres services de stockage compatibles S3. Notez que l'autorisation `sts:GetFederationToken` est uniquement applicable à Amazon S3 et n'est pas requise pour les autres services compatibles S3.

Important
Lors de la première connexion à Wasabi, des identifiants temporaires créés avec l'autorisation `AssumeRole` sont utilisés. Cela entraîne des autorisations d'accès supplémentaires, ce qui signifie que, même s'il existe des autorisations dans la stratégie Wasabi qui restreignent l'utilisation de compartiments spécifiques, ces compartiments seront toujours disponibles dans la liste déroulante des compartiments disponibles. Les opérations de sauvegarde et de restauration fonctionneront avec n'importe quel compartiment sélectionné dans la liste.

Toutefois, le jeton d'accès fourni à l'agent lors des opérations de sauvegarde/restauration est limité aux opérations d'un compartiment spécifique uniquement, soit le compartiment sélectionné lors de la création de l'emplacement de sauvegarde sur Wasabi dans la console Cyber Protect. Après la création de l'emplacement de sauvegarde, le système limitera les opérations de l'agent au compartiment sélectionné.

Exemples

L'exemple de stratégie suivant est réservée à Wasabi et montre les autorisations minimales pour n'importe quel compartiment dans le compte.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource": "*"
}, { "Effect": "Allow", "Action": [ "s3:ListBucket", "s3:ListBucketVersions" ],
"Resource": "*" }, { "Effect": "Allow", "Action": [ "iam:CreateRole",
"iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "*"
}, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject", "s3:GetObjectVersion", "s3:GetObjectRetention",
"s3:PutObjectRetention" ], "Resource": "*" } ] }
```

L'exemple de stratégie suivant concerne le stockage compatible S3, IONOS Cloud et Impossible Cloud, et montre des autorisations limitées avec un champ d'application restreint des ressources. Notez que `[BUCKETNAME]` doit être remplacé par le nom du compartiment.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
```


© Acronis International GmbH, 2003-2026

```
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

L'exemple de stratégie suivant concerne le stockage compatible S3, IONOS Cloud et Impossible Cloud, et montre les autorisations minimales pour tout compartiment du compte.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::*" } ] }
```

Clés d'accès

Les clés d'accès sont requises pour chaque connexion compatible S3 et sont utilisées lors de la définition de la connexion.

Notez que les clés d'accès des comptes utilisateur root (superutilisateur) sur Wasabi ne peuvent pas être utilisées, car AssumeRole ne peut pas être appelé par les utilisateurs root. Vous devez créer un utilisateur non-root distinct et générer des clés d'accès pour cet utilisateur.

Pour plus d'informations sur la génération de clés d'accès et d'identifiants de clé d'accès, consultez la documentation correspondante. Par exemple, voir la documentation Wasabi, la documentation IONOS Cloud et la documentation Impossible Cloud.

Paramètres de compartiment

Lors de l'utilisation de compartiments comme emplacement de sauvegarde, assurez-vous que le compartiment est configuré avec les paramètres par défaut. Pour plus d'informations sur la gestion des compartiments, consultez la documentation correspondante. Par exemple, voir la documentation Wasabi, la documentation IONOS Cloud ou la documentation Impossible Cloud.

Gestion de l'accès aux abonnements Microsoft Azure

En vous connectant aux abonnements Microsoft Azure pertinents dans la console Cyber Protect, vous pouvez sauvegarder les ressources pertinentes directement dans Microsoft Azure.

© Acronis International GmbH, 2003-2026

La connexion à un abonnement peut être configurée lors de la création d'un emplacement de sauvegarde via le menu **Terminaux** ou **Stockage de sauvegarde**, comme le décrit la section "Définition d'un emplacement de sauvegarde dans Microsoft Azure" (p. 745).

Ces abonnements Microsoft Azure peuvent également être configurés dans l'écran **Clouds publics** (accédez à **Infrastructure > Clouds publics**). Vous pouvez également gérer vos abonnements, notamment renouveler l'accès à l'abonnement, afficher les propriétés et les activités de l'abonnement, ou supprimer l'abonnement. Notez que si vous déployez l'agent pour Azure pour exécuter des sauvegardes sans agent de machines virtuelles Microsoft Azure, un onglet supplémentaire s'affiche dans lequel vous pouvez afficher et mettre à jour votre déploiement. Pour plus d'informations, voir "Affichage et mise à jour d'un agent pour Azure déployé" (p. 165).

En fonction du rôle d'utilisateur qui vous a été attribué, vous pouvez être en mesure de gérer les abonnements Microsoft Azure ajoutés par d'autres utilisateurs de votre organisation. Par exemple, si vous êtes administrateur d'entreprise ou d'unité, ou avez reçu le rôle de cyberadministrateur ou d'administrateur dans le service de cyberprotection, vous pouvez afficher et gérer les abonnements Microsoft Azure ajoutés par d'autres administrateurs et des utilisateurs non-administrateurs. Ces derniers peuvent uniquement afficher les abonnements Microsoft Azure qu'ils ont ajoutés à la console Cyber Protect.

Remarque
Les partenaires peuvent gérer les abonnements Microsoft Azure de clients de niveau hiérarchique inférieur. Toutefois, lorsqu'un partenaire sélectionne **Tous les clients**, le menu **Infrastructure** de la console Cyber Protect n'est pas disponible.

Important
Lors de la connexion à un abonnement Microsoft Azure, Acronis exige les autorisations minimales pour la connexion à l'abonnement. Pour plus d'informations sur les autorisations nécessaires, reportez-vous à l'article Microsoft Azure connection security and audit (72684).

Ajout de l'accès à un abonnement Microsoft Azure

En ajoutant un abonnement Microsoft Azure dans la console Cyber Protect, Acronis peut accéder en toute sécurité à votre abonnement et sauvegarder directement les ressources pertinentes dans Microsoft Azure.

Pour ajouter l'accès à un abonnement Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Cliquez sur **Ajouter**, puis sélectionnez **Microsoft Azure** dans la liste des options.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Se connecter**. Vous êtes redirigé vers la page de connexion de Microsoft.

© Acronis International GmbH, 2003-2026

Remarque
Pour établir la connexion à l'abonnement, vous devez disposer de l'un des rôles suivants dans Microsoft Azure AD : Administrateur d'applications dans le cloud, administrateur d'applications ou administrateur global. Vous devez également recevoir le rôle de propriétaire pour chaque abonnement sélectionné.

4. Dans l'écran de connexion Microsoft, saisissez vos identifiants de connexion et acceptez les autorisations demandées. Le processus de connexion démarre et peut prendre plusieurs minutes.

   Pour plus d'informations sur l'accès sécurisé à votre abonnement Microsoft Azure, voir l'article Microsoft Azure connection security and audit (72684).
5. Lorsque la connexion est terminée, procédez comme suit :
   a. Dans le champ **Abonnement Microsoft Azure**, sélectionnez l'abonnement pertinent dans la liste.
   b. [Facultatif] Dans le champ **Région Azure**, sélectionnez la région dans laquelle vous souhaitez déployer les ressources système.

      Remarque
      Le système présélectionne la région dans laquelle se trouvent la plupart des groupes de ressources, mais vous pouvez la modifier selon vos préférences.
6. Cliquez sur **Ajouter un abonnement**.

   L'abonnement est ajouté à la liste des clouds publics.

   Pour renouveler le certificat d'accès annuel de l'abonnement, voir "Renouvellement de l'accès à un abonnement Microsoft Azure" (p. 763).

   Pour supprimer l'accès à l'abonnement, voir "Suppression de l'accès à un abonnement Microsoft Azure" (p. 764).

Remarque
Si le compte Microsoft Azure auquel vous êtes connecté comprend l'accès à plusieurs AD Microsoft Azure, y compris ceux dans lesquels vous avez été invité en tant qu'utilisateur invité, seul le répertoire utilisateur par défaut est sélectionné. Si vous souhaitez utiliser un répertoire dans lequel vous êtes utilisateur invité, vous devez créer un nouvel utilisateur dans cet AD Microsoft Azure spécifique. Vous pouvez alors vous connecter à ce compte et à l'abonnement pertinent.

Renouvellement de l'accès à un abonnement Microsoft Azure

Une fois que vous êtes enregistré dans la console Cyber Protect, l'accès à un abonnement Microsoft Azure est défini automatiquement pour une année par Acronis à l'aide d'un certificat d'accès gratuit et unique. Lorsque le certificat s'approche de sa date d'expiration, vous pouvez le renouveler facilement et rapidement.

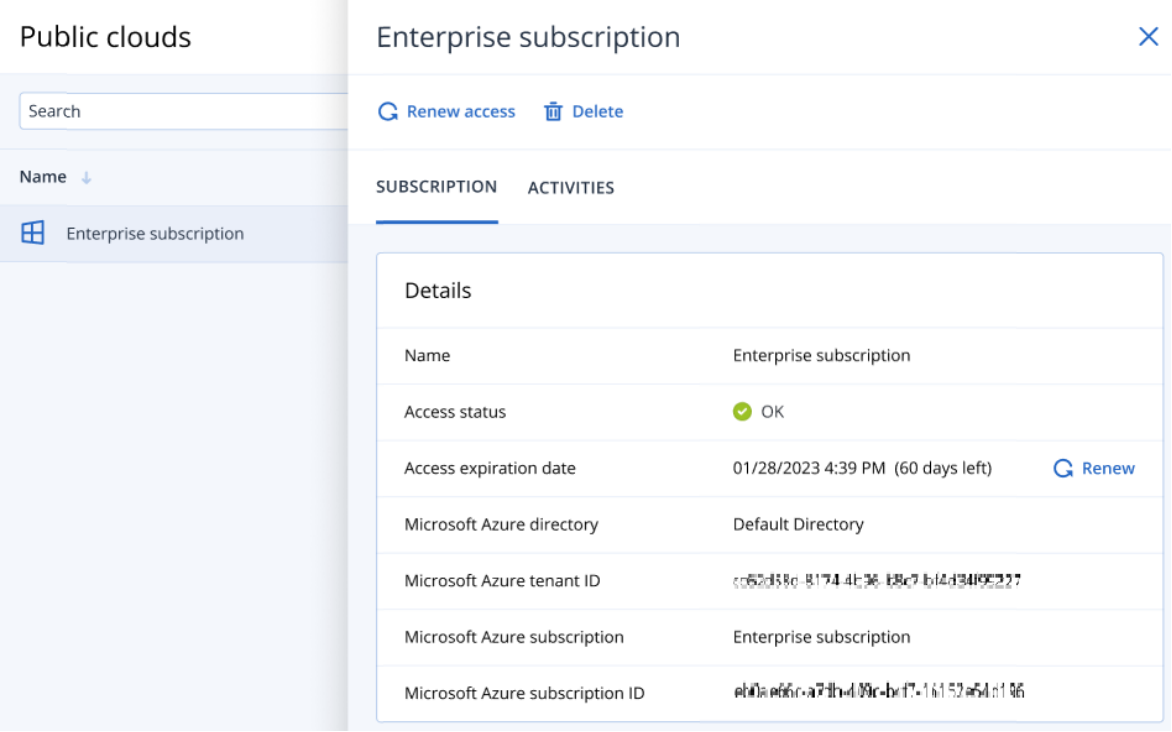
Pour renouveler le certificat d'accès de votre abonnement Microsoft Azure

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez l'abonnement pertinent dans la liste affichée.

   Remarque
   La colonne **État de l'accès** indique le statut actuel du certificat d'accès pour chaque abonnement et indique l'un des deux statuts : **OK** ou **Expiré**.

3. Dans le volet de droite, cliquez sur **Renouveler l'accès**.
   Vous pouvez également cliquer sur l'onglet **Abonnement**, puis sur **Renouveler** dans le champ **Date d'expiration de l'accès**.



4. Dans l'écran de connexion Microsoft, saisissez vos identifiants de connexion et acceptez les autorisations demandées. Le processus de connexion démarre et peut prendre plusieurs minutes.
   Lorsque l'authentification est réussie, l'accès est renouvelé automatiquement pour une année.
   Pour plus d'informations sur les autorisations nécessaires, reportez-vous à l'article Microsoft Azure connection security and audit (72684).

Suppression de l'accès à un abonnement Microsoft Azure

Vous devez supprimer l'accès à l'abonnement Microsoft Azure si vous ne sauvegardez pas les ressources dans Microsoft Azure.

Pour supprimer l'accès à un abonnement Microsoft Azure

© Acronis International GmbH, 2003-2026

Important
Vous ne pouvez pas supprimer un abonnement s'il est en cours d'utilisation par une sauvegarde dans Microsoft Azure.

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez l'abonnement pertinent dans la liste affichée.
3. Dans le volet de droite, cliquez sur **Supprimer**.

   Remarque
   Vous ne pouvez retirer qu'un abonnement que vous avez ajouté. Vous pouvez également supprimer un abonnement si vous êtes administrateur d'entreprise ou de division, ou avez reçu le rôle de cyberadministrateur ou d'administrateur du service de cyberprotection.

4. Dans le message de confirmation qui s'affiche, cliquez sur **Supprimer**.

Gestion de l'accès à d'autres services de stockage dans le cloud public

Remarque
Cette section concerne la gestion de l’accès aux services de stockage cloud public Amazon S3 ou compatibles S3. La gestion de l’accès pour Microsoft Azure est décrite dans "Gestion de l'accès aux abonnements Microsoft Azure" (p. 761).

En vous connectant au compte Amazon S3 ou cloud public compatible S3 concerné dans la console Cyber Protect, vous pouvez sauvegarder directement les ressources vers le stockage cloud public concerné.

Vous pouvez configurer les connexions aux comptes de stockage dans le cloud public lors de la création d'un emplacement de sauvegarde via le menu **Terminaux** ou **Stock. de sauvegarde**. Vous pouvez également configurer les connexions aux clouds publics dans l'écran **Clouds publics** (accédez à **Infrastructure > Clouds publics**). Vous pouvez également gérer votre connexion, notamment en renouvelant l'accès à la connexion, en affichant les propriétés et les activités de la connexion, ou en supprimant la connexion.

Selon le rôle d'utilisateur qui vous a été attribué, vous pouvez être en mesure de gérer les connexions dans le cloud public ajoutées par d'autres utilisateurs de votre organisation. Par exemple, si vous êtes administrateur d'entreprise ou d'unité, ou avez reçu le rôle de cyberadministrateur ou d'administrateur du service de cyberprotection, vous pouvez visualiser et gérer les connexions au cloud public ajoutées par d'autres administrateurs et les utilisateurs non-administrateurs. Les utilisateurs non-administrateurs peuvent uniquement afficher et utiliser les connexions au cloud public qu'ils ont ajoutés à la console Cyber Protect.

© Acronis International GmbH, 2003-2026

Remarque
Les partenaires peuvent gérer les connexions au cloud public des clients situés en dessous de leur niveau dans la hiérarchie. Toutefois, lorsqu'un partenaire sélectionne **Tous les clients**, le menu **Infrastructure** de la console Cyber Protect n'est pas disponible.

Important
Lors de la connexion à un cloud public, Acronis requiert un certain nombre d'autorisations. Pour plus d'informations, voir "Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public" (p. 757).

Ajout d'un accès à une connexion au cloud public

Remarque
Les compartiments dans des régions spéciales GovCloud (par exemple, `https://aws.amazon.com/govcloud-us/`, `https://learn.microsoft.com/en-us/azure/azure-government/regions`, ou d'autres URL de terminal provenant de fournisseurs de stockage soutenant le concept GovCloud) ne sont pas pris en charge comme emplacements de sauvegarde.

Après avoir ajouté une connexion cloud public pour Amazon S3 ou le stockage Microsoft Azure dans la console Cyber Protect, vous pouvez accéder de manière sécurisée à vos ressources cloud et sauvegarder directement les ressources vers le stockage cloud public concerné.

Avertissement !
Après avoir ajouté un emplacement, vous ne pouvez pas supprimer l'accès au cloud public. Pour supprimer l'accès, vous devez supprimer l'emplacement. Voir "Suppression d'une connexion à un cloud public" (p. 770).

Pour plus d'informations sur l'ajout d'accès au stockage cloud Microsoft Azure, voir "Gestion de l'accès aux abonnements Microsoft Azure" (p. 761).

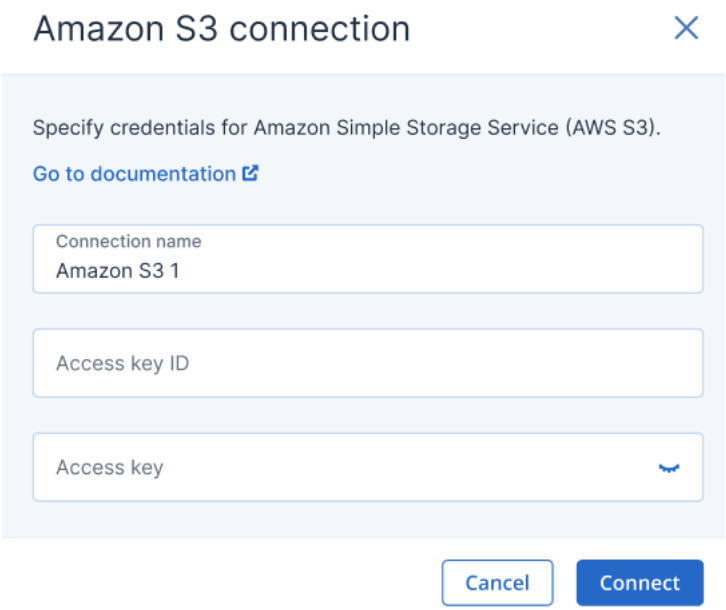
Pour ajouter un accès à une connexion au cloud public

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Cliquez sur **Ajouter** et sélectionnez l'une des options suivantes :

   Amazon S3
   Dans la boîte de dialogue qui s'affiche, définissez les options suivantes :
   - **Nom de la connexion** : nom de la connexion Amazon S3.
   - **Identifiant de la clé d'accès** : identifiant de la clé d'accès de l'utilisateur pour le service Amazon S3.
   - **Clé d'accès** : clé d'accès de l'utilisateur au service Amazon S3.
     La clé d'accès et son identifiant permettent d'accéder aux classes et aux compartiments de stockage pour la connexion concernée. Pour plus d'informations sur les clés d'accès et les

© Acronis International GmbH, 2003-2026

autorisations, voir "Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public" (p. 757).



Remarque
Pour que l'accès au stockage aboutisse, l'heure système sur l'agent qui exécute les opérations de sauvegarde et de restauration avec le stockage Amazon S3 doit être synchronisée avec celle des serveurs NTP.

Compatible S3

Remarque
Les services de stockage compatibles S3 hébergés en privé (c'est-à-dire inaccessibles via Internet) et en public sont pris en charge.

Dans la boîte de dialogue qui s'affiche, définissez les options suivantes :

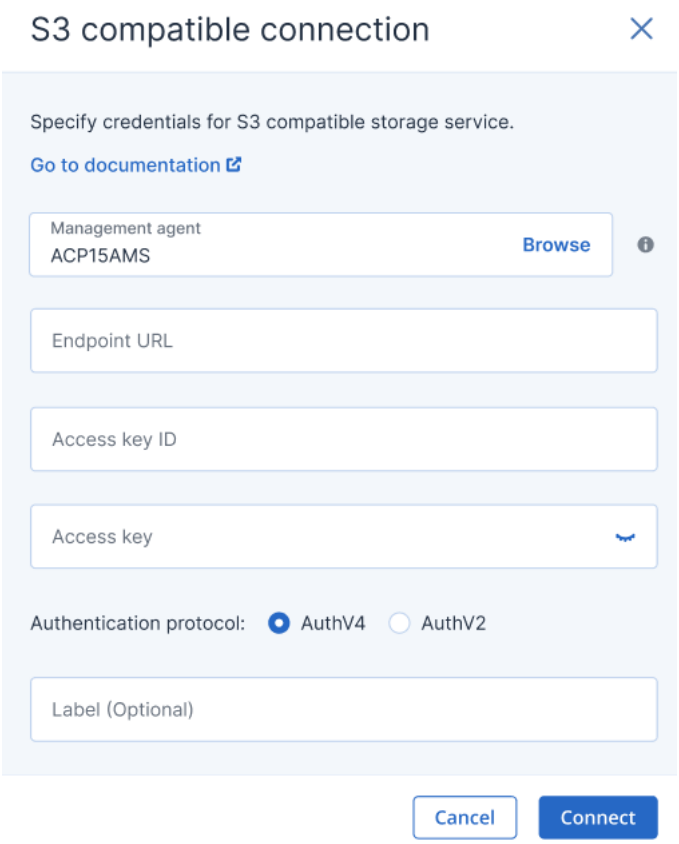
- **Agent de gestion** : cliquez sur **Parcourir** pour sélectionner l'agent de gestion dans la liste des agents appropriés. Cet agent établira la communication initiale avec le stockage compatible S3. Vous pouvez modifier les paramètres de l'emplacement de sauvegarde ultérieurement, si nécessaire.

  Cet agent de gestion, qui peut être sélectionné parmi n'importe quel type pris en charge (y compris l'agent pour Windows/Linux/VMware [appliance virtuelle]/Hyper-V/oVirt [mais pas l'agent pour Azure]), est utilisé uniquement lors de la création ou de la modification de l'emplacement de sauvegarde. L'état hors ligne/en ligne de l'agent n'aura pas d'impact sur les sauvegardes effectuées par d'autres agents standard.
- **URL de terminal** : saisissez l'URL du terminal partagé par le fournisseur de stockage compatible S3 pour effectuer des opérations avec le stockage. Notez qu'il doit y avoir une chaîne de certificats de sécurité valide pour le terminal spécifié dans cette URL. La connexion aux terminaux à l'aide de certificats autosignés n'est pas autorisée.

© Acronis International GmbH, 2003-2026

- **Identifiant de la clé d'accès** : identifiant de la clé d'accès de l'utilisateur pour le stockage compatible S3.
- **Clé d'accès** : clé d'accès de l'utilisateur au stockage compatible S3.

  La clé d'accès et son identifiant permettent d'accéder aux classes et aux compartiments de stockage pour la connexion concernée. Pour plus d'informations sur les clés d'accès et les autorisations, voir "Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public" (p. 757).
- **Protocole d'authentification** : sélectionnez la version du protocole d'authentification prise en charge côté stockage. Par défaut, la version **AuthV4** est sélectionnée.
- **Étiquette** : (facultatif) ajoutez des étiquettes si nécessaire.



Impossible Cloud

Dans la boîte de dialogue qui s'affiche, définissez les options suivantes :

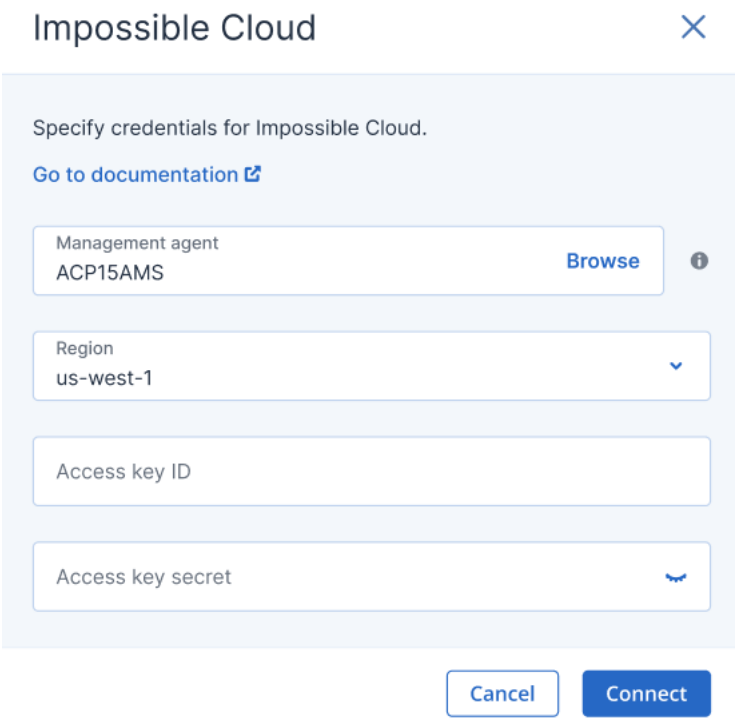
- **Agent de gestion** : cliquez sur **Parcourir** pour sélectionner l'agent de gestion dans la liste des agents appropriés. Cet agent établira la communication initiale avec Impossible Cloud. Vous pouvez modifier les paramètres de l'emplacement de sauvegarde ultérieurement, si nécessaire.

  Cet agent de gestion, qui peut être sélectionné parmi n'importe quel type pris en charge (y compris l'agent pour Windows/Linux/VMware [appliance virtuelle]/Hyper-V/oVirt [mais pas l'agent pour Azure]), est utilisé uniquement lors de la création ou de la modification de l'emplacement de sauvegarde. L'état hors ligne/en ligne de l'agent n'aura pas d'impact sur les sauvegardes effectuées par d'autres agents standard.

© Acronis International GmbH, 2003-2026

- **Région** : sélectionnez la région pertinente.
- **Identifiant de la clé d'accès** : identifiant de la clé d'accès de l'utilisateur pour le stockage Impossible Cloud.
- **Clé d'accès** : clé d'accès de l'utilisateur au stockage Impossible Cloud.

  La clé d'accès et son identifiant permettent d'accéder aux classes et aux compartiments de stockage pour la connexion concernée. Pour plus d'informations sur les clés d'accès et les autorisations, voir "Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public" (p. 757).



Remarque
Pour que l'accès au stockage aboutisse, l'heure système sur l'agent qui exécute les opérations de sauvegarde et de restauration avec le stockage Impossible Cloud doit être synchronisée avec celle des serveurs NTP.

3. Cliquez sur **Connexion**.

   Le processus de connexion démarre et peut durer plusieurs minutes. Une fois terminé, la connexion est ajoutée à la liste des clouds publics.

   Pour renouveler le certificat d'accès annuel à la connexion, voir "Renouvellement de l'accès à une connexion au cloud public" (p. 770).

   Pour supprimer l'accès à la connexion, voir "Suppression d'une connexion à un cloud public" (p. 770).

© Acronis International GmbH, 2003-2026

Renouvellement de l'accès à une connexion au cloud public

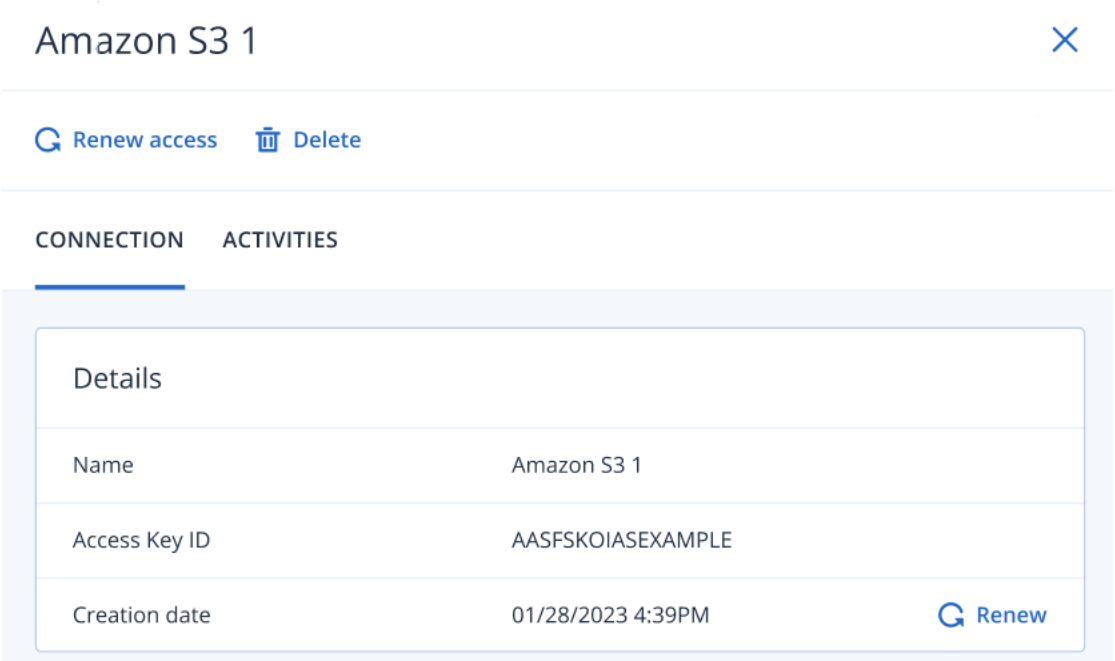
Après l'enregistrement d'une connexion au cloud public dans la console Cyber Protect, Acronis attribue automatiquement un certificat d'accès gratuit et unique qui permet d'accéder à la connexion au cloud public. Le certificat est valable un an. Lorsque le certificat approche de sa date d'expiration, vous pouvez le renouveler.

Pour renouveler le certificat d'accès à votre connexion au cloud public

1. Dans la console Cyber Protect, accédez à **Infrastructure > Clouds publics**.
2. Sélectionnez la connexion concernée dans la liste.

   Remarque
   La colonne **État d'accès** indique l'état actuel du certificat d'accès pour chaque connexion et présente l'un des deux états suivants : **OK** ou **Expiré**.

3. Dans le volet de droite, cliquez sur **Renouveler l'accès**.
   Vous pouvez également cliquer sur l'onglet **Connexion**, puis sur **Renouveler** dans la ligne **Date de création**.



   Lorsque l'authentification est réussie, l'accès est renouvelé automatiquement pour une année.

Suppression d'une connexion à un cloud public

Vous devez supprimer la connexion à un cloud public si vous ne sauvegardez pas de ressources dessus. La suppression de la connexion est le seul moyen de supprimer l'accès au cloud public.

© Acronis International GmbH, 2003-2026

Remarque
Vous ne pouvez supprimer que les connexions que vous avez ajoutées. Pour supprimer la connexion d'un autre utilisateur à un cloud public, vous devez avoir l'un des rôles suivants : Administrateur de l'entreprise, Administrateur de l'unité, Administrateur de la cyberprotection ou Administrateur dans le service de cyberprotection.

Important
Pour supprimer une connexion actuellement utilisée pour des sauvegardes vers un cloud public, vous devez d'abord supprimer tous les emplacements de sauvegarde qui utilisent cette connexion.

Pour supprimer une connexion au cloud public

1. Dans la console Cyber Protect, accédez à **Sauvegardes** > **Stockage de sauvegarde**.
2. Supprimez tous les emplacements de sauvegarde sur les clouds publics qui utilisent cette connexion.

   Remarque
   Les objets du stockage ne seront pas supprimés. Cette opération supprime uniquement l'emplacement de la liste des emplacements de sauvegarde dans la console Cyber Protect, sans impacter les données.

3. Accédez à **Infrastructure** > **Clouds publics**.
4. Sélectionnez la connexion dans la liste.
5. Dans le panneau le plus à droite, cliquez sur **Supprimer**.
6. Sur l'écran de confirmation, cliquez sur **Supprimer**.

En conséquence, l'accès au cloud public est supprimé.

Archivage d'e-mails

Avec l'archivage des e-mails, tous les e-mails de votre organisation Microsoft 365 sont conservés dans une archive externe stockée dans le cloud, ce qui vous permet de respecter les réglementations et de répondre aux demandes d'eDiscovery. Les nouveaux e-mails sont ajoutés à l'archive en continu, au fur et à mesure de leur envoi ou de leur réception, et ne peuvent pas être modifiés ni supprimés manuellement.

Les e-mails sont affichés dans deux dossiers pour chaque boîte aux lettres d'utilisateur, **Entrants** et **Sortants**. Dans chaque dossier, les e-mails sont triés chronologiquement, du plus récent au plus ancien.

L'archive est chiffrée avec l'algorithme AES-256. Seuls les utilisateurs autorisés peuvent accéder à l'archive en fonction de leur niveau d'accès, et une piste d'audit de toutes les actions est disponible.

Outre les fonctionnalités liées à la conformité, l'archivage des e-mails fournit des fonctionnalités de sauvegarde et de restauration.

© Acronis International GmbH, 2003-2026

Vous pouvez exécuter les opérations suivantes :

- Parcourir l'archive
- Rechercher de messages spécifiques à l'aide de requêtes de recherche ponctuelles et de requêtes de recherche enregistrées
- Prévisualiser des e-mails sans les restaurer
- Restaurer des e-mails spécifiques, les dossiers **Entrants** et **Sortants**, ainsi que des boîtes aux lettres complètes vers la boîte aux lettres d'origine ou vers une autre boîte aux lettres
- Téléchargement des pièces jointes aux e-mails

Par défaut, tous les e-mails sont conservés dans l'archive indéfiniment. Pour supprimer les e-mails dont vous n'avez plus besoin, vous pouvez appliquer des règles de rétention. Lorsque la période de rétention est atteinte, les e-mails sont automatiquement supprimés. Vous ne pouvez pas supprimer manuellement des e-mails de l'archive.

Pour conserver des e-mails spécifiques dans l'archive, quelle que soit la règle de rétention, vous pouvez appliquer des règles de conservation légale. Pendant la durée légale de conservation, ces e-mails ne peuvent pas être supprimés.

Par exemple, vous pouvez configurer des règles de rétention ou des règles de conservation légale pour les e-mails d'un expéditeur spécifique, les e-mails d'un destinataire spécifique ou les e-mails contenant un mot spécifique dans l'objet.

Limites

- En raison d'une limitation de Microsoft, la taille maximale d'un e-mail pouvant être inclus dans l'archive est de 150 Mo.
- Les brouillons d'e-mails ne sont pas inclus dans l'archive.
- Vous pouvez appliquer un plan d'archivage à un serveur de messagerie.

Configuration de l'archivage des e-mails

Ajout d'un serveur de messagerie

Prérequis

Les quotas suivants doivent être activés pour le tenant dans le Portail de gestion :

- **Postes d'archivage d'e-mails Microsoft 365**
- **Stockage d'archives**

Remarque
Les deux quotas sont requis. Si l'un d'eux est supprimé ou mal configuré après la configuration initiale, l'archivage des e-mails sera suspendu pour tous les plans du tenant jusqu'à ce que le quota soit restauré.

© Acronis International GmbH, 2003-2026

Pour ajouter un serveur de messagerie

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux**, puis cliquez sur **Ajouter** > **Microsoft 365 Business - Archivage des e-mails**.
   Vous êtes redirigé vers la page de connexion Microsoft 365.
3. Sur la page de connexion Microsoft, connectez-vous en tant qu'administrateur global.
4. Examinez la liste des autorisations requises, puis cliquez sur **Accepter**.
   Votre serveur de messagerie Microsoft 365 apparaît dans la console Cyber Protect, dans l'onglet **Terminaux** > **Serveurs de messagerie**.
5. Dans l'écran qui s'ouvre, configurez le plan d'archivage comme décrit dans "Création d'un plan d'archivage" (p. 776).

Affichage des activités d'archivage des e-mails

Vous pouvez afficher les activités d'archivage des e-mails suivantes :

- Activités liées uniquement aux serveurs de messagerie.
- Toutes les activités, y compris celles qui sont liées aux serveurs de messagerie et aux archives d'e-mails.

Pour afficher les activités

Lié aux serveurs de messagerie

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux** > **Serveurs de messagerie**.
3. Dans l'écran principal, cliquez sur le nom du serveur de messagerie, puis cliquez sur l'onglet **Activités**.

Tout

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Surveillance** > **Activités**.

Affichage des alertes d'archivage des e-mails

Vous pouvez consulter les alertes d'archivage des e-mails suivantes :

- Alertes qui ne concernent que les serveurs de messagerie.
- Toutes les alertes, y compris les activités liées aux serveurs de messagerie et aux archives d'e-mails.

Pour afficher les alertes

Lié aux serveurs de messagerie

© Acronis International GmbH, 2003-2026

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux** > **Serveurs de messagerie**.
3. Dans l'écran principal, cliquez sur le nom du serveur de messagerie, puis cliquez sur l'onglet **Alertes**.

Tout

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Surveillance** > **Alertes**.

Suppression d'un serveur de messagerie

Vous pouvez supprimer un serveur de messagerie ajouté à la console Cyber Protect.

Pour supprimer un serveur de messagerie

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux** > **Serveurs de messagerie**.
3. Dans l'écran principal, cliquez sur le nom du serveur de messagerie, puis cliquez sur **Supprimer**.
4. Pour confirmer votre choix, cliquez sur **Supprimer**.

Par conséquent, le serveur de messagerie est supprimé de la console Cyber Protect. L'archive d'e-mails est conservée, mais elle n'est plus mise à jour.

Téléchargement d'un rapport de licence pour l'archivage des e-mails

Vous pouvez télécharger un rapport de licences pour l’archivage des e-mails au niveau du partenaire et au niveau du client.

Dans les tenants de client, ce rapport n'est disponible que si un serveur de messagerie Microsoft 365 est ajouté.

Pour télécharger un rapport de licence

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit.
3. Cliquez sur **Rapport de licence d'archivage des e-mails**.
   Un fichier ZIP est téléchargé sur votre ordinateur. Le fichier ZIP contient le rapport de licence, au format CSV.

Archivage des e-mails dans des tenants désactivés ou supprimés

L'archivage des e-mails n'est pas activé dans les types de tenants suivants :

- Désactivé
  Vous pouvez réactiver un tenant désactivé.
- Supprimé de manière réversible (dans les 30 jours suivant la suppression)

© Acronis International GmbH, 2003-2026

Vous pouvez restaurer un tenant supprimé dans les 30 jours suivant sa suppression.

- Supprimé de manière définitive (plus de 30 jours de suppression)
  Vous ne pouvez pas restaurer un tenant si sa suppression date de plus de 30 jours.

Le tableau ci-dessous résume le comportement des solutions.

Type de tenant		
Désactivé ou supprimé (suppression réversible)	**Réactivé ou restauré**	**Supprimé (suppression définitive)**
• Les opérations de découverte ne s'exécutent pas. • Les nouveaux e-mails entrants et sortants ne sont pas ajoutés à l'archive d'e-mails. • Les règles de rétention ne sont pas appliquées. • Les règles de conservation légale ne sont pas appliquées. • Les opérations d'indexation ne s'exécutent pas.	• Les opérations de découverte sont réexécutées. • Les nouveaux e-mails entrants et sortants sont ajoutés à l'archive d'e-mails. • Les métadonnées des postes Microsoft 365 sont mises à jour (par exemple, les modifications de l'adresse e-mail des utilisateurs). • Les e-mails de la période pendant laquelle le tenant était désactivé ou supprimé sont importés dans la messagerie, conformément à la configuration du plan d'archivage (par exemple, messagerie de toutes les boîtes aux lettres ou de boîtes aux lettres sélectionnées). • Les règles de rétention sont appliquées. • Les règles de conservation légale sont appliquées. • Les opérations d'indexation sont réexécutées.	• Toutes les données du tenant, y compris l'archive d'e-mails, sont définitivement supprimées. Cette action est irréversible.

Plans d'archivage

Avec un plan d'archivage, vous pouvez configurer les e-mails qui seront importés dans l'archive d'e-mails.

L'importation initiale n'affecte que les e-mails qui se trouvaient sur le serveur de messagerie avant que ce serveur ne soit ajouté à la console Cyber Protect.

© Acronis International GmbH, 2003-2026

Après avoir ajouté le serveur de messagerie à la console Cyber Protect, tous les nouveaux e-mails seront automatiquement ajoutés à l'archive. Ce paramètre n'est pas configurable et ne dépend pas de la portée de l'importation initiale.

Vous pouvez appliquer un plan d'archivage à un serveur de messagerie.

Création d'un plan d'archivage

Vous pouvez créer un plan d'archivage lorsque vous ajoutez un nouveau serveur de messagerie à la console Cyber Protect, ou créer un plan d'archivage pour un serveur de messagerie existant sur la console Cyber Protect.

Nouveau serveur de messagerie

Pour créer un plan d'archivage

1. Ajoutez le serveur de messagerie à la console Cyber Protect en suivant les indications de "Ajout d'un serveur de messagerie" (p. 772).
   Un plan d'archivage s'ouvre.
2. [Facultatif] Pour modifier le nom du plan d'achivage, cliquez sur l'icône représentant un crayon, spécifiez un nouveau nom, puis cliquez sur **OK**.
3. Dans **Importer des e-mails existants**, sélectionnez **Toutes les boîtes aux lettres**, puis cliquez sur **Terminé**.
4. Cliquez sur **Chiffrement**, spécifiez et confirmez le mot de passe de chiffrement, puis cliquez sur **Enregistrer**.

   Avertissement !
   Si vous perdez ou oubliez ce mot de passe, vous ne pouvez pas parcourir l'archive d'e-mails ni restaurer les données.

5. Cliquez sur **Créer**.

Serveur de messagerie existant

Prérequis

- Un serveur de messagerie est ajouté à la console Cyber Protect, mais aucun plan d'archivage ne lui est appliqué.

Pour créer un plan d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux**, puis sélectionnez le serveur de messagerie pour lequel vous souhaitez créer un plan.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Protéger**.
4. [Facultatif] Pour modifier le nom du plan d'achivage, cliquez sur l'icône représentant un crayon, spécifiez un nouveau nom, puis cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

5. Dans **Importer des e-mails existants**, sélectionnez **Toutes les boîtes aux lettres**, puis cliquez sur **Terminé**.
6. Cliquez sur **Chiffrement**, spécifiez et confirmez le mot de passe de chiffrement, puis cliquez sur **Enregistrer**.

   Avertissement !
   Si vous perdez ou oubliez ce mot de passe, vous ne pouvez pas parcourir l'archive ni restaurer les données.

7. Cliquez sur **Créer**.

Un plan d'archivage des e-mails est créé et appliqué au serveur de messagerie, et l'archive d'e-mails est créée.

L'importation initiale prend un certain temps, en fonction du champ d'application et de la période d'importation sélectionnés. Tous les nouveaux e-mails sont ajoutés en continu à l'archive, au fur et à mesure de leur envoi ou de leur réception.

Création d'un plan d'archivage

Vous pouvez modifier le nom d'un plan d'archivage.

Pour modifier un plan d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Plans d'archivage des e-mails**.
3. Cliquez sur le nom du plan, puis cliquez sur **Modifier**.
4. Pour modifier le nom du plan, cliquez sur l'icône représentant un crayon, spécifiez un nouveau nom, puis cliquez sur **OK**.
5. Cliquez sur **Enregistrer**.

Création d'un plan d'archivage

Vous pouvez appliquer un plan d'archivage à un serveur de messagerie.

Remarque
Cette opération n'est disponible que si vous n'avez pas encore appliqué de plan d'archivage au serveur de messagerie. Vous ne pouvez appliquer qu'un seul plan d'archivage à un serveur de messagerie.

Pour appliquer un plan d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux** > **Serveurs de messagerie**.

© Acronis International GmbH, 2003-2026

3. Dans l'écran principal, cliquez sur le nom du serveur de messagerie, puis cliquez sur **Protéger**.
4. Sélectionnez un plan d'archivage, puis cliquez sur **Appliquer**.

   Le plan d'archivage des e-mails est appliqué au serveur de messagerie et l'archive d'e-mails est créée.

   L'importation initiale prend un certain temps, en fonction du champ d'application et de la période d'importation sélectionnés. Tous les nouveaux e-mails sont ajoutés en continu à l'archive, au fur et à mesure de leur envoi ou de leur réception.

Révocation d'un plan d'archivage

Vous pouvez révoquer un plan d'archivage sans le supprimer.

Pour révoquer un plan d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Terminaux** > **Serveurs de messagerie**.
3. Dans l'écran principal, cliquez sur le nom du serveur de messagerie.
4. Dans l'onglet **Protéger**, cliquez sur l'icône de points de suspension (...) à côté du nom du plan d'archivage, puis cliquez sur **Révoquer**.

Par conséquent, le plan ne sera plus appliqué au serveur de messagerie et l'archive d'e-mails ne sera plus mise à jour.

Suppression d'un plan d'archivage

Vous pouvez supprimer un plan d'archivage.

Pour supprimer un plan d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage**, puis cliquez sur **Plans d'archivage**.
3. Dans l'écran principal, cliquez sur le nom du plan, puis cliquez sur **Supprimer**.
4. Pour confirmer votre décision, cochez la case, puis cliquez sur **Supprimer**.

En conséquence, le plan d'archivage sera supprimé. L'archive d'e-mails ne sera pas supprimée, mais elle ne sera plus mise à jour.

Importation des e-mails à partir de fichiers PST

Vous pouvez utiliser des fichiers PST pour importer des e-mails dans une archive d'e-mails.

Lors de l'importation, les e-mails dans le fichier PST sont énumérés et des données statistiques sur leurs destinataires sont collectées. Les destinataires les plus fréquents deviennent propriétaires de la boîte aux lettres, pour lesquels une nouvelle boîte aux lettres est créée sous **Toutes les boîtes aux lettres** > **Importé depuis PST** dans la console Cyber Protect. Les e-mails importés sont

© Acronis International GmbH, 2003-2026

regroupés par heure d'importation et par propriétaire de la boîte aux lettres. Les e-mails qui ne peuvent pas être associés à un propriétaire de la boîte aux lettres et les e-mails qui ont des champs « De » ou « À » manquants ou corrompus apparaissent sous **Importé depuis PST** > **Autre**.

Remarque
Les e-mails importés ne sont pas ajoutés aux boîtes aux lettres qui sont archivées. Une boîte aux lettres qui est en cours d'archivage apparaît sous **Toutes les boîtes aux lettres**. Les e-mails importés sont affichés dans des boîtes aux lettres séparées sous **Toutes les boîtes aux lettres** > **Importé depuis PST**.

Limites

- Dans une tâche d'importation, vous pouvez sélectionner des fichiers PST d'un seul compte OneDrive personnel.
  L'importation depuis un compte SharePoint ou un compte OneDrive de groupe n'est pas prise en charge.
- Le temps d'importation dépend de la vitesse de téléchargement autorisée par OneDrive et peut varier considérablement selon les emplacements et les heures de la journée.
- Vous pouvez sélectionner jusqu'à 100 000 fichiers PST ou un dossier contenant des fichiers PST.
  Le dossier sélectionné peut contenir jusqu'à 10 000 sous-dossiers et jusqu'à 100 000 fichiers PST.
- La taille maximale autorisée par fichier PST est de 50 Go.
  Si vous sélectionnez un dossier, les fichiers PST de plus de 50 Go seront ignorés.
- Seuls les e-mails de 200 Mo maximum sont importés.
  Les e-mails, tâches, notes, invitations et autres éléments plus volumineux sont ignorés.
- Les fichiers PST Unicode sont entièrement pris en charge. Les fichiers PST ANSI peuvent ne pas être traités ou peuvent être traités de manière incorrecte.
- La déduplication n'est pas prise en charge.
  Si vous utilisez le même fichier PST deux fois, les e-mails importés seront dupliqués.
- Le formatage de texte enrichi (RTF) ne peut pas être préservé dans le corps d'un e-mail importé.
  Le corps d'un e-mail RTF au format texte brut ou html est préservé. Le corps RFT est joint à l'e-mail importé en tant que fichier `body.rtf` séparé.
- Les pièces jointes OLE en ligne sont importées en tant que pièces jointes d'image avec des noms affectés automatiquement et sans extensions de fichier.
- Aucun mot de passe PST n'est requis lors de l'importation de fichiers PST protégés par mot de passe créés dans Microsoft Outlook.
- Les e-mails importés à partir de fichiers PST ne peuvent être restaurés que vers de nouvelles cibles.

Prérequis

- Vous avez exporté les e-mails requis depuis la solution de messagerie source. Par exemple, cette exportation peut être effectuée dans le cadre d'une migration depuis un autre système d'archivage d'e-mails.

© Acronis International GmbH, 2003-2026

- Vous avez transféré tous les fichiers PST exportés vers le compte OneDrive d'un utilisateur dans votre organisation Microsoft 365. Par exemple, vous pouvez utiliser le compte de l'administrateur qui effectuera l'importation.

Pour importer des e-mails à partir de fichiers PST

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage de sauvegarde** > **Sauvegardes d'applications Cloud**, puis sélectionnez l'archive d'e-mails dans laquelle vous souhaitez importer les e-mails.
3. Cliquez sur **Importer à partir de fichiers PST**.
4. Spécifiez le mot de passe de chiffrement pour l'archive d'e-mails, puis cliquez sur **Poursuivre**.
5. Dans **Organisation**, sélectionnez l'organisation Microsoft 365 source.
   - Si une seule organisation Microsoft 365 est ajoutée à la console Cyber Protect, cette organisation est présélectionnée. Vous pouvez utiliser cette organisation comme source ou en ajouter une nouvelle.
   - [Si plusieurs organisations Microsoft 365 sont ajoutées à la console Cyber Protect] Effectuer les opérations suivantes :
     - Cliquez sur **Sélectionner**, puis sélectionnez l'organisation Microsoft 365 source.
     - Cliquez sur **Sélectionner**.
   - [Si aucune organisation Microsoft 365 n'est ajoutée à la console Cyber Protect] Effectuez les opérations suivantes :
     - Cliquez sur **Sélectionner**, puis sur **Ajouter une organisation**.
     - Sur la page de connexion de Microsoft 365, connectez-vous avec les identifiants d'administrateur global Microsoft 365.

       Microsoft 365 affiche une liste des permissions nécessaires pour sauvegarder et restaurer les données de votre organisation.
     - Confirmez que vous accordez les autorisations requises.
6. Dans **Éléments à importer**, sélectionnez un ou plusieurs fichiers PST ou dossiers contenant des fichiers PST.
   a. Cliquez sur **Sélectionner**.
   b. Sur la page de connexion Microsoft 365, connectez-vous avec les identifiants d'administrateur global de l'organisation Microsoft 365 source.

      Microsoft 365 nécessite les autorisations supplémentaires suivantes :
      - Lire des fichiers dans toutes les collections de sites
      - Lire les profils complets de tous les utilisateurs
      - Lire tous les fichiers auxquels l'utilisateur peut accéder
      - Se connecter et lire le profil utilisateur
   c. Confirmez que vous accordez les autorisations requises.

© Acronis International GmbH, 2003-2026

d. Dans la console Cyber Protect, accédez à OneDrive d'un utilisateur, puis sélectionnez un ou plusieurs fichiers PST.
e. Cliquez sur **Sélectionner**.

7. Cliquez sur **Importer**.
8. Après la fin de l'opération d'importation, vérifiez son résultat.

   Après une importation réussie, les e-mails importés sont affichés sous **Toutes les boîtes aux lettres** > **Importé à partir de PST**.

   Après une importation infructueuse, aucun e-mail importé n'est affiché. Une importation échouée ne reprendra ni ne redémarrera automatiquement.

Requêtes de recherche

Vous pouvez rechercher des e-mails dans l'archive d'e-mails en utilisant des requêtes de recherche, puis enregistrer ces requêtes pour une utilisation ultérieure.

Les requêtes de recherche constituent la base de la création de règles de rétention et de règles de conservation légale.

Vous pouvez lier une requête de recherche enregistrée à une archive d'e-mails spécifique. Une telle requête de recherche ne peut s'exécuter que sur l'archive d'e-mails liée.

Si vous ne liez pas la requête de recherche enregistrée à une archive d'e-mails, elle peut s'exécuter sur n'importe quelle archive d'e-mails. Vous pouvez utiliser des requêtes de recherche non liées dans des règles de rétention et des règles de conservation légale qui sont appliquées à plusieurs archives d'e-mails.

Recherche d'e-mails

Vous pouvez rechercher des e-mails spécifiques à l'aide de requêtes de recherche en texte intégral aux niveaux suivants :

- L'archive d'e-mails (**Tous les e-mails**)
- La boîte aux lettres d'utilisateur
- Le dossier **Entrants** ou **Sortants** d'une boîte aux lettres d'utilisateur

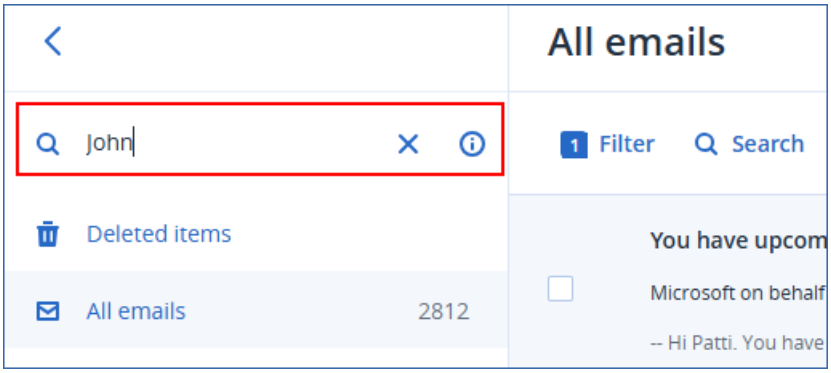
Pour rechercher des e-mails

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Pour rechercher dans une archive dans un stockage immuable] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.

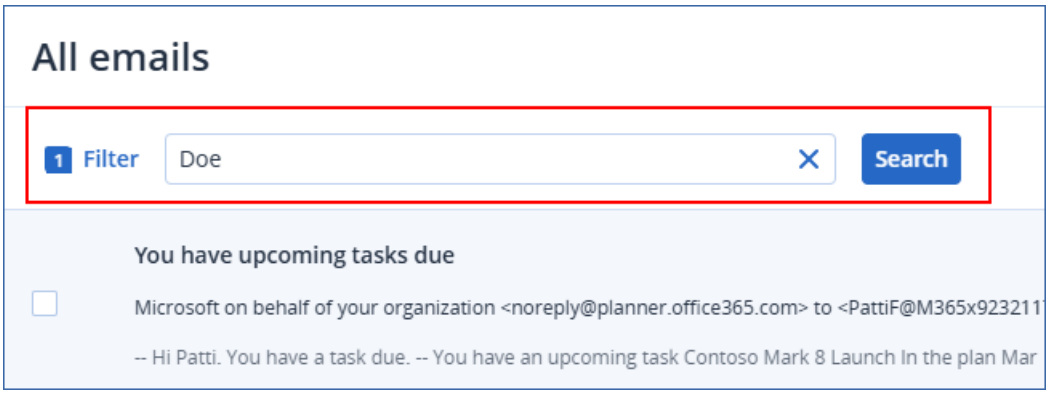
© Acronis International GmbH, 2003-2026

6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. Sélectionnez le niveau sur lequel vous souhaitez effectuer la recherche.

   Vous pouvez sélectionner **Tous les e-mails**, une boîte aux lettres d'utilisateur, ou encore le dossier **Entrants** ou **Sortants** dans une boîte aux lettres d'utilisateur.
8. [Facultatif] Pour rechercher la boîte aux lettres d'un utilisateur spécifique, dans le champ de recherche de la colonne de gauche, saisissez au moins trois caractères du nom de l'utilisateur, puis appuyez sur **Entrée**.



9. Sur l'écran principal, cliquez sur **Recherche**, saisissez votre requête de recherche, puis cliquez sur **Recherche**.



   Vous pouvez utiliser un ou plusieurs mots. Pour rechercher un groupe de mots spécifique, mettez-le entre guillemets. Les caractères génériques ne sont pas pris en charge.

   La recherche est effectuée dans les champs suivants :

   - Du
   - Jusqu'au
   - CC
   - Cci
   - Sujet
   - Corps de l'e-mail
10. [Facultatif] Pour effectuer une recherche dans un champ spécifique uniquement, par exemple **De**, **À/Cc/Cci**, **Objet contient**, ou pour spécifier des critères de recherche supplémentaires, cliquez sur **Filtre**.

© Acronis International GmbH, 2003-2026

a. Configurez vos critères de recherche.

   Par exemple, vous pouvez rechercher uniquement les e-mails comportant des pièces jointes, ou les e-mails envoyés ou reçus à une date spécifique.

b. Dans **Statut de la suppression**, sélectionnez le champ d'application de la recherche.

   La sélection de **Éléments non supprimés** limite la recherche uniquement aux e-mails qui ne sont pas dans un stockage immuable.

   La sélection de **Éléments supprimés** limite la recherche uniquement aux e-mails qui se trouvent dans un stockage immuable.

c. Cliquez sur **Appliquer**.

Les e-mails correspondant à la requête de recherche sont répertoriés.

Vous pouvez enregistrer la requête de recherche pour une utilisation ultérieure. Pour plus d'informations, voir "Création d'une requête de recherche enregistrée" (p. 785).

Tri des e-mails

Vous pouvez trier les e-mails aux niveaux suivants :

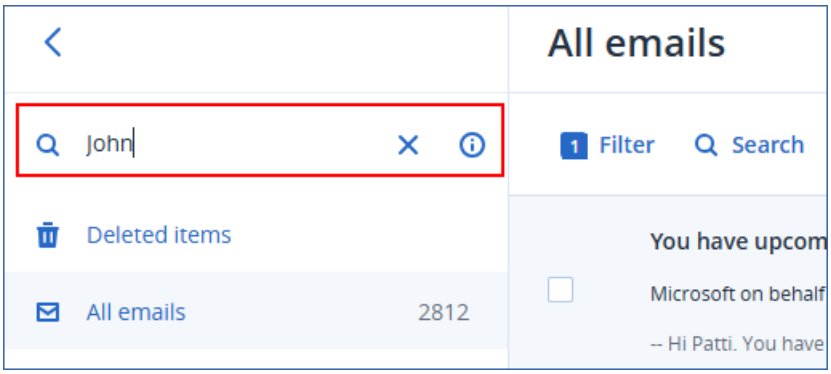
- L'archive d'e-mails (**Tous les e-mails**)
- La boîte aux lettres d'utilisateur
- Le dossier **Entrants** ou **Sortants** d'une boîte aux lettres d'utilisateur

Pour trier les e-mails

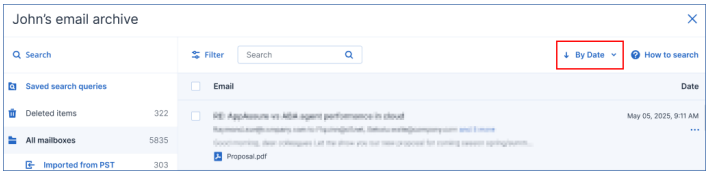
1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Pour trier les e-mails dans une archive en stockage immuable] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. Sélectionnez le niveau auquel vous souhaitez trier les e-mails.

   Vous pouvez sélectionner **Tous les e-mails**, une boîte aux lettres d'utilisateur, ou encore le dossier **Entrants** ou **Sortants** dans une boîte aux lettres d'utilisateur.
8. [Facultatif] Pour rechercher la boîte aux lettres d'un utilisateur spécifique, dans le champ de recherche de la colonne de gauche, saisissez au moins trois caractères du nom de l'utilisateur, puis appuyez sur **Entrée**.

© Acronis International GmbH, 2003-2026



9. Sur l'écran principal, cliquez sur le bouton de tri.



10. Sélectionnez le critère de tri et l'ordre de tri.

Critères de tri	Ordre de tri
Date	Chronologique : Du plus récent au plus ancien, Du plus ancien au plus récent
Sujet	Alphabétique : A–Z, Z-A
Destinataire	Alphabétique : A–Z, Z-A Les e-mails avec plusieurs destinataires sont triés selon le nom du premier destinataire.
Expéditeur	Alphabétique : A–Z, Z-A
Pièces jointes	Avec pièces jointes en haut (du plus récent au plus ancien), Sans pièces jointes en haut (du plus récent au plus ancien)
Pertinence	Disponible uniquement lorsque vous effectuez une recherche ou utilisez une requête de recherche enregistrée. L'algorithme de pertinence met l'accent sur la qualité des correspondances plutôt que sur la quantité en implémentant un système de notation multiniveau. Les correspondances exactes reçoivent le poids le plus élevé et suivent une règle de score maximal - une correspondance exacte peut l'emporter sur de nombreuses correspondances partielles. La diversité des termes uniques est ensuite priorisée, ce qui signifie que le nombre de correspondances de phrases exactes est plus important que la fréquence des correspondances de termes individuels, ce qui aide à réduire l'influence de la répétition des mots-clés. L'horodatage de l'e-mail fonctionne comme un critère de départage lorsque les éléments ont une qualité de correspondance identique. De plus, la longueur du contenu est normalisée pour garantir que les e-mails plus longs ne surpassent pas automatiquement ceux qui sont concis et hautement pertinents.

© Acronis International GmbH, 2003-2026

Création d'une requête de recherche enregistrée

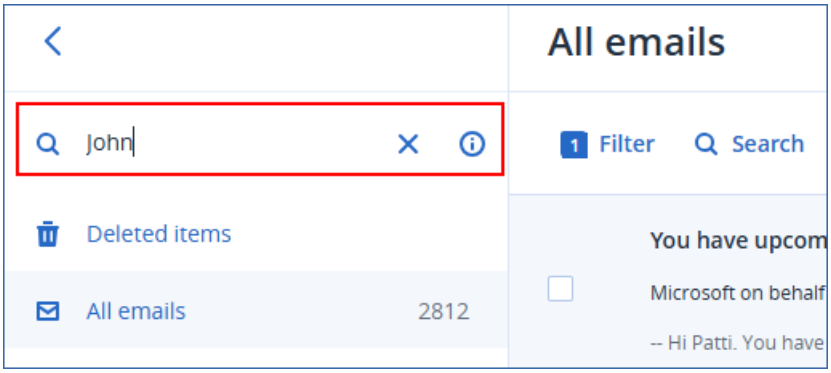
Vous pouvez créer une requête de recherche enregistrée à partir de l'archive d'e-mails ou de l'onglet **Gestion** > **Plans d'archivage**.

Vous pouvez utiliser une requête de recherche enregistrée dans les règles de rétention ou les règles de conservation légale, ou l'exécuter dans l'archive d'e-mails pour trouver les e-mails que vous souhaitez prévisualiser ou restaurer.

Pour créer une requête de recherche enregistrée

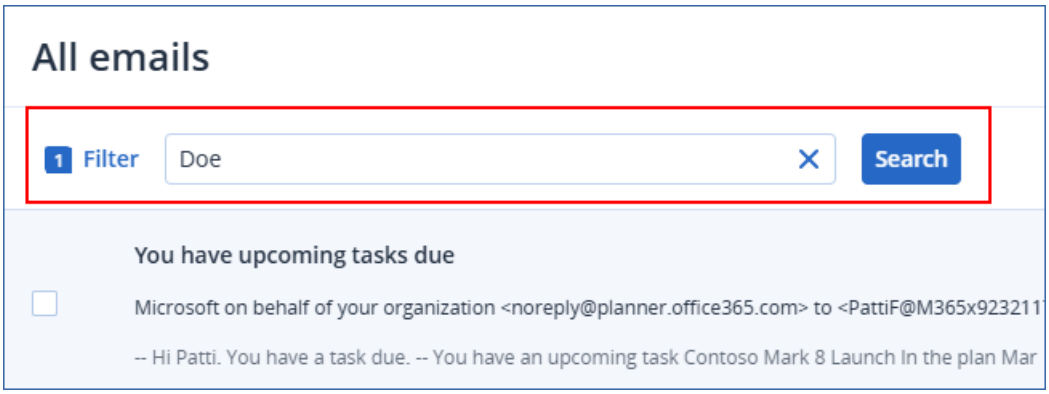
Depuis l'archive d'e-mails

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Pour rechercher dans une archive dans un stockage immuable] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. Sélectionnez le niveau sur lequel vous souhaitez effectuer la recherche.
   Vous pouvez sélectionner **Tous les e-mails**, une boîte aux lettres d'utilisateur, ou encore le dossier **Entrants** ou **Sortants** dans une boîte aux lettres d'utilisateur.
8. [Facultatif] Pour rechercher la boîte aux lettres d'un utilisateur spécifique, dans le champ de recherche de la colonne de gauche, saisissez au moins trois caractères du nom de l'utilisateur, puis appuyez sur **Entrée**.



9. Sur l'écran principal, cliquez sur **Recherche**, saisissez votre requête de recherche, puis cliquez sur **Recherche**.

© Acronis International GmbH, 2003-2026



Vous pouvez utiliser un ou plusieurs mots. Pour rechercher un groupe de mots spécifique, mettez-le entre guillemets. Les caractères génériques ne sont pas pris en charge.

La recherche est effectuée dans les champs suivants :

- Du
- Jusqu'au
- CC
- Cci
- Sujet
- Corps de l'e-mail

10. [Facultatif] Pour effectuer une recherche dans un champ spécifique uniquement, par exemple **De**, **À/Cc/Cci**, **Objet contient**, ou pour spécifier des critères de recherche supplémentaires, cliquez sur **Filtre**.
    a. Configurez vos critères de recherche.

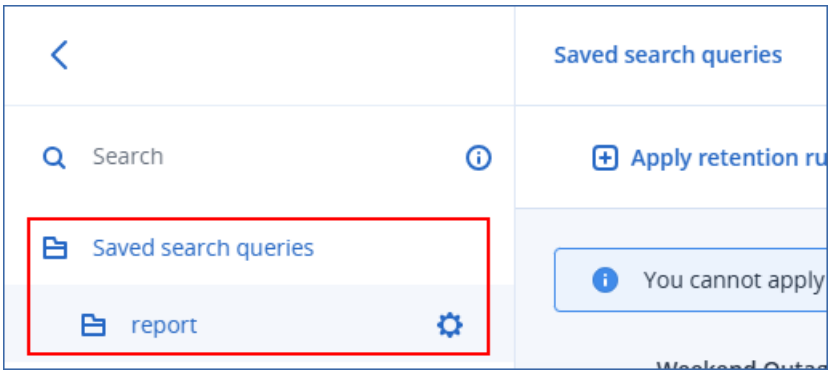
       Par exemple, vous pouvez rechercher uniquement les e-mails comportant des pièces jointes, ou les e-mails envoyés ou reçus à une date spécifique.
    b. Dans **Statut de la suppression**, sélectionnez le champ d'application de la recherche.

       La sélection de **Éléments non supprimés** limite la recherche uniquement aux e-mails qui ne sont pas dans un stockage immuable.

       La sélection de **Éléments supprimés** limite la recherche uniquement aux e-mails qui se trouvent dans un stockage immuable.
    c. Cliquez sur **Appliquer**.
11. Cliquez sur **Enregistrer sous**.
12. Dans **Nom de la requête de recherche**, indiquez un nom.
13. Cliquez sur **Enregistrer**.

En conséquence, une requête de recherche enregistrée est créée et est affichée dans la section **Requêtes de recherche enregistrées**. Les résultats de recherche sont dynamiques et incluent tous les nouveaux e-mails qui correspondent à la requête.

© Acronis International GmbH, 2003-2026



La requête de recherche est liée à cette archive d'e-mails et ne peut être exécutée que sur celle-ci. N'utilisez pas cette requête de recherche dans une règle de rétention ou une règle de conservation légale que vous souhaitez appliquer à une autre archive d'e-mails.

De Gestion > Plans d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Requêtes de recherche**, puis cliquez sur **Créer une requête de recherche**.
3. Dans **Nom de la requête de recherche**, saisissez un nom.
4. [Facultatif] Sélectionnez une archive d'e-mails à laquelle vous souhaitez lier la requête de recherche.

   Si vous sélectionnez une archive d'e-mails, vous pourrez exécuter la requête uniquement sur cette archive.

   Si vous ne sélectionnez pas d'archive d'e-mails, vous pourrez appliquer la requête sur n'importe quelle archive d'e-mails.
5. Dans **Requête de recherche**, spécifiez votre requête de recherche.

   Vous pouvez utiliser un ou plusieurs mots. Pour rechercher un groupe de mots spécifique, mettez-le entre guillemets. Les caractères génériques ne sont pas pris en charge.

   La recherche est effectuée dans les champs suivants :

   - Du
   - Jusqu'au
   - CC
   - Cci
   - Sujet

   Vous pouvez également effectuer une recherche dans ces champs séparément en utilisant les champs **De**, **À/CC/Cci** et **Objet contient**.
6. Dans **Statut de la suppression**, sélectionnez le champ d'application de la recherche.

   La sélection de **Éléments non supprimés** limite la recherche uniquement aux e-mails qui ne sont pas dans un stockage immuable.

   La sélection de **Éléments supprimés** limite la recherche uniquement aux e-mails qui se trouvent dans un stockage immuable.

© Acronis International GmbH, 2003-2026

7. [Facultatif] Spécifiez d'autres critères de recherche.

   Par exemple, vous pouvez rechercher uniquement les e-mails qui ont des pièces jointes, les e-mails qui ont été envoyés ou reçus à une date spécifique ou les e-mails d'une taille spécifique.
8. Cliquez sur **Créer**.

En conséquence, une nouvelle requête de recherche enregistrée est créée. Les résultats de la recherche sont dynamiques et incluent tous les nouveaux e-mails qui correspondent à la requête.

Exécution d'une requête de recherche enregistrée

Vous pouvez exécuter une requête de recherche enregistrée à partir d'une archive d'e-mails ou de l'onglet **Gestion** > **Plans d'archivage**.

Pour créer une requête de recherche enregistrée

Depuis l'archive d'e-mails

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Si vous souhaitez rechercher une archive dans un stockage immuable] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. Sous **Requêtes de recherche enregistrées**, cliquez sur la requête que vous souhaitez exécuter.

Les e-mails correspondant à la requête de recherche sont répertoriés.

De Gestion > Plans d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Requêtes de recherche**.
3. Cliquez sur une requête de recherche, puis cliquez sur **Recherche**.
4. [Si la requête de recherche n'est pas liée à une archive d'e-mails] Sélectionnez une archive d'e-mails, puis cliquez sur **Recherche**.
5. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.

Les e-mails correspondant à la requête de recherche sont répertoriés.

© Acronis International GmbH, 2003-2026

Création d'une requête de recherche enregistrée

Vous pouvez modifier une requête de recherche enregistrée à partir de l'archive d'e-mails ou de l'onglet **Gestion** > **Plans d'archivage**.

Pour modifier une requête de recherche

Depuis l'archive d'e-mails

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Si vous souhaitez rechercher une archive dans un stockage immuable] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. Sous **Requêtes de recherche enregistrées**, cliquez sur l'icône en forme d'engrenage à côté de la requête, puis cliquez sur **Modifier**.
8. Modifiez la requête de recherche, puis cliquez sur **Rechercher**.

Avertissement !
La modification d'une requête de recherche affecte les règles de rétention et les règles de conservation légale dans lesquelles cette requête de recherche est utilisée.

De Gestion > Plans d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Requêtes de recherche**.
3. Cliquez sur une requête de recherche, puis cliquez sur **Modifier**.
4. Modifiez la requête de recherche, puis cliquez sur **Rechercher**.

Avertissement !
La modification d'une requête de recherche affecte les règles de rétention et les règles de conservation légale dans lesquelles cette requête de recherche est utilisée.

Création d'une requête de recherche enregistrée

Vous pouvez supprimer une requête de recherche enregistrée de l'archive d'e-mails ou de l'onglet **Gestion** > **Plans d'archivage**.

Pour supprimer une requête de recherche

© Acronis International GmbH, 2003-2026

Depuis l'archive d'e-mails

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Si vous souhaitez rechercher une archive dans un stockage immuable] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. Sous **Requêtes de recherche enregistrées**, cliquez sur l'icône en forme d'engrenage à côté de la requête, puis cliquez sur **Supprimer**.
8. Pour confirmer votre choix, cliquez sur **Supprimer**.

Avertissement !
La suppression d'une requête de recherche affecte les règles de rétention et les règles de conservation légale dans lesquelles cette requête de recherche est utilisée.

De Gestion > Plans d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Requêtes de recherche**.
3. Cliquez sur une requête de recherche, puis cliquez sur **Supprimer**.
4. Pour confirmer votre choix, cliquez sur **Supprimer**.

Avertissement !
La suppression d'une requête de recherche affecte les règles de rétention et les règles de conservation légale dans lesquelles cette requête de recherche est utilisée.

Règles de rétention

Avec les règles de rétention, vous pouvez configurer la durée de conservation des e-mails dans l'archive d'e-mails.

Les règles de rétention sont basées sur des requêtes de recherche. Les e-mails qui correspondent aux requêtes de recherche sont conservés dans l'archive d'e-mails pendant la période de rétention configurée. À l'expiration de la période de rétention, les e-mails sont automatiquement supprimés. Vous ne pouvez pas supprimer manuellement des e-mails de l'archive d'e-mails.

Vous pouvez utiliser une ou plusieurs requêtes de recherche dans une règle de rétention. Les e-mails qui correspondent à l'une des requêtes de recherche suivront cette règle de rétention.

Vous pouvez appliquer plusieurs plans de protection à la même ressource.

© Acronis International GmbH, 2003-2026

Remarque
Si un e-mail correspond à plus d'une règle de rétention, la règle avec la période de rétention la plus longue est appliquée.

Vous pouvez appliquer une règle de rétention à une ou plusieurs archives d'e-mails. Lorsque vous créez une règle de rétention que vous souhaitez appliquer à plusieurs archives d'e-mails, utilisez des requêtes de recherche enregistrées qui ne sont pas liées à une archive d'e-mails spécifique.

Les règles de rétention s'exécutent sur leurs archives d'e-mails une fois toutes les 24 heures. Cette opération n'est pas configurable par l'utilisateur.

Création d'une règle de rétention

Vous pouvez créer une règle de rétention à partir de l'archive d'e-mails ou de l'onglet **Gestion** > **Plans d'archivage**.

Les règles de rétention créées à partir de l'archive d'e-mails peuvent utiliser une seule requête de recherche et une seule archive d'e-mails.

Les règles de rétention créées à partir de l'onglet **Gestion** > **Plans d'archivage** peuvent utiliser plusieurs requêtes de recherche et plusieurs archives d'e-mails.

Pour créer une règle de rétention

Depuis l'archive d'e-mails

1. Exécutez une requête de recherche sur l'archive d'e-mails, comme décrit dans "Exécution d'une requête de recherche enregistrée" (p. 788).
2. Au-dessus de la liste des e-mails correspondants, cliquez sur **Appliquer la règle de rétention**.
3. [S'il existe des règles de rétention] Dans la fenêtre **Appliquer la règle de rétention à la requête de recherche**, cliquez sur **Créer une règle de rétention**.
4. [Facultatif] Pour modifier le nom de la règle de rétention, cliquez sur l'icône en forme de crayon, saisissez un nouveau nom, puis cliquez sur **OK**.
5. Dans **Période de rétention**, sélectionnez une option.
   a. [Si vous sélectionnez **Par ancienneté d'e-mail**] Spécifiez la période et sélectionnez l'unité de temps.
   b. Cliquez sur **Enregistrer**.

   Par exemple, vous pouvez spécifier 1 an, 2 mois ou 300 jours. Les e-mails plus anciens que la période sélectionnée seront supprimés de l'archive. L'âge de l'e-mail est calculé en fonction de la date d'envoi ou de réception de chaque e-mail.
6. Dans **Mot de passe de chiffrement pour les archives**, spécifiez le mot de passe de chiffrement pour l'archive d'e-mails, puis cliquez sur **Poursuivre**.
7. Cliquez sur **Créer**.

   En conséquence, une règle de rétention est créée.

© Acronis International GmbH, 2003-2026

Les e-mails qui correspondent à l'une des requêtes de recherche de cette règle de rétention seront supprimés lorsque la période de rétention prendra fin.

Remarque
Si un e-mail correspond à plus d'une règle de rétention, la règle avec la période de rétention la plus longue est appliquée.

De Gestion > Plans d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de rétention**, puis cliquez sur **Créer une règle de rétention**.
3. [Facultatif] Pour modifier le nom de la règle de rétention, cliquez sur l'icône en forme de crayon, saisissez un nouveau nom, puis cliquez sur **OK**.
4. Dans **Archives d'e-mails**, sélectionnez les archives d'e-mails auxquelles les règles de rétention s'appliqueront.
   a. Cliquez sur **Sélectionner**.
   b. Sélectionnez une ou plusieurs archives d'e-mails.
   c. Cliquez sur **Sélectionner**.
5. Dans **Période de rétention**, sélectionnez une option.
   a. [Si vous sélectionnez **Par ancienneté d'e-mail**] Spécifiez la période et sélectionnez l'unité de temps.
   b. Cliquez sur **Enregistrer**.

   Par exemple, vous pouvez spécifier 1 an, 2 mois ou 300 jours. Les e-mails plus anciens que la période sélectionnée seront supprimés de l'archive. L'âge de l'e-mail est calculé en fonction de la date d'envoi ou de réception de chaque e-mail.
6. Dans **Requêtes de recherche enregistrées**, sélectionnez les requêtes de recherche sur lesquelles cette règle de rétention sera basée.
   a. Cliquez sur **Sélectionner**.
   b. [Pour créer une nouvelle requête de recherche] Cliquez sur **Créer une requête de recherche**, puis créez la requête comme décrit dans "Création d'une requête de recherche enregistrée" (p. 785).
   c. Sélectionnez une ou plusieurs requêtes de recherche.

      Remarque
      Lorsque vous créez une règle de rétention que vous souhaitez appliquer à plusieurs archives d'e-mails, utilisez des requêtes de recherche enregistrées qui ne sont pas liées à une archive d'e-mails spécifique.

   d. Cliquez sur **Sélectionner**.
7. Dans **Mot de passe de chiffrement pour les archives**, spécifiez le mot de passe de

© Acronis International GmbH, 2003-2026

chiffrement pour les archives d'e-mails sélectionnées, puis cliquez sur **Poursuivre**.

8. Cliquez sur **Créer**.

En conséquence, une règle de rétention est créée.

Les e-mails qui correspondent à l'une des requêtes de recherche de cette règle de rétention seront supprimés lorsque la période de rétention prendra fin.

Remarque
Si un e-mail correspond à plus d'une règle de rétention, la règle avec la période de rétention la plus longue est appliquée.

Modification d'une règle de rétention

Vous pouvez modifier une règle de rétention.

Pour modifier une règle de rétention

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de rétention**.
3. lectionnez une règle de rétention, puis cliquez sur **Modifier**.
4. Modifiez la règle de rétention, puis cliquez sur **Enregistrer**.

En conséquence, la règle de rétention est modifiée. Les paramètres mis à jour seront appliqués à l'archive d'e-mails lors de la prochaine exécution de la règle de rétention.

Les règles de rétention s'exécutent sur leurs archives d'e-mails une fois toutes les 24 heures. Cette opération n'est pas configurable par l'utilisateur.

Activation d'une règle de rétention

Une règle de rétention est automatiquement activée lorsque vous la créez.

Vous pouvez activer manuellement une règle de rétention que vous avez désactivée précédemment.

Pour activer une règle de rétention

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de rétention**.
3. Sélectionnez la case à cocher à côté du nom d'une règle de rétention désactivée, puis cliquez sur **Activer**.
4. Pour confirmer votre choix, cliquez sur **Activer**.

En conséquence, la règle de rétention est activée et sera appliquée à l'archive d'e-mails lors de la prochaine exécution.

© Acronis International GmbH, 2003-2026

Les règles de rétention s'exécutent sur leurs archives d'e-mails une fois toutes les 24 heures. Cette opération n'est pas configurable par l'utilisateur.

Désactivation d'une règle de rétention

Une règle de rétention désactivée n'est pas appliquée à l'archive d'e-mails. La règle de rétention désactivée n'est pas supprimée et vous pouvez l'activer ultérieurement.

Pour désactiver une règle de rétention

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de rétention**.
3. Sélectionnez la case à cocher à côté du nom d'une règle de rétention, puis cliquez sur **Désactiver**.
4. Pour confirmer votre choix, cliquez sur **Désactiver**.

En conséquence, la règle de rétention ne sera plus appliquée à l'archive d'e-mails.

Suppression d'une règle de rétention

Vous pouvez supprimer une règle de rétention.

Pour supprimer une règle de rétention

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de rétention**.
3. Sélectionnez une règle de rétention, puis cliquez sur **Supprimer**.
4. Pour confirmer votre choix, cochez la case, puis cliquez sur **Supprimer**.

En conséquence, la règle de rétention est supprimée et ne sera plus appliquée à l'archive d'e-mails.

Règles de conservation légale

Avec les règles de conservation légale, vous pouvez remplacer les règles de rétention et empêcher la suppression des e-mails.

Les règles de conservation légale sont basées sur des requêtes de recherche. Les e-mails qui correspondent aux requêtes de recherche sont protégés contre la suppression pendant la durée légale de conservation. Une fois la durée légale de conservation terminée, ces e-mails peuvent être supprimés par une règle de rétention.

Vous pouvez utiliser une ou plusieurs requêtes de recherche dans une règle de conservation légale. Les e-mails qui correspondent à l'une des requêtes de recherche suivront cette règle de conservation légale.

Vous pouvez appliquer plusieurs règles de conservation légale à la même archive.

© Acronis International GmbH, 2003-2026

Remarque
Si un e-mail correspond à plus d'une règle de conservation légale, la règle avec la durée légale de conservation la plus longue est appliquée.

Vous pouvez appliquer une règle de conservation légale à une ou plusieurs archives d'e-mails. Lorsque vous créez une règle de conservation légale que vous souhaitez appliquer à plusieurs archives d'e-mails, utilisez des requêtes de recherche enregistrées qui ne sont pas liées à une archive d'e-mails spécifique.

Les règles de conservation légale s'exécutent une fois toutes les 24 heures. Cette opération n'est pas configurable par l'utilisateur.

Création d'une règle de conservation légale

Vous pouvez créer une règle de conservation légale à partir de l'archive d'e-mails ou de l'onglet **Gestion** > **Plans d'archivage**.

Les règles de conservation légale créées à partir de l'archive d'e-mails peuvent utiliser une seule requête de recherche et une seule archive d'e-mails.

Les règles de conservation légale créées à partir de l'onglet **Gestion** > **Plans d'archivage** peuvent utiliser plusieurs requêtes de recherche et plusieurs archives d'e-mails.

Pour créer une règle de conservation légale

Depuis l'archive d'e-mails

1. Exécutez une requête de recherche sur l'archive d'e-mails, comme décrit dans "Exécution d'une requête de recherche enregistrée" (p. 788).
2. Au-dessus de la liste des e-mails correspondants, cliquez sur **Appliquer la règle de conservation légale**.
3. [S'il existe des règles de conservation légale] Dans la fenêtre **Appliquer la règle de conservation légale à la requête de recherche**, cliquez sur **Créer une règle de conservation légale**.
4. [Facultatif] Pour changer le nom de la règle de conservation légale, cliquez sur l'icône en forme de crayon, indiquez un nouveau nom, puis cliquez sur **OK**.
5. Dans **Durée légale de conservation**, sélectionnez une option.
   a. [Si vous sélectionnez **Date limite de conservation**] Sélectionnez une date.
   b. Cliquez sur **Enregistrer**.

   Les e-mails qui correspondent à cette règle de conservation légale seront protégés contre la suppression jusqu'à cette date, y compris.
6. Dans **Mot de passe de chiffrement pour les archives**, spécifiez le mot de passe de chiffrement pour l'archive d'e-mails, puis cliquez sur **Poursuivre**.
7. Cliquez sur **Créer**.
   En conséquence, une règle de conservation légale est créée.

© Acronis International GmbH, 2003-2026

Les e-mails qui correspondent à l'une des requêtes de recherche de cette règle de conservation légale seront protégés contre la suppression jusqu'à la fin de la durée légale de conservation.

Remarque
Si un e-mail correspond à plus d'une règle de conservation légale, la règle avec la durée légale de conservation la plus longue est appliquée.

De Gestion > Plans d'archivage

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de conservation légale**, puis cliquez sur **Créer une règle de conservation légale**.
3. [Facultatif] Pour changer le nom de la règle de conservation légale, cliquez sur l'icône en forme de crayon, indiquez un nouveau nom, puis cliquez sur **OK**.
4. Dans **Archives d'e-mails**, sélectionnez les archives d'e-mails auxquelles les règles de rétention s'appliqueront.
   a. Cliquez sur **Sélectionner**.
   b. Sélectionnez une ou plusieurs archives d'e-mails.
   c. Cliquez sur **Sélectionner**.
5. Dans **Durée légale de conservation**, sélectionnez une option.
   a. [Si vous sélectionnez **Date limite de conservation**] Sélectionnez une date.
   b. Cliquez sur **Enregistrer**.

   Les e-mails qui correspondent à cette règle de conservation légale seront protégés contre la suppression jusqu'à cette date, y compris.
6. Dans **Requêtes de recherche enregistrées**, sélectionnez les requêtes de recherche sur lesquelles cette règle de rétention sera basée.
   a. Cliquez sur **Sélectionner**.
   b. [Pour créer une nouvelle requête de recherche] Cliquez sur **Créer une requête de recherche**, puis créez la requête comme décrit dans "Création d'une requête de recherche enregistrée" (p. 785).
   c. Sélectionnez une ou plusieurs requêtes de recherche.

      Remarque
      Lorsque vous créez une règle de conservation légale que vous souhaitez appliquer à plusieurs archives d'e-mails, utilisez des requêtes de recherche qui ne sont pas liées à une archive d'e-mails spécifique.

   d. Cliquez sur **Sélectionner**.
7. Dans **Mot de passe de chiffrement pour les archives**, spécifiez le mot de passe de chiffrement pour les archives d'e-mails sélectionnées, puis cliquez sur **Poursuivre**.
8. Cliquez sur **Créer**.

© Acronis International GmbH, 2003-2026

En conséquence, une règle de conservation légale est créée.

Les e-mails qui correspondent à l'une des requêtes de recherche de cette règle de conservation légale seront protégés contre la suppression jusqu'à la fin de la durée légale de conservation.

Remarque
Si un e-mail correspond à plus d'une règle de conservation légale, la règle avec la durée légale de conservation la plus longue est appliquée.

Modification d'une règle de conservation légale

Vous pouvez modifier une règle de conservation légale.

Pour modifier une règle de conservation légale

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de conservation légale**.
3. Sélectionnez une règle de conservation légale, puis cliquez sur **Modifier**.
4. Modifiez la règle de conservation légale, puis cliquez sur **Enregistrer**.

En conséquence, la règle de conservation légale est modifiée. Les paramètres mis à jour seront appliqués à l'archive d'e-mails la prochaine fois que la règle de conservation légale sera exécutée.

Les règles de conservation légale s'exécutent une fois toutes les 24 heures. Cette opération n'est pas configurable par l'utilisateur.

Ajouter une règle de conservation légale

Une règle de conservation légale est automatiquement activée lorsque vous la créez.

Vous pouvez activer manuellement une règle de conservation légale que vous avez précédemment désactivée.

Pour activer une règle de conservation légale

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de conservation légale**.
3. Sélectionnez la case à cocher à côté du nom d'une règle de conservation légale désactivée, puis cliquez sur **Activer**.
4. Pour confirmer votre choix, cliquez sur **Activer**.

En conséquence, la règle de conservation légale est activée et sera appliquée à l'archive d'e-mails lors de la prochaine exécution.

Les règles de conservation légale s'exécutent une fois toutes les 24 heures. Cette opération n'est pas configurable par l'utilisateur.

© Acronis International GmbH, 2003-2026

Désactiver une règle de conservation légale

Une règle de conservation légale désactivée n'est pas appliquée à l'archive d'e-mails. La règle de conservation légale désactivée n'est pas supprimée et vous pouvez l'activer ultérieurement.

Pour désactiver une règle de conservation légale

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de conservation légale**.
3. Sélectionnez la case à cocher à côté du nom d'une règle de conservation légale, puis cliquez sur **Désactiver**.
4. Pour confirmer votre choix, cliquez sur **Désactiver**.

En conséquence, la règle de conservation légale ne sera plus appliquée à l'archive d'e-mails.

Supprimer la règle de conservation légale

Vous pouvez supprimer une règle de conservation légale.

Pour supprimer une règle de conservation légale

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans d'archivage** > **Règles de conservation légale**.
3. Sélectionnez une règle de conservation légale, puis cliquez sur **Supprimer**.
4. Pour confirmer votre choix, cochez la case, puis cliquez sur **Supprimer**.

En conséquence, la règle de conservation légale est supprimée et ne sera plus appliquée à l'archive d'e-mails.

Restauration de données à partir d'une archive d'e-mails

Prévisualisation des e-mails

Vous pouvez prévisualiser des e-mails archivés sans les restaurer au préalable.

Pour prévisualiser des e-mails

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage de sauvegarde** > **Sauvegardes d'applications dans le cloud**, puis sélectionnez l'archive d'e-mails dans laquelle effectuer la recherche.
3. Cliquez sur **Parcourir l'archive**.
4. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
5. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.

© Acronis International GmbH, 2003-2026

6. Recherchez les e-mails que vous souhaitez prévisualiser.

   Vous pouvez utiliser des requêtes de recherche ponctuelles et des requêtes de recherche enregistrées. Pour plus d'informations, voir "Recherche d'e-mails" (p. 781).
7. Sélectionnez l'e-mail que vous souhaitez prévisualiser.

L'e-mail s'affiche et vous pouvez vérifier son contenu et ses métadonnées.

Restauration d'e-mails, de dossiers et de boîtes aux lettres

Vous pouvez restaurer des e-mails, des dossiers et des boîtes aux lettres dans la boîte aux lettres d'origine ou dans une autre boîte aux lettres.

E-mails

Pour restaurer des bases de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage de sauvegarde** > **Sauvegardes d'applications dans le cloud**, puis sélectionnez l'archive d'e-mails à partir de laquelle vous souhaitez restaurer des données.
3. Cliquez sur **Parcourir l'archive**.
4. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
5. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
6. [Facultatif] Recherchez les e-mails que vous souhaitez restaurer.

   Vous pouvez utiliser des requêtes de recherche ponctuelles et des requêtes de recherche enregistrées. Pour plus d'informations, voir "Recherche d'e-mails" (p. 781).
7. Sélectionnez les e-mails que vous souhaitez restaurer, puis cliquez sur **Restaurer les e-mails**.
8. [Si plusieurs serveurs de messagerie sont ajoutés à la console Cyber Protect] Sélectionnez l'organisation dans laquelle vous souhaitez restaurer les données.
   a. Dans **Organisation**, cliquez sur **Sélectionner**.
   b. Sélectionnez l'organisation, puis cliquez sur **Sélectionner**.
9. Dans **Emplacement de restauration**, sélectionnez la boîte aux lettres dans laquelle vous souhaitez restaurer les e-mails.
10. [Si vous avez sélectionné **Autre boîte aux lettres**] Sélectionnez la boîte aux lettres cible.
    a. Dans **Restaurer vers**, cliquez sur **Sélectionner**.
    b. Sélectionnez la boîte aux lettres cible, puis cliquez sur **Sélectionner**.
11. Cliquez sur **Démarrer la restauration**.

Les e-mails entrants de la boîte aux lettres sélectionnée sont restaurés dans le dossier **Boîte de réception** de la boîte aux lettres cible, et les e-mails sortants de la boîte aux lettres sélectionnée sont restaurés dans le dossier **Envoyés** de la boîte aux lettres cible.

Dossiers

© Acronis International GmbH, 2003-2026

Pour restaurer un dossier

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage de sauvegarde** > **Sauvegardes d'applications dans le cloud**, puis sélectionnez l'archive d'e-mails à partir de laquelle vous souhaitez restaurer des données.
3. Cliquez sur **Parcourir l'archive**.
4. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
5. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
6. Sélectionnez le dossier **Entrants** ou **Sortants** que vous souhaitez restaurer, puis cliquez sur **Restaurer le dossier**.
7. [Si plusieurs serveurs de messagerie sont ajoutés à la console Cyber Protect] Sélectionnez l'organisation dans laquelle vous souhaitez restaurer les données.
   a. Dans **Organisation**, cliquez sur **Sélectionner**.
   b. Sélectionnez l'organisation, puis cliquez sur **Sélectionner**.
8. Dans **Emplacement de restauration**, sélectionnez la boîte aux lettres dans laquelle vous souhaitez restaurer les données.
9. [Si vous avez sélectionné **Autre boîte aux lettres**] Sélectionnez la boîte aux lettres cible.
   a. Dans **Restaurer vers**, cliquez sur **Sélectionner**.
   b. Sélectionnez la boîte aux lettres cible, puis cliquez sur **Sélectionner**.
10. Cliquez sur **Démarrer la restauration**.

Les e-mails entrants de la boîte aux lettres sélectionnée sont restaurés dans le dossier **Boîte de réception** de la boîte aux lettres cible, et les e-mails sortants de la boîte aux lettres sélectionnée sont restaurés dans le dossier **Envoyés** de la boîte aux lettres cible.

Boîtes aux lettres

Pour restaurer une boîte aux lettres

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage de sauvegarde** > **Sauvegardes d'applications dans le cloud**, puis sélectionnez l'archive d'e-mails à partir de laquelle vous souhaitez restaurer des données.
3. Cliquez sur **Parcourir l'archive**.
4. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
5. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
6. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer les e-mails de l'utilisateur**.

© Acronis International GmbH, 2003-2026

7. [Si plusieurs serveurs de messagerie sont ajoutés à la console Cyber Protect] Sélectionnez l'organisation dans laquelle vous souhaitez restaurer les données.
   a. Dans **Organisation**, cliquez sur **Sélectionner**.
   b. Sélectionnez l'organisation, puis cliquez sur **Sélectionner**.
8. Dans **Emplacement de restauration**, sélectionnez la boîte aux lettres dans laquelle vous souhaitez restaurer les données.
9. [Si vous avez sélectionné **Autre boîte aux lettres**] Sélectionnez la boîte aux lettres cible.
   a. Dans **Restaurer vers**, cliquez sur **Sélectionner**.
   b. Sélectionnez la boîte aux lettres cible, puis cliquez sur **Sélectionner**.
10. Cliquez sur **Démarrer la restauration**.

Les e-mails entrants de la boîte aux lettres sélectionnée sont restaurés dans le dossier **Boîte de réception** de la boîte aux lettres cible, et les e-mails sortants de la boîte aux lettres sélectionnée sont restaurés dans le dossier **Envoyés** de la boîte aux lettres cible.

Envoi d'e-mails archivés

Vous pouvez sélectionner jusqu'à 10 e-mails dans une archive d'e-mails et les envoyer aux destinataires de votre choix.

Pour envoyer des e-mails archivés

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Effectuez une recherche dans l'archive d'e-mails ou utilisez une requête de recherche enregistrée.
   Pour en savoir plus, consultez "Recherche d'e-mails" (p. 781) et "Création d'une requête de recherche enregistrée" (p. 785).
3. Sélectionnez jusqu'à 10 e-mails, puis cliquez sur **Envoyer sous forme de message électronique**.
4. [Si plusieurs organisations sont enregistrées] Sélectionnez une organisation.
5. Cliquez sur le champ **Expéditeur**, puis sélectionnez l'utilisateur au nom duquel les e-mails seront envoyés.
   Le nom de cet utilisateur apparaît dans le champ **De** des e-mails.
6. Dans **Destinataires**, saisissez une ou plusieurs adresses e-mail auxquelles vous souhaitez envoyer les e-mails sélectionnés.
   Si vous spécifiez plusieurs adresses e-mail, séparez-les par une virgule ou un point-virgule.
7. [Facultatif] Ajoutez une description qui sera ajoutée en haut de tous les e-mails envoyés.
8. Cliquez sur **Envoyer**.

Par conséquent, les e-mails sélectionnés seront envoyés comme des e-mails individuels aux adresses e-mail que vous avez spécifiées.

© Acronis International GmbH, 2003-2026

Téléchargement de pièces jointes

Vous pouvez télécharger les pièces jointes d'un ou de plusieurs e-mails dans l'archive.

Pour télécharger des pièces jointes

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage de sauvegarde** > **Sauvegardes d'applications dans le cloud**, puis sélectionnez l'archive d'e-mails.
3. Cliquez sur **Parcourir l'archive**.
4. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
5. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
6. [Facultatif] Recherchez les e-mails avec les pièces jointes que vous souhaitez télécharger.
   Vous pouvez utiliser des requêtes de recherche ponctuelles et des requêtes de recherche enregistrées. Pour plus d'informations, voir "Recherche d'e-mails" (p. 781).
7. Sélectionnez les e-mails avec les pièces jointes que vous souhaitez télécharger, puis cliquez sur **Télécharger les pièces jointes**.

Les pièces jointes des e-mails sélectionnés sont téléchargées sur votre ordinateur.

Lorsque vous téléchargez plusieurs éléments, les pièces jointes sont téléchargées sous forme de fichier ZIP.

Stockage immuable pour l'archivage des e-mails

Avec le stockage immuable, vous pouvez accéder aux éléments supprimés suivants pendant la période de rétention du stockage immuable :

- Messages e-mail qui ont été supprimés automatiquement par les règles de rétention.
- Les archives d'e-mails qui ont été supprimées par un administrateur, ainsi que les messages e-mail dans ces archives.

Vous pouvez parcourir et rechercher les messages e-mail supprimés, les restaurer et annuler leur suppression.

Vous ne pouvez pas appliquer de règles de rétention et de règles de conservation légale à des e-mails supprimés.

Après la fin de la période de rétention, les éléments du stockage immuable sont supprimés définitivement. Pour plus d'informations, voir "Stockage immuable" (p. 1617).

Annuler la suppression d'e-mails dans le stockage immuable

Vous pouvez annuler la suppression des e-mails qui se trouvent dans le stockage immuable et les restaurer dans l'archive d'e-mails.

© Acronis International GmbH, 2003-2026

Remarque
Vous pouvez annuler la suppression d'e-mails individuels. L'annulation de la suppression d'archives d'e-mails n'est pas prise en charge.

Pour annuler la suppression

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes d'applications dans le cloud**.
3. [Si l'archive de tous les e-mails est supprimée] Cliquez sur **Afficher les éléments supprimés**.
4. Sélectionnez une archive d'e-mails, puis cliquez sur **Parcourir l'archive**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Dans la boîte de dialogue **Mot de passe de chiffrement**, spécifiez le mot de passe, puis cliquez sur **Poursuivre**.
7. [Facultatif] Recherchez des e-mails spécifiques à l'aide du champ de recherche. Pour plus d'informations, voir "Recherche d'e-mails" (p. 781).
   Vous pouvez également utiliser une requête de recherche qui inclut les éléments supprimés. Pour plus d'informations, voir "Création d'une requête de recherche enregistrée" (p. 785).
8. Sélectionnez jusqu'à 10 e-mails supprimés, puis cliquez sur **Annuler la suppression**.

Les e-mails sélectionnés ne seront donc plus marqués comme supprimés et seront restaurés dans l'archive d'e-mails.

Protection d'applications Microsoft

Protection des serveurs Microsoft SQL Server et Microsoft Exchange Server

Remarque
La sauvegarde de Microsoft SQL n'est prise en charge que pour les bases de données fonctionnant sur les systèmes de fichiers NFTS, REFS et FAT32. ExFat n'est pas pris en charge.

Il existe deux méthodes de protection pour les applications Microsoft :

- **Sauvegarde de base de données**
  Il s'agit d'une sauvegarde des bases de données et des métadonnées associées. Les bases de données peuvent être restaurées sur une application active ou en tant que fichiers.
- **Sauvegarde reconnaissant les applications**
  Il s'agit d'une sauvegarde de niveau disque qui collecte également les métadonnées des applications. Ces métadonnées permettent l'exploration et la restauration des données de l'application sans restaurer la totalité du disque ou du volume. Le disque et le volume peuvent

© Acronis International GmbH, 2003-2026

également être restaurés intégralement. Cela signifie qu'une seule solution et un seul plan de protection peuvent être utilisés à la fois à des fins de reprise d'activité après sinistre et de protection des données.

Pour Microsoft Exchange Server, vous pouvez choisir **Sauvegarde de boîte de réception**. Il s'agit d'une sauvegarde de boîtes aux lettres individuelles via le protocole Services web Exchange. La ou les boîtes aux lettres peuvent être restaurée(s) sur Exchange Server en temps réel ou sur Microsoft 365. La sauvegarde des boîtes aux lettres est prise en charge pour Microsoft Exchange Server 2010 Service Pack 1 (SP1) et version ultérieure.

Protection de Microsoft SharePoint

Une batterie de serveurs Microsoft SharePoint contient des serveurs frontaux qui exécutent des services SharePoint, des serveurs de bases de données qui exécutent Microsoft SQL Server, et (facultativement) des serveurs d'applications qui déchargent certains services SharePoint des serveurs frontaux. Certains serveurs d'applications et serveurs frontaux peuvent être identiques l'un à l'autre.

Pour protéger une batterie de serveurs SharePoint dans son intégralité :

- Sauvegardez tous les serveurs de bases de données avec une sauvegarde reconnaissant les applications.
- Sauvegardez tous les serveurs d'applications et les serveurs frontaux uniques avec une sauvegarde de niveau disque habituelle.

Les sauvegardes de tous les serveurs doivent être effectuées en utilisant la même planification.

Pour protéger le contenu uniquement, vous pouvez sauvegarder les bases de données de contenu séparément.

Protection d'un contrôleur de domaine

Une machine exécutant les services de domaine Active Directory peut être protégée par une sauvegarde reconnaissant les applications. Si un domaine comprend plusieurs contrôleurs de domaine et que vous en restaurez un, une restauration ne faisant pas autorité est effectuée et une restauration USN n'a pas lieu par la suite.

Restauration d'applications

Le tableau suivant résume les méthodes de restauration d'applications disponibles.

	À partir d'une sauvegarde de base de données	**À partir d'une sauvegarde reconnaissant les applications**	**À partir d'une sauvegarde de disque**
Microsoft SQL Server	Bases de données sur une instance SQL Server distante active	Toute la machine Bases de données sur une	Toute la machine

© Acronis International GmbH, 2003-2026

	Bases de données en tant que fichiers	instance SQL Server distante active Bases de données en tant que fichiers	
Microsoft Exchange Server	Bases de données sur un serveur Exchange actif Bases de données en tant que fichiers Restauration granulaire sur un serveur Exchange ou Microsoft 365*	Toute la machine Bases de données sur un serveur Exchange actif Bases de données en tant que fichiers Restauration granulaire sur un serveur Exchange ou Microsoft 365*	Toute la machine
Serveurs de bases de données Microsoft SharePoint	Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers Restauration granulaire avec SharePoint Explorer	Toute la machine Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers Restauration granulaire avec SharePoint Explorer	Toute la machine
Serveurs Web frontaux Microsoft SharePoint	-	-	Toute la machine
Services de domaine Active Directory	-	Toute la machine	-

* La restauration granulaire est également disponible à partir d'une sauvegarde de boîte aux lettres. La restauration d'éléments de données Exchange vers Microsoft 365, et inversement, est prise en charge à la condition que l'agent pour Microsoft 365 soit installé localement.

Exigences supplémentaires pour les sauvegardes reconnaissant les applications

Avant de configurer l'application de sauvegarde, assurez-vous que les exigences répertoriées ci-dessous sont remplies.

Pour vérifier l'état des enregistreurs VSS, utilisez la commande `vssadmin list writers`.

Exigences communes

Pour Microsoft SQL Server, assurez-vous que :

© Acronis International GmbH, 2003-2026

- Au moins une instance de Microsoft SQL Server est démarrée.
- L'enregistreur SQL pour VSS est activé.

Pour Microsoft Exchange Server, assurez-vous que :

- le service Microsoft Exchange Information Store est démarré.
- Windows PowerShell est installé. Pour Exchange 2010 ou version ultérieure, la version de Windows PowerShell doit être au moins la 2.0.
- Microsoft .NET Framework est installé.

  Pour Exchange 2007, la version de Microsoft .NET Framework doit être au moins la 2.0.

  Pour Exchange 2010 ou version ultérieure, la version de Microsoft .NET Framework doit être au moins la 3.5.
- L'enregistreur Exchange pour VSS est activé.

Remarque
L'agent pour Exchange requiert un stockage temporaire pour fonctionner. Par défaut, les fichiers temporaires sont situés dans `%ProgramData%\Acronis\Temp`. Veillez à disposer à l'emplacement du dossier `%ProgramData%` d'au moins autant d'espace que 15 % de la taille d'une base de données Exchange. Sinon, modifiez l'emplacement des fichiers temporaires avant la création des sauvegardes Exchange, comme décrit dans Changing Temp Files and Folder Location (40040).

Sur un contrôleur de domaine, assurez-vous que :

- L'enregistreur Active Directory pour VSS est activé.

Lors de la création d'un plan de protection, procédez aux vérifications suivantes :

- Pour les machines physiques et les machines sur lesquelles l'agent est installé, l'option de sauvegarde Service de cliché instantané des volumes (VSS) est activée.
- Pour les machines virtuelles, l'option de sauvegarde Service de cliché instantané des volumes (VSS) pour les machines virtuelles est activée.

Exigences supplémentaires pour les sauvegardes reconnaissant les applications

Lors de la création d'un plan de protection, assurez-vous que l'option **Tout l'ordinateur** est sélectionnée pour la sauvegarde. L'option de sauvegarde **Secteur par secteur** doit être désactivée dans un plan de protection. Dans le cas contraire, il sera impossible d'exécuter la restauration des données d'application à partir de ces sauvegardes. Si le plan est exécuté en mode **Secteur par secteur** en raison d'un basculement automatique vers ce mode, la restauration des données d'application sera également impossible.

Exigences pour les machines virtuelles ESXi

Si l'application s'exécute sur une machine virtuelle sauvegardée par l'agent pour VMware, assurez-vous que :

© Acronis International GmbH, 2003-2026

- La machine virtuelle sauvegardée répond aux exigences de sauvegarde et de restauration cohérentes avec l'application répertoriées dans l'article Implémentations de sauvegarde Windows de la documentation VMware : https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere-sdks-tools/8-0/virtual-disk-development-kit-programming-guide/backing-up-virtual-disks-in-vsphere/windows-backup-implementations/working-with-microsoft-shadow-copy.html.
- VMware Tools est installé et à jour sur la machine.
- Le contrôle de compte utilisateur (CCU) est désactivé sur la machine. Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.
  Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

  Remarque
  Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

Exigences pour les machines virtuelles Hyper-V

Si l'application s'exécute sur une machine virtuelle sauvegardée par l'agent pour Hyper-V, assurez-vous que :

- Le système d'exploitation invité est Windows Server 2008 ou version ultérieure.
- Pour Hyper-V 2008 R2 : le système d'exploitation invité est Windows Server 2008/2008 R2/2012.
- La machine virtuelle ne possède aucun disque dynamique.
- La connexion réseau existe entre l'hôte Hyper-V et le système d'exploitation invité. Ceci est requis pour exécuter des demandes WMI distantes au sein de la machine virtuelle.
- Le contrôle de compte utilisateur (CCU) est désactivé sur la machine. Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.
  Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

  Remarque
  Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

- La configuration de la machine virtuelle correspond aux critères suivants :
  - La technologie Hyper-V Integration Services est installée et à jour. La mise à jour critique est https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - Dans les paramètres de votre machine virtuelle, l'option **Gestion** > **Services d'intégration** > **Sauvegarde (point de contrôle du volume)** est activée.

© Acronis International GmbH, 2003-2026

- Pour Hyper-V 2012 et version ultérieure : la machine virtuelle ne possède aucun point de contrôle.
- Pour Hyper-V 2012 R2 et version ultérieure : la machine virtuelle possède un contrôleur SCSI (consultez **Paramètres** > **Matériel**).

Sauvegarde de base de données

Avant de sauvegarder des bases de données, assurez-vous que les exigences répertoriées dans « Prérequis » sont respectées.

Sélectionnez les bases de données comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Sélection des bases de données SQL

Une sauvegarde de base de données SQL contient les fichiers de bases de données (.mdf, .ndf), les fichiers journaux (.ldf) et d'autres fichiers associés. Les fichiers sont sauvegardés à l'aide du service SQL Writer. Le service doit être exécuté au moment où le service de cliché instantané des volumes (VSS) nécessite une sauvegarde ou une restauration.

Les fichiers journaux des transactions SQL sont tronqués après chaque sauvegarde réussie. La troncation de journal SQL peut être désactivée dans les options du plan de protection.

Pour sélectionner des bases de données SQL

1. Cliquez sur **Terminaux** > **Microsoft SQL**.
   Le logiciel affiche l'arborescence des groupes de disponibilité Always On Microsoft SQL Server (AAG), les machines fonctionnant sous Microsoft SQL Server, les instances SQL Server et les bases de données.
2. Accédez aux données que vous voulez sauvegarder.
   Développez les nœuds de l'arborescence ou double-cliquez sur les éléments de la liste à la droite de l'arborescence.
3. Sélectionnez les données que vous voulez sauvegarder. Vous pouvez sélectionner les AAG, les machines fonctionnant sous SQL Server, les instances SQL Server ou les bases de données individuelles.
   - Si vous sélectionnez un AAG, toutes les bases de données incluses dans l'AAG sélectionné seront sauvegardées. Pour plus d'informations sur la sauvegarde des AAG ou de bases de données AAG individuelles, consultez la section « Protection des groupes de disponibilité Always On (AAG) ».
   - Si vous sélectionnez une machine fonctionnant sous SQL Server, toutes les bases de données attachées aux instances SQL Server fonctionnant sur la machine sélectionnée seront sauvegardées.
   - Si vous sélectionnez une instance SQL Server, toutes les bases de données incluses dans l'instance sélectionnée seront sauvegardées.

© Acronis International GmbH, 2003-2026

- Si vous sélectionnez directement les bases de données, seules les bases de données sélectionnées seront sauvegardées.

4. Cliquez sur **Protection**. Si vous y êtes invité, spécifiez les identifiants donnant accès aux données SQL Server.

   Si vous utilisez l'authentification Windows, le compte doit être membre des groupes **Opérateurs de sauvegarde** ou **Administrateurs** de la machine, et du rôle **sysadmin** de chacune des instances faisant l'objet d'une sauvegarde.

   Si vous utilisez l'authentification SQL Server, le compte doit être membre du rôle **sysadmin** de chacune des instances faisant l'objet d'une sauvegarde.

Sélection de données Exchange Server

Le tableau suivant résume les données de Microsoft Exchange Server que vous pouvez sélectionner pour leur sauvegarde, ainsi que les droits d'utilisateur nécessaires pour effectuer cette tâche.

Version d'Exchange	Eléments de données	Droits utilisateur
2007	Groupes de stockage	Appartenance au groupe de rôles **Gestion d'organisation Exchange**
2010/2013/2016/2019	Bases de données, Groupes de disponibilité de la base de données (DAG)	Appartenance au groupe de rôles **Gestion de serveur**.

Une sauvegarde complète inclut l'ensemble des données Exchange Server sélectionnées.

Une sauvegarde incrémentielle comprend les blocs modifiés des fichiers de la base de données, les fichiers de point de contrôle, ainsi que quelques fichiers journaux plus récents que le point de contrôle de la base de données correspondant. Puisque les modifications apportées aux fichiers de la base de données sont intégrées à la sauvegarde, il n'est pas nécessaire de sauvegarder tous les enregistrements des journaux de transaction depuis la sauvegarde précédente. Seul le fichier journal ultérieur au point de contrôle doit être réutilisé après une restauration. Cela permet une restauration plus rapide et assure la réussite de la sauvegarde de la base de données, même lorsque l'enregistrement circulaire est activé.

Les fichiers journaux des transactions sont tronqués après chaque sauvegarde réussie.

Pour sélectionner des données Exchange Server

1. Cliquez sur **Terminaux** > **Microsoft Exchange**.

   Le logiciel affiche l'arborescence des groupes de disponibilité de la base de données (DAG) Exchange Server, les machines fonctionnant sous Microsoft Exchange Server et les bases de données Exchange Server. Si vous avez configuré l'agent pour Exchange tel que décrit dans "Sauvegarde de boîte de réception" (p. 817), les boîtes aux lettres s'affichent également dans cette arborescence.
2. Accédez aux données que vous voulez sauvegarder.

© Acronis International GmbH, 2003-2026

Développez les nœuds de l'arborescence ou double-cliquez sur les éléments de la liste à la droite de l'arborescence.

3. Sélectionnez les données que vous voulez sauvegarder.
   - Si vous sélectionnez un DAG, une copie de chaque base de données en cluster sera sauvegardée. Pour plus d'informations sur la sauvegarde des DAG, reportez-vous à "Protection des groupes de disponibilité de la base de données (DAG)" (p. 812).
   - Si vous sélectionnez une machine fonctionnant sous Microsoft Exchange Server, toutes les bases de données montées sur Exchange Server fonctionnant sur la machine sélectionnée seront sauvegardées.
   - Si vous sélectionnez directement les bases de données, seules les bases de données sélectionnées seront sauvegardées.
   - Si vous avez configuré l'agent pour Exchange tel que décrit dans "Sauvegarde de boîte de réception" (p. 817), vous pouvez sélectionner les boîtes aux lettres pour la sauvegarde.

   Si votre sélection comporte plusieurs bases de données, deux d'entre elles sont traitées simultanément. Une fois la sauvegarde du premier groupe terminée, celle du groupe suivant commence.
4. Le cas échéant, spécifiez les identifiants donnant accès aux données.
5. Cliquez sur **Protection**.

Protection des groupes de disponibilité Always On (AAG)

Présentation des solutions SQL Server haute disponibilité

La fonctionnalité de clustering de basculement Windows Server (WSFC) vous permet de configurer SQL Server pour qu'il soit à haute disponibilité en utilisant la redondance au niveau de l'instance (instance de cluster de basculement, FCI) ou au niveau de la base de données (groupe de disponibilité AlwaysOn, AAG). Vous pouvez également combiner les deux méthodes.

Dans une instance de cluster de basculement, les bases de données SQL sont situées sur un stockage partagé. Ce stockage est accessible uniquement à partir du nœud cluster actif. Si le nœud actif échoue, un basculement se produit et un autre nœud devient actif.

Dans un groupe de disponibilité, chaque réplica de base de données réside sur un nœud différent. Si le réplica principal devient non disponible, le rôle principal est attribué à un réplica secondaire résidant sur un autre nœud.

Ainsi, les clusters sont déjà utilisés comme solution de reprise d'activité après sinistre. Toutefois, il peut arriver que les clusters ne puissent pas fournir de protection de données : par exemple, dans le cas d'un endommagement logique d'une base de données ou d'une panne du cluster entier. De plus, des solutions de cluster ne protègent pas contre les modifications dangereuses de contenu car elles sont immédiatement reproduites sur tous les nœuds de cluster.

© Acronis International GmbH, 2003-2026

Configurations de cluster prises en charge

Le logiciel de sauvegarde prend *uniquement* en charge les groupes de disponibilité Always On (AAG) pour SQL Server 2012 ou version ultérieure. Les autres configurations de cluster, comme les instances de cluster de basculement, la mise en miroir de base de données et l'envoi des journaux, *ne sont pas* prises en charge.

Combien d'agents sont nécessaires pour la sauvegarde et la restauration de données de cluster ?

Pour réussir la sauvegarde et la restauration de données d'un cluster, Agent pour SQL doit être installé sur chaque nœud du cluster WSFC.

Sauvegarde des bases de données incluses dans un AAG

1. Installez Agent pour SQL sur tous les nœuds du cluster WSFC.
2. Sélectionnez l'AAG à sauvegarder comme décrit dans la section « Sélection des bases de données SQL ».

   Vous devez sélectionner l'AAG lui-même pour sauvegarder toutes les bases de données qu'il contient. Pour sauvegarder un ensemble de bases de données, définissez cet ensemble de bases de données dans tous les nœuds de l'AAG.

   Avertissement !
   L'ensemble de bases de données doit être exactement le même dans tous les nœuds. Si le moindre ensemble est différent ou n'est pas défini dans tous les nœuds, la sauvegarde de cluster ne fonctionnera pas correctement.
3. Configurez l'option de sauvegarde « Mode de sauvegarde de cluster ».

Restauration de bases de données incluses dans un AAG

1. Sélectionnez les bases de données que vous voulez restaurer, puis sélectionnez le point de restauration à partir duquel vous voulez les restaurer.

   Quand vous sélectionnez une base de données en cluster sous **Terminaux** > **Microsoft SQL** > **Bases de données** et que vous cliquez sur **Restaurer**, le logiciel n'affiche que les points de restauration correspondant aux fois où la copie sélectionnée de la base de données a été sauvegardée.

   La façon la plus simple de voir tous les points de restauration d'une base de données en cluster est de sélectionner la sauvegarde de l'AAG entier dans l'onglet Stockage de sauvegarde. Les noms des sauvegardes d'AAG sont basés sur le modèle suivant : `<AAG name> - <protection plan name>` et sont dotés d'une icône spéciale.
2. Pour configurer la restauration, suivez les étapes décrites dans « Restauration de bases de données SQL », en commençant par l'étape 5.

© Acronis International GmbH, 2003-2026

Le logiciel définit automatiquement un nœud cluster vers lequel les données seront restaurées. Le nom du nœud est affiché dans le champ **Récupérer vers**. Vous pouvez modifier le nœud cible manuellement.

Important
Une base de données incluse dans un groupe de disponibilité Always On ne peut pas être écrasée lors d'une restauration, car Microsoft SQL Server l'interdit. Vous devez exclure la base de données cible de l'AAG avant la restauration. Ou restaurez simplement la base de données en tant que nouvelle base de données non AAG. Lorsque la restauration est terminée, vous pouvez reconstruire la configuration AAG d'origine.

Protection des groupes de disponibilité de la base de données (DAG)

Présentation des clusters Exchange Server

L'idée principale des clusters Exchange est d'offrir une disponibilité élevée des bases de données, avec un basculement rapide et sans aucune perte de données. Généralement, cela se réalise en conservant une ou plusieurs copies de bases de données ou de groupes de stockage sur les membres du cluster (nœuds de cluster). Si le nœud de cluster qui héberge la copie de base de données active ou si la copie de la base de données active elle-même échoue, l'autre nœud qui héberge la copie passive prend automatiquement la relève des opérations du nœud qui a échoué et fournit l'accès aux services Exchange avec un temps d'arrêt minimal. Ainsi, les clusters sont déjà utilisés comme solution de reprise d'activité après sinistre.

Toutefois, il y a des cas où les solutions de cluster de basculement ne peuvent pas fournir une protection des données : par exemple, dans le cas d'un endommagement logique d'une base de données, lorsqu'une base de données particulière d'un cluster n'a aucune copie (réplica) ou bien lorsque le cluster entier est en panne. De plus, des solutions de cluster ne protègent pas contre les modifications dangereuses de contenu car elles sont immédiatement reproduites sur tous les nœuds de cluster.

Sauvegarde prenant en charge les clusters

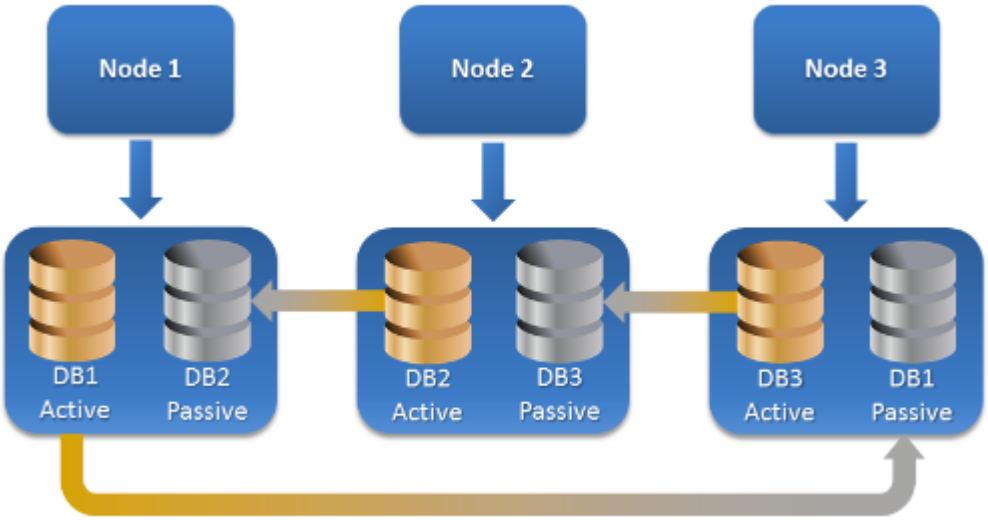
Grâce à la sauvegarde prenant en charge les clusters, vous sauvegardez seulement une copie des données du cluster. Si les données changent d'emplacement au sein du cluster (en raison d'un déplacement ou d'un basculement), le logiciel fait le suivi de toutes les relocalisations de ces données et les sauvegarde en toute sécurité.

Configurations de cluster prises en charge

La sauvegarde prenant en charge les clusters est prise en charge *uniquement* pour Database Availability Group (DAG) dans Exchange Server 2010 ou des versions plus récentes. Les autres configurations de cluster, comme Single Copy Cluster (SCC) et Cluster Continuous Replication (CCR) pour Exchange 2007 *ne sont pas* prises en charge.

© Acronis International GmbH, 2003-2026

DAG est un groupe pouvant contenir jusqu'à 16 serveurs de boîtes aux lettres Exchange. N'importe quel nœud peut accueillir une copie de base de données de boîtes aux lettres provenant de n'importe quel autre nœud. Chaque nœud peut héberger des copies de bases de données passives et actives. Jusqu'à 16 copies de chaque base de données peuvent être créées.



Combien d'agents sont nécessaires pour la sauvegarde et la restauration prenant en charge les clusters ?

Pour assurer le succès de la sauvegarde et de la restauration de bases de données en cluster, l'agent pour Exchange doit être installé sur chaque nœud du cluster Exchange.

Remarque
Une fois que vous avez installé l'agent sur l'un des nœuds, la console Cyber Protect affiche le DAG et ses nœuds sous **Terminaux** > **Microsoft Exchange** > **Bases de données**. Pour installer Agents pour Exchange sur les autres nœuds, sélectionnez le DAG et cliquez sur **Détails**, puis sur **Installer un agent** en regard de chaque nœud.

Sauvegarde des données de cluster Exchange

1. Lors de la création d'un plan de protection, sélectionnez le DAG comme décrit dans "Sélection de données Exchange Server" (p. 809).
2. Configurez l'option de sauvegarde "Mode de sauvegarde de cluster" (p. 616).
3. Spécifiez les autres paramètres du plan de protection, le cas échéant.

Important
Pour la sauvegarde prenant en compte les clusters, assurez-vous de bien sélectionner le DAG. Si vous sélectionnez des noeuds individuels ou des bases de données au sein du DAG, seuls les éléments sélectionnés seront sauvegardés et l'option **Mode de sauvegarde de cluster** sera ignorée.

© Acronis International GmbH, 2003-2026

Restauration des données du cluster Exchange

1. Sélectionnez le point de restauration de la base de données que vous voulez restaurer. Si ça n'est pas possible, sélectionnez un cluster complet pour la restauration.

   Quand vous sélectionnez la copie d'une base de données en cluster sous **Terminaux** > **Microsoft Exchange** > **Bases de données** > `<cluster name>` > `<node name>` et cliquez sur **Restaurer**, le logiciel n'affiche que les points de restauration correspondant aux fois où la copie a été sauvegardée.

   La façon la plus simple d'afficher tous les points de restauration d'une base de données en cluster est de sélectionner sa sauvegarde dans l'onglet Stockage de sauvegarde.
2. Suivez les étapes décrites dans "Restauration de bases de données Exchange" (p. 828) à partir de l'étape 5.

   Le logiciel définit automatiquement un nœud cluster vers lequel les données seront restaurées. Le nom du nœud est affiché dans le champ **Récupérer vers**. Vous pouvez modifier le nœud cible manuellement.

Sauvegarde reconnaissant les applications

La sauvegarde au niveau du disque prenant en charge les applications est disponible pour les différentes machines physiques, les machines virtuelles ESXi et les machines virtuelles Hyper-V. Elle n'est pas disponible pour les groupes de terminaux.

Lorsque vous sauvegardez une machine exécutant Microsoft SQL Server, Microsoft Exchange Server ou les services de domaine Active Directory, activez la **Sauvegarde d'application** pour une protection renforcée des données de ces applications.



Pourquoi utiliser la sauvegarde reconnaissant les applications ?

En utilisant la sauvegarde reconnaissant les applications, vous vous assurez que :

- Les applications sont sauvegardées dans un état cohérent et sont donc immédiatement disponibles après la restauration de la machine.
- Vous pouvez restaurer les bases de données, boîtes aux lettres et éléments de boîte aux lettres SQL et Exchange sans restaurer l'intégralité de la machine.
- Les fichiers journaux des transactions SQL sont tronqués après chaque sauvegarde réussie. La troncation de journal SQL peut être désactivée dans les options du plan de protection. Les fichiers journaux des transactions Exchange sont tronqués sur les machines virtuelles uniquement. Vous pouvez activer l'option de sauvegarde complète VSS si vous souhaitez tronquer les fichiers journaux des transactions Exchange sur une machine physique.

© Acronis International GmbH, 2003-2026

- Si un domaine comprend plusieurs contrôleurs de domaine et que vous en restaurez un, une restauration ne faisant pas autorité est effectuée et une restauration USN n'a pas lieu par la suite.

De quoi ai-je besoin pour utiliser la sauvegarde reconnaissant les applications ?

Sur une machine physique, l'agent pour SQL et/ou l'agent pour Exchange doivent être installés, en plus de l'agent pour Windows.

Sur une machine virtuelle, aucune installation d'agent n'est requise. Il est supposé que la machine est sauvegardée par l'Agent pour VMware ou l'Agent pour Hyper-V.

Remarque
La sauvegarde sans agent reconnaissant les applications n'est pas prise en charge pour les machines virtuelles Hyper-V et VMware ESXi qui exécutent Windows Server 2022 ou Windows Server 2025. Pour protéger les applications Microsoft sur ces machines, installez l'agent de protection dans le système d'exploitation invité. Pour plus d'informations, voir "Configuration de la sauvegarde reconnaissant les applications des machines virtuelles exécutant Windows Server 2022 et versions ultérieures" (p. 816).

L'agent pour VMware (appliance virtuelle) peut créer des sauvegardes reconnaissant les applications, mais il ne peut pas restaurer de données d'application provenant de ces sauvegardes. Pour restaurer des données d'application à partir de sauvegardes créées par cet agent, vous avez besoin d'un agent pour VMware (Windows), d'un agent pour SQL ou d'un agent pour Exchange sur une machine ayant accès à l'emplacement sur lequel les sauvegardes ont été stockées. Lors de la configuration de la restauration de données d'application, sélectionnez le point de restauration sur l'onglet **Stock. de sauvegarde**, puis sélectionnez cette machine dans **Machine à parcourir**.

D'autres critères sont répertoriés dans les sections "Exigences supplémentaires pour les sauvegardes reconnaissant les applications" (p. 805) et "Droits utilisateur requis pour les sauvegardes reconnaissant les applications" (p. 816).

Remarque
Les sauvegardes reconnaissant les applications des machines virtuelles Hyper-V peuvent échouer avec l'erreur « La commande ExecQuery de WMI n'a pas réussi l'exécution de la demande. » ou « Échec de création d'un nouveau processus via WMI » si les sauvegardes sont exécutées sur un hôte présentant une charge élevée en raison de l'absence de réponse ou d'un retard de réponse depuis Windows Management Instrumentation. Retentez ces sauvegardes dans un créneau horaire où la charge sur l'hôte est réduite.

© Acronis International GmbH, 2003-2026

Configuration de la sauvegarde reconnaissant les applications des machines virtuelles exécutant Windows Server 2022 et versions ultérieures

Pour effectuer une sauvegarde reconnaissant les applications sur des machines virtuelles Hyper-V et VMware ESXi exécutant Windows Server 2022 ou Windows Server 2025, vous devez utiliser une sauvegarde avec agent. Pour plus d'informations sur les modes de sauvegarde, voir "Sauvegarde avec et sans agent" (p. 40).

	Sauvegarde basée sur un agent	**Sauvegarde sans agent**
Sauvegarde reconnaissant les applications	Pris en charge	Non pris en charge
Icône de machine virtuelle dans la console Cyber Protect		

Pour configurer une sauvegarde reconnaissant les applications en mode avec agent

1. Installez l'agent de protection (agent pour Windows, agent pour SQL ou agent pour Exchange) dans le système d'exploitation invité de la machine virtuelle.
2. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel vous avez installé l'agent de protection.
3. Configurez la sauvegarde reconnaissant les applications dans un nouveau plan de protection.
4. Appliquez le plan de protection à la machine virtuelle.
5. Exécutez le plan de protection.

En conséquence, une archive de sauvegarde contenant la sauvegarde reconnaissant les applications sera créée.

Droits utilisateur requis pour les sauvegardes reconnaissant les applications

Une sauvegarde reconnaissant les applications comprend des métadonnées d'applications compatibles VSS présentes sur le disque. Pour accéder à ces métadonnées, l'agent nécessite un compte avec les droits appropriés, répertoriés ci-dessous. Vous êtes invité à indiquer ce compte lors de l'activation de la sauvegarde d'applications.

- Pour SQL Server :

  Le compte doit être membre du groupe **Opérateurs de sauvegarde** ou **Administrateurs** sur l'ordinateur et membre du rôle **sysadmin** sur chacune des instances que vous allez sauvegarder.

  Remarque
  Seule l'authentification Windows est prise en charge.

- Pour Exchange Server :

© Acronis International GmbH, 2003-2026

Exchange 2007 : Le compte doit être un membre du groupe **Administrateurs** sur la machine, et un membre du groupe de rôles **Gestion d'organisation Exchange**.

Exchange 2010 et versions ultérieures : Le compte doit être un membre du groupe **Administrateurs** sur la machine, et un membre du groupe de rôles **Gestion d'organisation**.

- Pour Active Directory :

  Le compte doit être un administrateur de domaine.

Exigences supplémentaires pour les machines virtuelles

Si l'application s'exécute sur une machine virtuelle sauvegardée par l'agent pour VMware ou l'agent pour Hyper-V, assurez-vous que le contrôle de compte utilisateur (CCU) est désactivé sur la machine.

Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

Remarque
Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

Exigences supplémentaires pour les ordinateurs exécutant Windows

Pour toutes les versions Windows, vous devez désactiver les politiques de contrôle de compte utilisateur (CCU) afin d'autoriser les sauvegardes reconnaissant les applications.

Si vous ne souhaitez pas désactiver le CCU, vous devez fournir les identifiants de l'administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

Remarque
Utilisez le compte administrateur du domaine intégré qui a été configuré lors de la création du domaine. Les comptes créés plus tard ne sont pas pris en charge.

Pour désactiver les politiques CCU dans Windows

1. Dans l'Éditeur de la base de registre, localisez la clé de la base de registre suivante : `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Modifiez la valeur **EnableLUA** et définissez-la sur **0**.
3. Redémarrez la machine.

Sauvegarde de boîte de réception

La sauvegarde des boîtes aux lettres est prise en charge pour Microsoft Exchange Server 2010 Service Pack 1 (SP1) et version ultérieure.

La sauvegarde de boîte aux lettres est disponible si au moins un agent pour Exchange est enregistré sur le serveur de gestion. L'agent doit être installé sur une machine appartenant à la même forêt Active Directory que Microsoft Exchange Server.

© Acronis International GmbH, 2003-2026

Avant de sauvegarder des boîtes aux lettres, vous devez connecter l'agent pour Exchange à la machine exécutant le **serveur d'Accès Client** (CAS) de Microsoft Exchange Server. Dans Exchange 2016 et les versions ultérieures, le rôle CAS n'est pas disponible en tant qu'option d'installation séparée. Il est automatiquement installé dans le cadre du rôle serveur de boîtes aux lettres. Ainsi, vous pouvez connecter l'agent à n'importe quel serveur exécutant le **rôle de boîte aux lettres**.

Remarque
Vous pouvez restaurer les boîtes aux lettres et les éléments de boîte aux lettres également depuis des sauvegardes de bases de données et des sauvegardes reconnaissant les applications. Pour plus d'informations, voir "Restauration de boîtes aux lettres et éléments de boîtes aux lettres Exchange" (p. 831). Les sauvegardes de bases de données et les sauvegardes reconnaissant les applications ne vous permettent pas de créer des plans de protection pour des boîtes aux lettres indépendantes.

Pour connecter l'agent pour Exchange au CAS

1. Cliquez sur **Terminaux** > **Ajouter**.
2. Cliquez sur **Microsoft Exchange Server**.
3. Cliquez sur **Boîtes aux lettres Exchange**.
   S'il n'y a pas d'agent pour Exchange enregistré sur le serveur de gestion, le logiciel vous propose d'installer l'agent. Après l'installation, répétez cette procédure à partir de l'étape 1.
4. [Facultatif] Si plusieurs agents pour Exchange sont enregistrés sur le serveur de gestion, cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera la sauvegarde.
5. Dans le **serveur d'accès client**, spécifiez le nom de domaine qualifié complet (FQDN) de la machine où le rôle **Accès Client** de Microsoft Exchange Server est activé.
   Dans Exchange 2016 et les versions ultérieures, les services d'accès au client sont automatiquement installés dans le cadre du rôle serveur de boîtes aux lettres. Ainsi, vous pouvez spécifier n'importe quel serveur exécutant le **rôle de boîte aux lettres**. Nous nous référons à ce serveur en tant que CAS plus loin dans cette section.
6. Dans **Type d'authentification**, sélectionnez le type d'authentification utilisé par le CAS. Vous pouvez sélectionner **Kerberos** (par défaut) ou **Basic**.
7. [Uniquement pour une authentification basique] Sélectionnez le protocole à utiliser. Vous pouvez sélectionner **HTTPS** (par défaut) ou **HTTP**.
8. [Uniquement pour une authentification basique avec le protocole HTTPS] Si le CAS utilise un certificat SSL obtenu à partir d'une autorité de certification, il faut que le logiciel vérifie le certificat SSL lors de la connexion au CAS. Pour cela, cochez **Vérifier le certificat SSL**. Sinon, ignorez cette étape.
9. Fournissez les informations d'identification d'un compte qui sera utilisé pour accéder au CAS. Les exigences pour ce compte sont répertoriées dans « Droits utilisateurs requis ».
10. Cliquez sur **Ajouter**.

Ainsi, les boîtes aux lettres apparaissent sous **Terminaux** > **Microsoft Exchange** > **Boîtes aux lettres**.

© Acronis International GmbH, 2003-2026

Sélectionner les boîtes aux lettres Exchange Server

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner les boîtes aux lettres Exchange

1. Cliquez sur **Terminaux** > **Microsoft Exchange**.
   Le logiciel affiche l'arborescence des bases de données et boîtes aux lettres Exchange Server.
2. Cliquez sur **Boîtes aux lettres**, puis sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
3. Cliquez sur **Protection**.

Droits utilisateurs requis

Pour accéder aux boîtes aux lettres, l'agent pour Exchange nécessite un compte doté des droits appropriés. Vous êtes invité à indiquer ce compte lors de la configuration de différentes opérations avec les boîtes aux lettres.

L'appartenance du compte au groupe de rôles **Gestion d'organisation** permet d'accéder à n'importe quelle boîte aux lettres, y compris celles créées à l'avenir.

Les droits utilisateurs minimums requis sont les suivants :

- Le compte doit être un membre du groupe de rôles **Gestion des serveurs** et **Gestion des destinataires**.
- Le compte doit avoir le rôle de gestion **ApplicationImpersonation** activé pour tous les utilisateurs ou groupes d'utilisateurs possédant les boîtes aux lettres auxquelles accédera l'agent.
  Pour plus d'informations sur la configuration du rôle de gestion **ApplicationImpersonation**, consultez l'article suivant de la base de connaissances Microsoft: https://msdn.microsoft.com/fr-fr/library/office/dn722376.aspx.

Restauration de bases de données SQL

Vous pouvez restaurer les bases de données SQL depuis des sauvegardes de base de données et des sauvegardes reconnaissant les applications. Pour plus d'informations sur la différence entre les deux types de sauvegarde, voir "Protection des serveurs Microsoft SQL Server et Microsoft Exchange Server" (p. 803).

Vous pouvez restaurer les bases de données SQL vers l'instance d'origine, vers une autre instance sur l'ordinateur d'origine ou vers une instance sur un ordinateur différent de l'ordinateur d'origine. Lorsque vous effectuez une restauration vers un ordinateur différent de l'ordinateur d'origine, l'agent pour SQL doit être installé sur la machine cible.

Vous pouvez également restaurer les bases de données sous forme de fichiers.

© Acronis International GmbH, 2003-2026

Si vous utilisez l'authentification Windows pour l'instance SQL, vous devrez fournir les identifiants d'un compte membre du groupe **Opérateurs de sauvegarde** ou **Administrateurs** sur l'ordinateur, et membre du rôle **sysadmin** sur l'instance cible. Si vous utilisez l'authentification SQL Server, vous devez fournir les identifiants d'un compte membre du rôle **sysadmin** sur l'instance cible.

Les bases de données système sont restaurées en tant que bases de données utilisateur, avec certaines distinctions. Pour en savoir plus sur ces distinctions, voir "Restauration des bases de données système" (p. 827).

Lors d'une restauration, vous pouvez vérifier la progression de l'opération dans la console Cyber Protect, dans l'onglet **Surveillance** > **Activités**.

Restauration de bases de données SQL vers l'ordinateur d'origine

Vous pouvez restaurer les bases de données SQL vers leur instance d'origine, vers une autre instance sur l'ordinateur d'origine ou vers une instance sur une machine cible différente de la machine d'origine.

Pour restaurer des bases de données SQL vers l'ordinateur d'origine

À partir d'une sauvegarde de base de données

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft SQL**.
2. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Pour restaurer les données vers une machine différente de la machine d'origine, voir "Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine" (p. 822).
3. Sélectionnez un point de restauration.
   Les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données vers une instance**.
   Par défaut, l'instance et les bases de données sont restaurées vers les machines d'origine. Vous pouvez également restaurer une base de données d'origine comme nouvelle base de données.
5. [Lors de la restauration vers une instance différente de l'instance d'origine sur la même machine] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
6. [Lors de la restauration d'une base de données en tant que nouvelle base de données] Cliquez sur le nom de la base de données, puis, dans **Restaurer vers**, sélectionnez **Nouvelle base de données**.
   - Spécifiez le nom de la nouvelle base de données.
   - Spécifiez le chemin d'accès de la nouvelle base de données.
   - Spécifiez le chemin d'accès du journal.
7. [Facultatif] [Non disponible lors de la de la restauration d'une base de données en tant que nouvelle base de données] Pour changer l'état d'une base de données après reprise, cliquez sur

© Acronis International GmbH, 2003-2026

le nom de la base de données, choisissez l'un des états suivants et cliquez sur **Terminé**.

- **Prête à l'emploi (RESTORE WITH RECOVERY)** (par défaut)

  Après l'achèvement de la restauration, la base de données sera prête à l'emploi. Les utilisateurs y auront un accès complet. Le logiciel restaurera toutes les transactions non validées de la base de données restaurée qui sont stockées dans les journaux des transactions. Vous ne pourrez pas restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL.
- **Non-opérationnelle (RESTORE WITH NORECOVERY)**

  Après l'achèvement de la restauration, la base de données sera non-opérationnelle. Les utilisateurs n'y auront aucun accès. Le logiciel conservera toutes les transactions non validées de la base de données restaurée. Vous pourrez restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL et ainsi atteindre le point de restauration nécessaire.
- **En lecture seule (RESTORE WITH STANDBY)**

  Après l'achèvement de la restauration, les utilisateurs auront accès en lecture seule à la base de données. Le logiciel annulera les transactions non validées. Toutefois, il enregistrera les actions d'annulation dans un fichier de secours temporaire afin que les effets de la restauration puissent être annulés.

  Cette valeur est principalement utilisée pour détecter le moment dans le temps où une erreur SQL Server s'est produite.

8. Cliquez sur **Démarrer la restauration**.

À partir d'une sauvegarde reconnaissant les applications

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur qui contenait à l'origine les données que vous souhaitez restaurer, puis cliquez sur **Restauration**.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Pour restaurer les données vers une machine différente de la machine d'origine, voir "Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine" (p. 822).
3. Sélectionnez un point de restauration.

   Les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données SQL**.
5. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

   Par défaut, l'instance et les bases de données sont restaurées vers les machines d'origine. Vous pouvez également restaurer une base de données d'origine comme nouvelle base de données.
6. [Lors de la restauration vers une instance différente de l'instance d'origine sur la même machine] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
7. [Lors de la restauration d'une base de données en tant que nouvelle base de données] Cliquez sur le nom de la base de données, puis, dans **Restaurer vers**, sélectionnez **Nouvelle base de**

© Acronis International GmbH, 2003-2026

données.

- Spécifiez le nom de la nouvelle base de données.
- Spécifiez le chemin d'accès de la nouvelle base de données.
- Spécifiez le chemin d'accès du journal.

8. [Facultatif] [Non disponible lors de la de la restauration d'une base de données en tant que nouvelle base de données] Pour changer l'état d'une base de données après reprise, cliquez sur le nom de la base de données, choisissez l'un des états suivants et cliquez sur **Terminé**.
   - **Prête à l'emploi (RESTORE WITH RECOVERY)** (par défaut)

     Après l'achèvement de la restauration, la base de données sera prête à l'emploi. Les utilisateurs y auront un accès complet. Le logiciel restaurera toutes les transactions non validées de la base de données restaurée qui sont stockées dans les journaux des transactions. Vous ne pourrez pas restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL.
   - **Non-opérationnelle (RESTORE WITH NORECOVERY)**

     Après l'achèvement de la restauration, la base de données sera non-opérationnelle. Les utilisateurs n'y auront aucun accès. Le logiciel conservera toutes les transactions non validées de la base de données restaurée. Vous pourrez restaurer des journaux des transactions supplémentaires à partir des sauvegardes natives de Microsoft SQL et ainsi atteindre le point de restauration nécessaire.
   - **En lecture seule (RESTORE WITH STANDBY)**

     Après l'achèvement de la restauration, les utilisateurs auront accès en lecture seule à la base de données. Le logiciel annulera les transactions non validées. Toutefois, il enregistrera les actions d'annulation dans un fichier de secours temporaire afin que les effets de la restauration puissent être annulés.

     Cette valeur est principalement utilisée pour détecter le moment dans le temps où une erreur SQL Server s'est produite.
9. Cliquez sur **Démarrer la restauration**.

Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine

Vous pouvez restaurer les sauvegardes reconnaissant les applications et les sauvegardes de bases de données dans des instances SQL Server sur des machines cibles différentes des ordinateurs d'origine sur lesquelles l'agent pour SQL est installé. Les sauvegardes doivent être localisées dans le stockage dans le cloud ou dans un stockage partagé accessible par la machine cible.

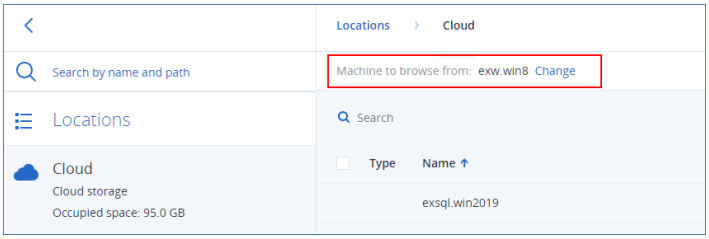
La version SQL Server sur la machine cible doit être identique à la version sur la machine source ou plus récente.

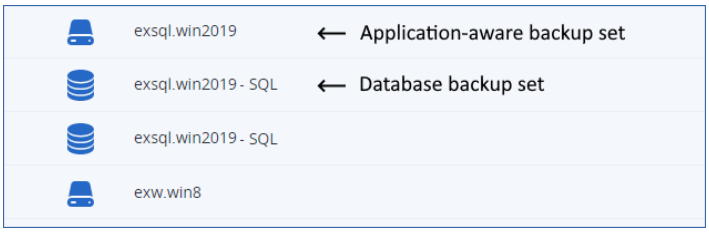
Pour restaurer les bases de données SQL vers un ordinateur différent de l'ordinateur d'origine

Depuis le stockage des sauvegardes

© Acronis International GmbH, 2003-2026

Cette procédure s'applique aux sauvegardes reconnaissant les applications et aux sauvegardes de bases de données.

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de l'ensemble de sauvegardes à partir duquel vous souhaitez restaurer des données.
3. Dans **Machine à parcourir**, sélectionnez la machine cible.
   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.
   

4. Sélectionnez l'ensemble de sauvegardes et, dans le volet **Actions**, cliquez sur **Afficher les sauvegardes**.
   Les ensembles de sauvegardes reconnaissant les applications et les ensembles de sauvegardes de bases de données ont des icônes différentes.
   

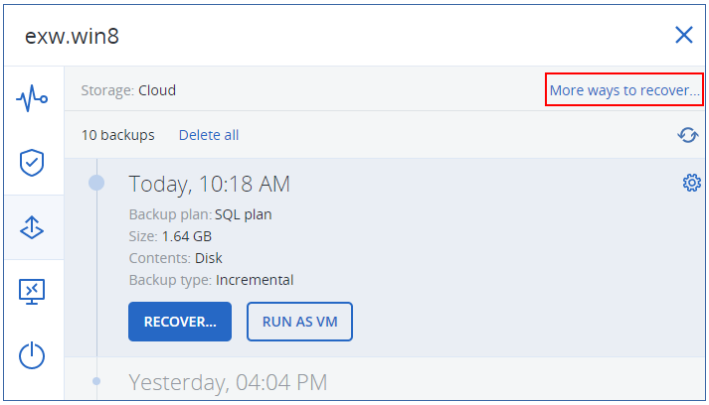
5. Sélectionnez le point de restauration à partir duquel vous souhaitez restaurer des données.
6. [Pour les sauvegardes de base de données] Cliquez sur **Restaurer les bases de données SQL**.
7. [Pour les sauvegardes reconnaissant les applications] Cliquez sur **Restaurer** > **Bases de données SQL**.
8. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
9. [Si la machine cible comprend plusieurs instances SQL] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
10. Cliquez sur le nom de la base de données, spécifiez le chemin d'accès de la nouvelle base de données et des fichiers journaux, puis cliquez sur **Terminé**.
    Vous pouvez indiquer le même chemin d'accès dans les deux champs, par exemple :
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```
11. Cliquez sur **Démarrer la restauration**.

À partir de terminaux

Cette procédure ne s'applique qu'aux sauvegardes reconnaissant les applications.

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur qui contenait à l'origine les données que vous souhaitez restaurer, puis cliquez sur **Restauration**.
3. [Si la machine source est en ligne] Cliquez sur **Autres méthodes de restauration**.



4. Cliquez sur **Sélectionner la machine** pour sélectionner la machine cible, puis cliquez sur **OK**.
   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.
5. Sélectionnez un point de restauration.
   Les points de restauration sont filtrés en fonction de leur emplacement.
6. Cliquez sur **Restaurer** > **Bases de données SQL**.
7. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
8. [Si la machine cible comprend plusieurs instances SQL] Cliquez sur **Instance SQL Server cible**, sélectionnez l'instance cible, puis cliquez sur **Terminé**.
9. Cliquez sur le nom de la base de données, spécifiez le chemin d'accès de la nouvelle base de données et des fichiers journaux, puis cliquez sur **Terminé**.
   Vous pouvez indiquer le même chemin d'accès dans les deux champs, par exemple :

```
C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
```

10. Cliquez sur **Démarrer la restauration**.

Restauration de bases de données SQL sous forme de fichiers

Vous pouvez restaurer les bases de données sous forme de fichiers. Cette option peut être utile si vous devez extraire des données pour l'exploration de données, un audit ou tout autre traitement ultérieur effectué par des outils tiers. Pour savoir comment joindre les fichiers de base de données SQL à une instance SQL Server, voir "Attacher des bases de données SQL Server" (p. 828).

Vous pouvez restaurer les bases de données sous forme de fichiers sur l'ordinateur d'origine ou sur d'autres ordinateurs sur lesquels l'agent pour SQL est installé. Lorsque vous restaurez des données sur d'autres ordinateurs que l'ordinateur d'origine, les sauvegardes doivent être localisées dans le stockage dans le cloud ou dans un stockage partagé accessible par la machine cible.

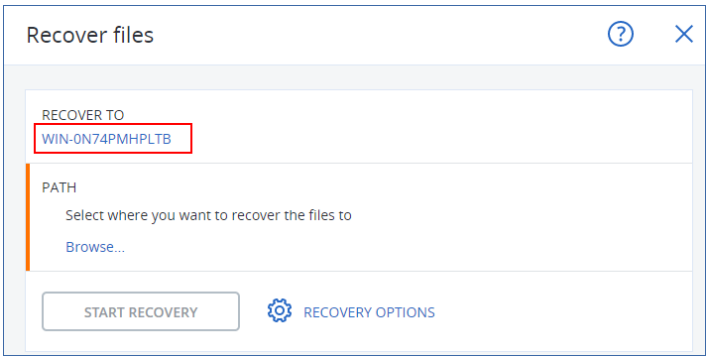
© Acronis International GmbH, 2003-2026

Remarque
La restauration de bases de données sous forme de fichiers est la seule méthode de reprise disponible si vous utilisez l'agent pour VMware (Windows). La restauration de bases de données à l'aide de l'agent pour VMware (appliance virtuelle) n'est pas possible.

Pour restaurer des bases de données SQL sous forme de fichiers

À partir d'une sauvegarde de base de données

Cette procédure s'applique aux machines sources en ligne.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft SQL**.
2. Sélectionnez les bases de données que vous souhaitez restaurer, puis cliquez sur **Restauration**.
3. Sélectionnez un point de restauration.
   Les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Bases de données en tant que fichiers**.
5. [Lorsque de la restauration sur un ordinateur différent de l'ordinateur d'origine] Dans **Restaurer vers**, sélectionnez la machine cible.
   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.
   Pour modifier la sélection, cliquez sur le nom de l'ordinateur, sélectionnez un autre ordinateur, puis cliquez sur **OK**.
   

6. Dans **Chemin d'accès**, cliquez sur **Parcourir**, sélectionnez un dossier local ou réseau dans lequel enregistrer les fichiers, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer la restauration**.

À partir d'une sauvegarde reconnaissant les applications

Cette procédure s'applique aux machines sources en ligne.

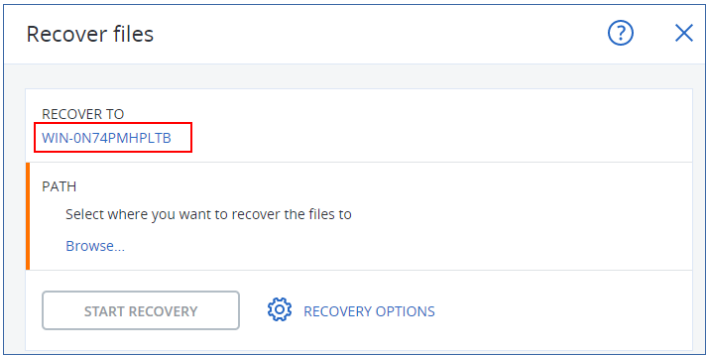
1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur qui contenait à l'origine les données que vous souhaitez restaurer, puis cliquez sur **Restauration**.
3. Sélectionnez un point de restauration.
   Les points de restauration sont filtrés en fonction de leur emplacement.

© Acronis International GmbH, 2003-2026

4. Cliquez sur **Restaurer** > **Bases de données SQL**, sélectionnez les bases de données que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
5. [Lorsque de la restauration sur un ordinateur différent de l'ordinateur d'origine] Dans **Restaurer vers**, sélectionnez la machine cible.

   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.

   Pour modifier la sélection, cliquez sur le nom de l'ordinateur, sélectionnez un autre ordinateur, puis cliquez sur **OK**.



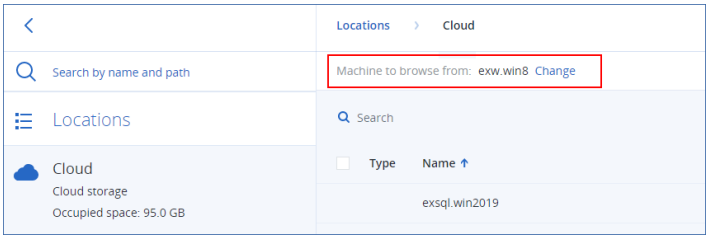
6. Dans **Chemin d'accès**, cliquez sur **Parcourir**, sélectionnez un dossier local ou réseau dans lequel enregistrer les fichiers, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer la restauration**.

À partir d'une sauvegarde sur un ordinateur hors ligne

Cette procédure s'applique aux sauvegardes reconnaissant les applications et aux sauvegardes de bases de données sur les machines sources hors ligne.

1. Sur la console Cyber Protect, accédez à **Stockage de sauvegarde**.
2. Sélectionnez l'emplacement de l'ensemble de sauvegardes à partir duquel vous souhaitez restaurer des données.
3. Dans **Machine à parcourir**, sélectionnez la machine cible.

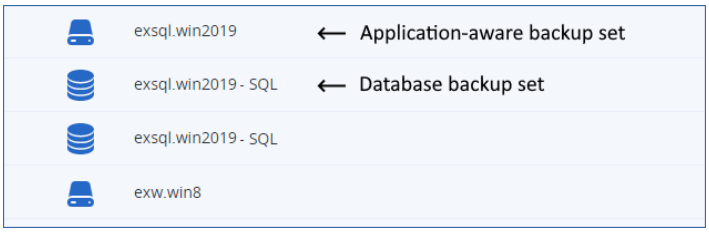
   Il s'agit de la machine sur laquelle vous allez restaurer les données. La machine cible doit être en ligne.



4. Sélectionnez l'ensemble de sauvegardes et, dans le volet **Actions**, cliquez sur **Afficher les sauvegardes**.

   Les ensembles de sauvegardes reconnaissant les applications et les ensembles de sauvegardes de bases de données ont des icônes différentes.

© Acronis International GmbH, 2003-2026



5. Sélectionnez le point de restauration à partir duquel vous souhaitez restaurer des données.
6. [Pour les sauvegardes de base de données] Cliquez sur **Restaurer les bases de données SQL**.
7. [Pour les sauvegardes reconnaissant les applications] Cliquez sur **Restaurer** > **Bases de données SQL**.
8. Sélectionnez l'instance SQL Server ou cliquez sur le nom de l'instance pour sélectionner les bases de données spécifiques que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
9. Dans **Chemin d'accès**, cliquez sur **Parcourir**, sélectionnez un dossier local ou réseau dans lequel enregistrer les fichiers, puis cliquez sur **Terminé**.
10. Cliquez sur **Démarrer la restauration**.

Restauration des bases de données système

Toutes les bases de données système d'une même instance sont restaurées en une seule fois. Lors de la restauration de bases de données système, le logiciel redémarre automatiquement l'instance de destination dans le mode mono-utilisateur. Une fois la restauration terminée, le logiciel redémarre l'instance et restaure d'autres bases de données (le cas échéant).

Autres points à considérer lors de la restauration de bases de données système :

- Les bases de données système ne peuvent être restaurées que sur une instance de la même version que l'instance d'origine.
- Les bases de données système sont toujours restaurées dans l'état « prête à l'emploi ».

Restauration de la base de données MASTER

Les bases de données système contiennent la base de données **MASTER**. La base de données **MASTER** enregistre les informations sur toutes les bases de données de l'instance. Par conséquent, la base de données **MASTER** dans la sauvegarde contient des informations à propos des bases de données qui existaient dans l'instance au moment de la sauvegarde. Après la restauration de la base de données **MASTER**, vous devrez peut-être effectuer les opérations suivantes :

- Les bases de données qui sont apparues dans l'instance après que la sauvegarde a été effectuée ne sont pas visibles par l'instance. Pour amener ces bases de données en production, attachez-les manuellement à l'instance, en utilisant SQL Server Management Studio.
- Les bases de données qui ont été supprimées après que la sauvegarde a été effectuée sont affichées comme hors ligne dans l'instance. Supprimez ces bases de données en utilisant SQL Server Management Studio.

© Acronis International GmbH, 2003-2026

Attacher des bases de données SQL Server

Cette section décrit comment attacher une base de données dans SQL Server en utilisant SQL Server Management Studio. Une seule base de données peut être attachée à la fois.

Attacher une base de données requiert une des autorisations suivantes : **CREATE DATABASE**, **CREATE ANY DATABASE** ou **ALTER ANY DATABASE**. Normalement, ces autorisations sont accordées au rôle **sysadmin** de l'instance.

Pour attacher une base de données

1. Lancez Microsoft SQL Server Management Studio.
2. Connectez-vous à l'instance SQL Server, puis développez l'instance.
3. Cliquez avec le bouton droit de la souris sur **Bases de données** et cliquez sur **Attacher**.
4. Cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Localiser les fichiers de base de données**, trouvez et sélectionnez le fichier .mdf de la base de données.
6. Dans la section **Détails de la base de données**, assurez-vous que le reste des fichiers de base de données (fichiers .ndf et .ldf) sont trouvés.

   Détails. Les fichiers de base de données SQL Server peuvent ne pas être trouvés automatiquement si :
   - ils ne sont pas dans l'emplacement par défaut, ou ils ne sont pas dans le même dossier que le fichier de la base de données principale (.mdf). Solution : Spécifiez manuellement le chemin d'accès aux fichiers requis dans la colonne **Chemin d'accès du fichier actuel**.
   - Vous avez restauré un ensemble incomplet de fichiers qui composent la base de données. Solution : Restaurez les fichiers de base de données SQL Server manquants à partir de la sauvegarde.
7. Lorsque tous les fichiers sont trouvés, cliquez sur **OK**.

Restauration de bases de données Exchange

Cette section décrit la restauration depuis des sauvegardes de base de données et des sauvegardes reconnaissant les applications.

Vous pouvez restaurer des données Exchange Server sur un serveur Exchange actif. Il peut s'agir du serveur Exchange d'origine ou d'un serveur Exchange de la même version exécuté sur la machine avec le même nom de domaine complet (FQDN). L'agent pour Exchange doit être installé sur la machine.

Le tableau suivant résume les données d'Exchange Server que vous pouvez sélectionner pour leur restauration, ainsi que les droits d'utilisateur nécessaires pour effectuer cette tâche.

Version d'Exchange	Eléments de données	Droits utilisateur

© Acronis International GmbH, 2003-2026

2007	Groupes de stockage	Appartenance au groupe de rôles **Gestion d'organisation Exchange**.
2010/2013/2016/2019	Bases de données	Appartenance au groupe de rôles **Gestion de serveur**.

Parallèlement, vous pouvez restaurer les bases de données (groupes de stockage) en tant que fichiers. Les fichiers de bases de données, tout comme les fichiers journaux de transactions, seront extraits de la sauvegarde pour être placés dans le dossier de votre choix. Cela peut être utile si vous devez extraire des données pour un audit ou un autre traitement par des outils tiers, ou si la restauration échoue pour une raison quelconque et que vous recherchez une solution de rechange pour monter les bases de données manuellement.

Si vous utilisez uniquement l'agent pour VMware (Windows), la restauration de bases de données sous forme de fichiers est la seule méthode de restauration disponible. La restauration de bases de données à l'aide de l'agent pour VMware (appliance virtuelle) n'est pas possible.

Tout au long des procédures ci-après, nous utiliserons le terme « bases de données » pour se référer à la fois aux bases de données et aux groupes de stockage.

Pour restaurer des bases de données Exchange sur un serveur Exchange actif

1. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez les bases de données que vous voulez restaurer.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications]Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec Agent pour Exchange, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions ci-dessus devient une machine cible pour la restauration de données Exchange.
4. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, cliquez sur **Restaurer** > **Bases de données Exchange**, sélectionnez la base de données que vous

© Acronis International GmbH, 2003-2026

souhaitez restaurer, puis cliquez sur **Restaurer**.

- Lors d'une restauration depuis une sauvegarde de base de données, cliquez sur **Restaurer** > **Bases de données vers un serveur Exchange**.

5. Par défaut, les bases de données sont restaurées vers leur état d'origine. Si la base de données d'origine n'existe pas, elle sera recréée.

   Pour restaurer une base de données en tant que base de données différente :

   a. Cliquez sur le nom de la base de données.

   b. Dans **Restaurer vers**, sélectionnez **Nouvelle base de données**.

   c. Spécifiez le nom de la nouvelle base de données.

   d. Spécifiez le chemin de la nouvelle base de données et des fichiers journaux. Le dossier que vous spécifiez ne doit contenir ni la base de données initiale, ni les fichiers journaux.

6. Cliquez sur **Démarrer la restauration**.

La progression de la restauration sont affichées dans l'onglet Activités.

Pour restaurer des bases de données Exchange sous forme de fichiers

1. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez les bases de données que vous voulez restaurer.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications] Si la sauvegarde est située dans le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec agent pour Exchange ou agent pour VMware, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions ci-dessus devient une machine cible pour la restauration de données Exchange.
4. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, cliquez sur **Restaurer** > **Bases de données Exchange**, sélectionnez la base de données que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.

© Acronis International GmbH, 2003-2026

- Lors d'une restauration depuis une sauvegarde de base de données, cliquez sur **Restaurer** > **Bases de données en tant que fichiers**.

5. Cliquez sur **Parcourir**, puis sélectionnez un fichier local ou réseau où enregistrer les fichiers.
6. Cliquez sur **Démarrer la restauration**.

La progression de la restauration sont affichées dans l'onglet Activités.

Montage de bases de données Exchange Server

Après avoir restauré les fichiers de la base de données, vous pouvez mettre les bases de données en ligne en les montant. Le montage est exécuté en utilisant la console de gestion Exchange, le gestionnaire système Exchange ou l'environnement de ligne de commande Exchange Management Shell.

Les bases de données restaurées seront dans un état d'arrêt incorrect. Une base de données qui est dans un état d'arrêt incorrect peut être montée par le système si elle est restaurée sur son emplacement d'origine (cela signifie donc que les informations concernant la base de données d'origine sont présentes dans Active Directory). Lors de la restauration d'une base de données vers un autre emplacement (tel qu'une nouvelle base de données ou la base de données de restauration), la base de données ne peut pas être montée tant qu'elle ne retourne pas dans un état d'arrêt normal à l'aide de la commande `Eseutil /r <Enn>`. `<Enn>` indique le préfixe du fichier journal pour la base de données (ou du groupe de stockage qui contient la base de données) dans laquelle vous devez appliquer les fichiers journaux des transactions.

Le compte que vous utilisez pour attacher une base de données doit être un délégué d'un rôle d'administrateur d'Exchange Server et d'un groupe d'administrateurs local sur le serveur cible.

Pour plus de détails sur la façon de monter des bases de données, reportez-vous aux articles suivants :

- Exchange 2010 ou versions plus récentes : http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007 : http://technet.microsoft.com/fr-fr/library/aa998871(v=EXCHG.80).aspx

Restauration de boîtes aux lettres et éléments de boîtes aux lettres Exchange

Vous pouvez restaurer des boîtes aux lettres et éléments de boîtes aux lettres Exchange à partir des sauvegardes suivantes :

- Sauvegardes de base de données (y compris les sauvegardes DAG)
- Sauvegardes reconnaissant les applications
- Sauvegardes de boîtes aux lettres

Vous pouvez restaurer les éléments suivants :

© Acronis International GmbH, 2003-2026

- Boîtes aux lettres (à l'exception des boîtes aux lettres archivées)
- Dossiers publics

> **Remarque**
> Disponible uniquement depuis les sauvegardes de base de données. Consultez "Sélection de données Exchange Server" (p. 809).

- Éléments de dossier Public
- Dossiers de courriers électroniques
- Messages de courriers électroniques
- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

La ou les boîtes aux lettres peuvent être restaurée(s) sur Exchange Server en temps réel ou sur Microsoft 365.

Restauration sur Exchange Server

La restauration granulaire peut uniquement être réalisée sur Microsoft Exchange Server 2010 Service Pack 1 (SP1) et versions ultérieures. Il est possible que la sauvegarde source contienne des bases de données ou des boîtes aux lettres de toute autre version d'Exchange compatible.

La restauration granulaire peut être effectuée par l'agent pour Exchange ou l'agent pour VMware (Windows). Le serveur Exchange cible et la machine exécutant l'agent doivent appartenir à la même forêt Active Directory.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres existante, les éléments existants dont les identifiants sont identiques sont écrasés.

La restauration des éléments de boîtes aux lettres n'écrase aucun élément. À la place, le chemin d'accès complet vers un élément de boîte aux lettres est recréé dans le dossier cible.

Exigences sur les comptes d'utilisateur

Une boîte aux lettres restaurée à partir d'une sauvegarde doit être associée à un compte d'utilisateur dans Active Directory.

Les boîtes aux lettres des utilisateurs et leur contenu peuvent être restaurés uniquement si les comptes d'utilisateur qui leur sont associés sont *activés*. Les boîtes aux lettres partagées, de salles et d'équipement peuvent être restaurées uniquement si leurs comptes d'utilisateur associés sont *désactivés*.

© Acronis International GmbH, 2003-2026

Une boîte aux lettres qui ne répond pas aux conditions énoncées ci-dessus est ignorée lors de la restauration.

Si certaines boîtes aux lettres sont ignorées, la restauration réussira avec des avertissements. Si toutes les boîtes aux lettres sont ignorées, la restauration échouera.

Restauration vers Microsoft 365

La restauration d'éléments de données Exchange vers Microsoft 365, et inversement, est prise en charge à la condition que l'agent pour Microsoft 365 soit installé localement.

La restauration peut être réalisée à partir de Microsoft Exchange Server 2010 et versions ultérieures.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres Microsoft 365 existante, les éléments existants sont intacts et les éléments restaurés sont placés à leurs côtés.

Lors de la restauration d'une boîte aux lettres unique, vous devez d'abord sélectionner la boîte aux lettres Microsoft 365 cible. Lors de la restauration de plusieurs boîtes aux lettres en une seule opération de restauration, le logiciel essaiera de restaurer chaque boîte aux lettres vers la boîte aux lettres de l'utilisateur avec le même nom. Si l'utilisateur est introuvable, la boîte aux lettres est ignorée. Si certaines boîtes aux lettres sont ignorées, la restauration réussira avec des avertissements. Si toutes les boîtes aux lettres sont ignorées, la restauration échouera.

Pour plus d'informations sur la restauration vers Microsoft 365, voir "Protection des données Microsoft 365" (p. 844).

Restauration de boîtes aux lettres

Pour restaurer des boîtes aux lettres à partir d'une sauvegarde de base de données ou d'une sauvegarde reconnaissant les applications

1. [Uniquement lors de la restauration à partir d'une sauvegarde de base de données vers Microsoft 365] Si l'agent pour Microsoft 365 n'est pas installé sur la machine exécutant Exchange Server qui était sauvegardée, effectuez l'une des actions suivantes :
   - S'il n'y a pas d'agent pour Microsoft 365 au sein de votre organisation, installez un agent pour Microsoft 365 sur la machine qui a été sauvegardée (ou sur une autre machine possédant la même version de Microsoft Exchange Server).
   - Si vous avez déjà un agent pour Microsoft 365 au sein de votre organisation, copiez des bibliothèques depuis l'ordinateur qui a été sauvegardée (ou à partir d'une autre machine possédant la même version de Microsoft Exchange Server) vers la machine avec l'agent pour Microsoft 365, comme décrit dans "Copier les bibliothèques Microsoft Exchange Server" (p. 839).
2. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications : sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.

© Acronis International GmbH, 2003-2026

- Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez la base de données qui contenait à l'origine les données que vous voulez restaurer.

3. Cliquez sur **Restauration**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Utilisez d'autres méthodes de restauration :

   - [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications] Si la sauvegarde est située dans le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec agent pour Exchange ou agent pour VMware, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde.

   La machine choisie pour la navigation dans l'une des actions présentées ci-dessus effectuera la restauration des données à la place de la machine d'origine hors ligne.
5. Cliquez sur **Restaurer** > **Boîtes aux lettres Exchange**.
6. Sélectionnez les boîtes aux lettres que vous souhaitez restaurer.

   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.
7. Cliquez sur **Restaurer**.
8. [Uniquement lors de la restauration vers Microsoft 365] :
   a. Dans **Restaurer vers**, sélectionnez **Microsoft 365**.
   b. [Si vous avez sélectionné uniquement une boîte aux lettres à l'étape 6] Dans **Boîte aux lettres cible**, spécifiez la boîte aux lettres cible.
   c. Cliquez sur **Démarrer la restauration**.

   Les étapes suivantes de cette procédure ne sont pas nécessaires.
9. Cliquez sur **Machine cible avec Microsoft Exchange Server** pour sélectionner ou modifier la machine cible. Cette étape permet la restauration d'une machine qui n'exécute par l'agent pour Exchange.

   Spécifiez le nom de domaine qualifié complet (FQDN) de la machine où le rôle **Accès client** (dans Microsoft Exchange Server 2010/2013) ou le **rôle de boîte aux lettres** (dans Microsoft Exchange Server 2016 ou version ultérieure) est activé. La machine doit appartenir à la même forêt Active Directory que la machine qui effectue la restauration.

   Si vous y êtes invité, fournissez les informations d'identification d'un compte qui sera utilisé pour accéder à la machine. Les exigences pour ce compte sont répertoriées dans "Droits utilisateurs requis" (p. 819).
10. [Facultatif] Cliquez sur **Base de données pour recréer toutes boîtes aux lettres manquantes** pour modifier la base de données automatiquement sélectionnée.
11. Cliquez sur **Démarrer la restauration**.

© Acronis International GmbH, 2003-2026

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Pour restaurer une boîte aux lettres à partir d'une sauvegarde de boîte aux lettres

1. Cliquez sur **Terminaux** > **Microsoft Exchange** > **Boîtes aux lettres**.
2. Sélectionnez la boîte aux lettres à restaurer, puis cliquez sur **Restauration**.
   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.
   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Boîte aux lettres**.
5. Exécutez les étapes 8-11 de la procédure ci-dessus.

Restauration d'éléments de boîte aux lettres

Pour restaurer des boîtes aux lettres à partir d'une sauvegarde de base de données ou d'une sauvegarde reconnaissant les applications

1. [Uniquement lors de la restauration à partir d'une sauvegarde de base de données vers Microsoft 365] Si l'agent pour Microsoft 365 n'est pas installé sur la machine exécutant Exchange Server qui était sauvegardée, effectuez l'une des actions suivantes :
   - S'il n'y a pas d'agent pour Microsoft 365 au sein de votre organisation, installez un agent pour Microsoft 365 sur la machine qui a été sauvegardée (ou sur une autre machine possédant la même version de Microsoft Exchange Server).
   - Si vous avez déjà un agent pour Microsoft 365 au sein de votre organisation, copiez des bibliothèques depuis la machine qui a été sauvegardée (ou à partir d'une autre machine possédant la même version de Microsoft Exchange Server) vers la machine avec l'agent pour Microsoft 365, comme décrit dans « Copier des bibliothèques Microsoft Exchange ».
2. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications : sous **Terminaux**, sélectionnez la machine qui contenait à l'origine les données que vous voulez restaurer.
   - Lors d'une restauration à partir d'une sauvegarde de base de données, cliquez sur **Terminaux** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez la base de données qui contenait à l'origine les données que vous voulez restaurer.
3. Cliquez sur **Restauration**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Utilisez d'autres méthodes de restauration :

© Acronis International GmbH, 2003-2026

- [Uniquement lors d'une restauration à partir d'une sauvegarde reconnaissant les applications] Si la sauvegarde est située dans le Cloud ou à un emplacement de stockage partagé (c'est-à-dire si d'autres agents peuvent y accéder), cliquez sur **Sélectionner une machine**, sélectionnez une machine en ligne avec agent pour Exchange ou agent pour VMware, puis choisissez un point de restauration.
- Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde.

La machine choisie pour la navigation dans l'une des actions présentées ci-dessus effectuera la restauration des données à la place de la machine d'origine hors ligne.

5. Cliquez sur **Restaurer** > **Boîtes aux lettres Exchange**.
6. Cliquez sur la boîte aux lettres dans laquelle les éléments que vous souhaitez restaurer étaient initialement présents.
7. Sélectionnez les éléments que vous souhaitez restaurer.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

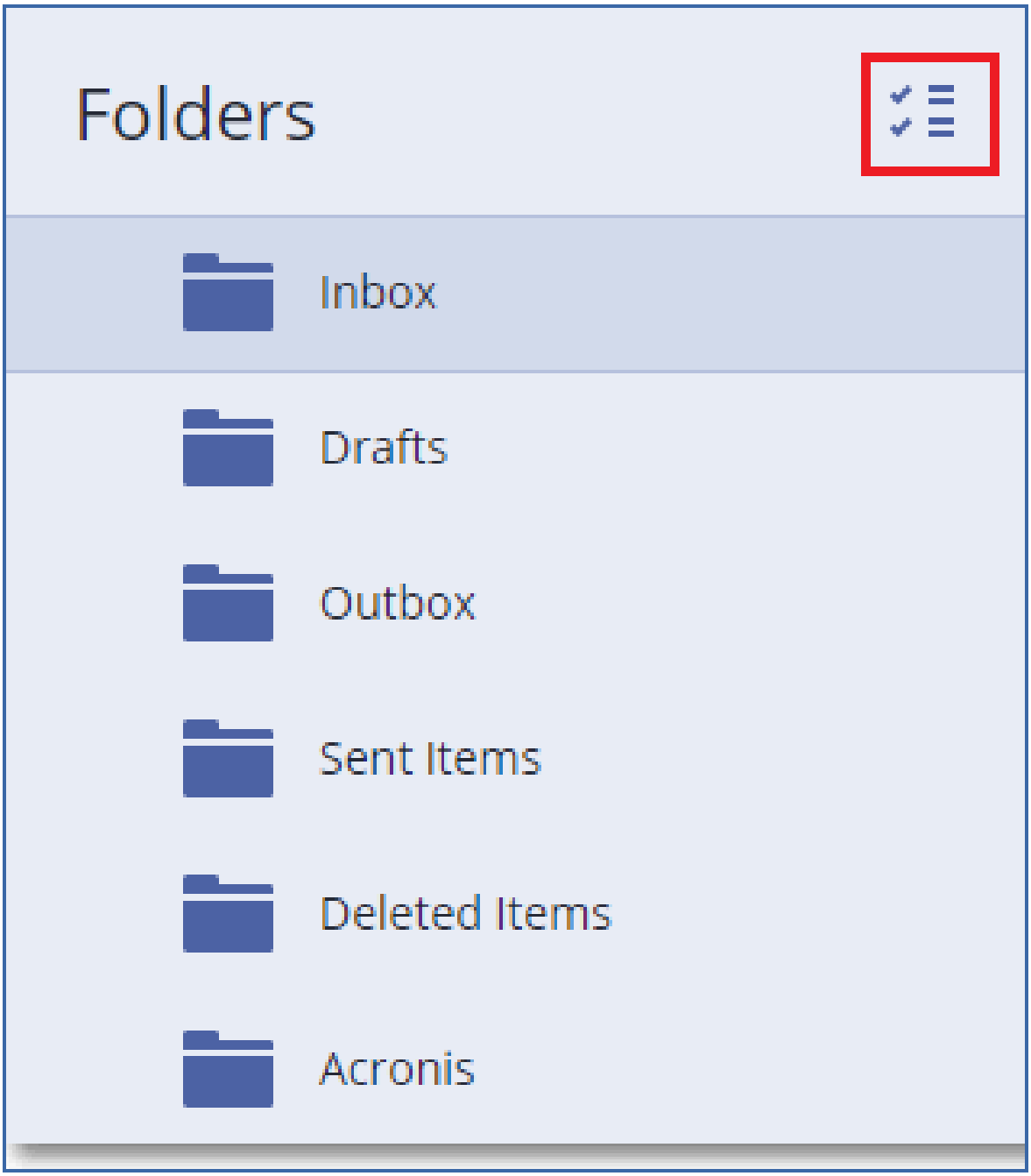
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes.

   Remarque
   Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.

   Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers de restauration.

© Acronis International GmbH, 2003-2026



8. Cliquez sur **Restaurer**.
9. Pour restaurer Microsoft 365, sélectionnez **Microsoft 365** dans **Restaurer vers**.

   Pour effectuer une restauration vers un serveur Exchange, conservez la valeur par défaut **Microsoft Exchange** dans **Restaurer vers**.
10. [Uniquement lors de la restauration vers Exchange Server] Cliquez sur **Machine cible avec Microsoft Exchange Server** pour sélectionner ou modifier la machine cible. Cette étape permet la restauration d'une machine qui n'exécute par l'agent pour Exchange.

    Spécifiez le nom de domaine qualifié complet (FQDN) de la machine où le rôle **Accès client** (dans Microsoft Exchange Server 2010/2013) ou le **rôle de boîte aux lettres** (dans Microsoft

© Acronis International GmbH, 2003-2026

Exchange Server 2016 ou version ultérieure) est activé. La machine doit appartenir à la même forêt Active Directory que la machine qui effectue la restauration.

Si vous y êtes invité, fournissez les informations d'identification d'un compte qui sera utilisé pour accéder à la machine. Les exigences pour ce compte sont répertoriées dans "Droits utilisateurs requis" (p. 819).

11. Dans **Boîte aux lettres cible**, afficher, modifier ou spécifier la boîte aux lettres cible.

    Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une machine cible non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
12. [Uniquement lors de la restauration de messages électroniques] Dans **Dossier cible**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Par défaut, le dossier **Éléments restaurés** est sélectionné. En raison des limites de Microsoft Exchange, les évènements, tâches, notes et contacts sont restaurés dans leur emplacement d'origine, quel que soit le **dossier cible** spécifié.
13. Cliquez sur **Démarrer la restauration**.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Pour restaurer un élément de boîte aux lettres à partir d'une sauvegarde de boîte aux lettres

1. Cliquez sur **Terminaux** > **Microsoft Exchange** > **Boîtes aux lettres**.
2. Sélectionnez la boîte aux lettres d'origine des éléments à restaurer, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.

   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. Sélectionnez les éléments que vous souhaitez restaurer.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes.

© Acronis International GmbH, 2003-2026

Remarque
Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.

Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer à une adresse électronique. Le message est envoyé à partir de l'adresse électronique de votre compte d'administrateur.

Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

6. Cliquez sur **Restaurer**.
7. Exécutez les étapes 9-13 de la procédure ci-dessus.

Copier les bibliothèques Microsoft Exchange Server

Lors de la restauration de boîtes aux lettres Exchange ou d'éléments de boîte aux lettres vers Microsoft 365, vous aurez peut-être besoin de copier les bibliothèques suivantes depuis la machine qui a été sauvegardée (ou depuis une autre machine possédant la même version de Microsoft Exchange Server) vers la machine avec l'agent pour Microsoft 365.

Copiez les fichiers suivants, en fonction de la version de Microsoft Exchange Server sauvegardée.

Version Microsoft Exchange Server	Bibliothèques	Emplacement par défaut

Microsoft Exchange Server 2010	`ese.dll`
	`esebcli2.dll`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016, 2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

Les bibliothèques doivent être placées dans le dossier `%ProgramData%\Acronis\ese`. Si ce dossier n'existe pas, créez-le manuellement.

Modification des informations d'identification de SQL Server ou d'Exchange Server

Vous pouvez modifier les informations d'identification de SQL Server ou Exchange Server sans réinstaller l'agent.

© Acronis International GmbH, 2003-2026

Pour modifier les informations d'identification de SQL Server ou Exchange Server

1. Cliquez sur **Terminaux**, puis sur **Microsoft SQL** ou **Microsoft Exchange**.
2. Sélectionnez le groupe de disponibilité Always On, le groupe de disponibilité de la base de données, l'instance SQL Server ou l'instance Exchange Server dont vous voulez modifier les identifiants d'accès.
3. Cliquez sur **Indiquer l'identifiant**.
4. Indiquez les nouvelles informations d'identification, puis cliquez sur **OK**.

Pour modifier les informations d'identification d'Exchange Server pour la sauvegarde de boîte aux lettres

1. Cliquez sur **Terminaux** > **Microsoft Exchange**, puis développez **Boîtes aux lettres**.
2. Sélectionnez l'Exchange Server dont vous souhaitez modifier les informations d'identification.
3. Cliquez sur **Paramètres**.
4. Indiquez les nouvelles informations d'identification sous **Compte administrateur Exchange**, puis cliquez sur **OK**.

Protection des terminaux mobiles

L'application Acronis Cyber Protect vous permet de sauvegarder vos données mobiles vers le stockage dans le cloud, puis de les restaurer en cas de perte ou d'endommagement. Veuillez noter que, pour effectuer une sauvegarde vers le stockage dans le cloud, vous devez posséder un compte et un abonnement au cloud.

Terminaux mobiles pris en charge

Vous pouvez installer l'application Acronis Cyber Protect sur un terminal mobile qui utilise l'un des systèmes d'exploitation suivants :

- iOS 17 à iOS 26 (iPhone, iPod, iPad)
- Android 11 à Android 15

Important
Pour lancer le processus de sauvegarde, vous devez démarrer l'application manuellement.

Ce que vous pouvez sauvegarder

- Contacts (nom, numéro de téléphone et adresse e-mail)
- Photos (la taille et le format d'origine de vos photos sont préservés)

Remarque
Sur iOS, les live photos sont restaurées sous forme d'images fixes.

© Acronis International GmbH, 2003-2026

- Vidéos
- Calendriers
- Rappels (iOS uniquement)

Ce que vous devez savoir

- Vous pouvez uniquement sauvegarder les données dans le stockage sur le Cloud.
- Lorsque vous ouvrez l'application, le résumé des changements dans les données s'affiche et vous pouvez démarrer une sauvegarde manuellement.
- La fonctionnalité **Sauvegarde continue** est activée par défaut. Si ce paramètre est activé, l'application Acronis Cyber Protect détecte automatiquement les nouvelles données à la volée et les télécharge dans le cloud.
- L'option **Utiliser uniquement le Wi-Fi** est activée par défaut dans les paramètres de l'application. Si ce paramètre est activé, l'application Acronis Cyber Protect ne sauvegardera vos données que lorsqu'une connexion Wi-Fi sera disponible. Si la connexion Wi-Fi est perdue, le processus de sauvegarde ne démarre pas. Pour que l'application utilise également la connexion par réseau cellulaire, désactivez cette option.
- L'optimisation de la batterie de votre terminal peut empêcher l'application Acronis Cyber Protect de fonctionner correctement. Pour exécuter les sauvegardes dans les temps, vous devez arrêter l'optimisation de la batterie pour l'application.
- Vous pouvez économiser de l'énergie de deux façons :
  - La fonctionnalité **Sauvegarder pendant la charge** est désactivée par défaut. Si ce paramètre est activé, l'application Acronis Cyber Protect ne sauvegardera vos données que lorsque votre terminal sera connecté à une source d'alimentation. Lorsque le terminal est déconnecté d'une source d'alimentation au cours d'un processus de sauvegarde continue, la sauvegarde est interrompue.
  - L'option **Mode d'économie d'énergie** est activée par défaut. Si ce paramètre est activé, l'application Acronis Cyber Protect ne sauvegardera vos données que si la batterie de votre terminal n'est pas faible. Lorsque la batterie du terminal est faible, la sauvegarde continue est interrompue.
- Vous pouvez accéder aux données sauvegardées à partir de tous les terminaux mobiles enregistrés sur votre compte. Cela vous permet de transférer les données d'un ancien terminal mobile à un nouveau. Les contacts et les photos d'un terminal Android peuvent être récupérés sur un terminal iOS, et inversement. Vous pouvez également télécharger une photo, une vidéo ou un contact sur n'importe quel terminal à l'aide de la console Cyber Protect.
- Les données sauvegardées à partir des terminaux mobiles associés à votre compte sont uniquement disponible sous ce compte. Personne d'autre que vous ne peut visualiser et restaurer vos données.
- Dans l'application Acronis Cyber Protect, vous pouvez restaurer uniquement la dernière version des données. Si vous souhaitez effectuer une restauration à partir d'une version de sauvegarde en particulier, utilisez la console Cyber Protect sur une tablette ou sur un ordinateur.

© Acronis International GmbH, 2003-2026

- Les règles de rétention ne s'appliquent pas aux sauvegardes de terminaux mobiles.
- [Pour les terminaux Android uniquement] Si une carte SD est présente lors d'une sauvegarde, les données stockées sur cette carte sont également sauvegardées. Ces données seront restaurées sur la carte SD, vers le dossier **Restauré par la sauvegarde**, si la carte est présente lors de la restauration. À défaut, l'application demandera un autre emplacement vers lequel restaurer les données.

Où trouver l'application Acronis Cyber Protect

Selon le terminal mobile que vous possédez, installez l'application depuis l'App Store ou sur Google Play.

Comment commencer à sauvegarde vos données

1. Ouvrez l'application.
2. Connectez-vous à votre compte.
3. Appuyez sur **Configurer** pour créer votre sauvegarde. Notez que ce bouton ne s'affiche que si vous n'avez pas de sauvegarde de votre terminal mobile.
4. Sélectionnez les catégories de données que vous voulez sauvegarder. Par défaut, toutes les catégories sont sélectionnées.
5. [étape facultative] Activez **Chiffrer la sauvegarde** pour protéger votre sauvegarde par chiffrage. Dans ce cas, vous devrez également :
   a. Saisir un mot de passe de chiffrement deux fois.

      Remarque
      Assurez-vous de vous souvenir du mot de passe, car il est impossible de le restaurer ou de le modifier en cas d'oubli.

   b. Appuyez sur **Chiffrer**.
6. Sélectionnez **Sauvegarder**.
7. Autorisez l'application à accéder à vos données personnelles. Si vous refusez l'accès à certaines catégories de données, celles-ci ne seront pas sauvegardées.

La sauvegarde commence.

Comment restaurer les données vers un terminal mobile

Avertissement !
Pour restaurer des données mobiles, vous devez utiliser le compte de l'utilisateur final.

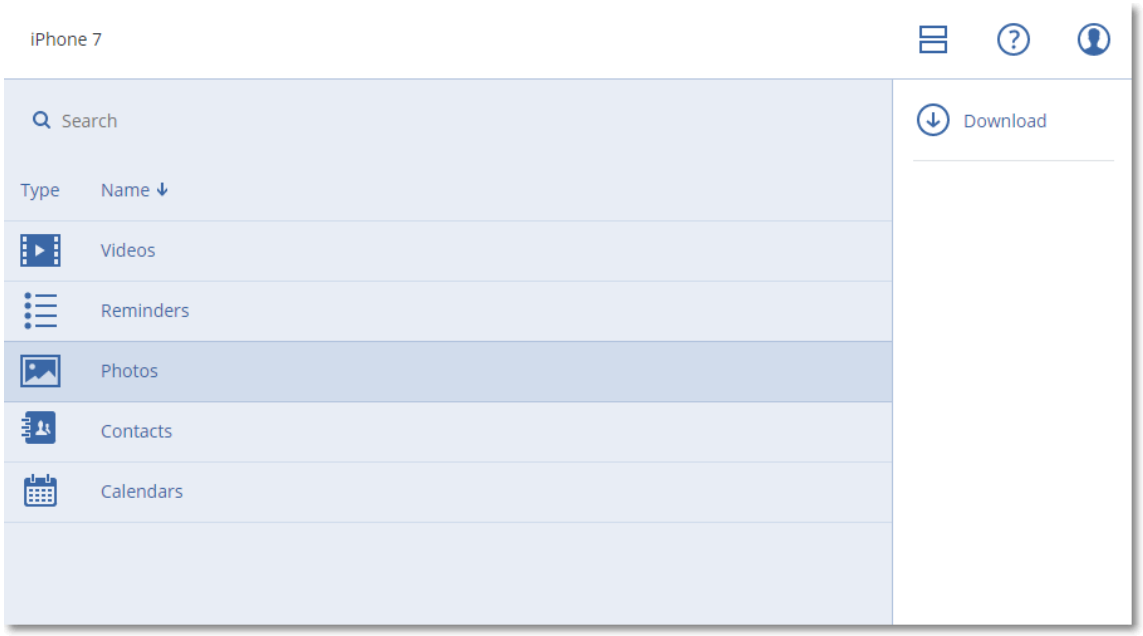
1. Ouvrez l'application Acronis Cyber Protect.
2. Appuyez sur **Parcourir**.
3. Entrez le nom du terminal.

© Acronis International GmbH, 2003-2026

4. Effectuez l'une des actions suivantes :
   - Pour restaurer toutes les données sauvegardées, appuyez sur **Tout restaurer**. Aucune autre action n'est requise.
   - Pour restaurer une ou plusieurs catégories de données, appuyez sur **Sélectionner**, puis sélectionnez les cases à cocher correspondant aux catégories de données requises. Appuyez sur **Restaurer**. Aucune autre action n'est requise.
   - Pour restaurer un ou plusieurs éléments de données appartenant à une même catégorie de données, sélectionnez la catégorie de données requise. Continuez avec les étapes ci-après.
5. Effectuez l'une des actions suivantes :
   - Pour restaurer un seul élément de données, sélectionnez-le en appuyant dessus.
   - Pour restaurer plusieurs éléments de données, appuyez sur **Sélectionner**, puis sélectionnez les cases correspondant aux éléments de données requis.
6. Appuyez sur **Restaurer**.

Comment examiner des données à partir de la console Cyber Protect

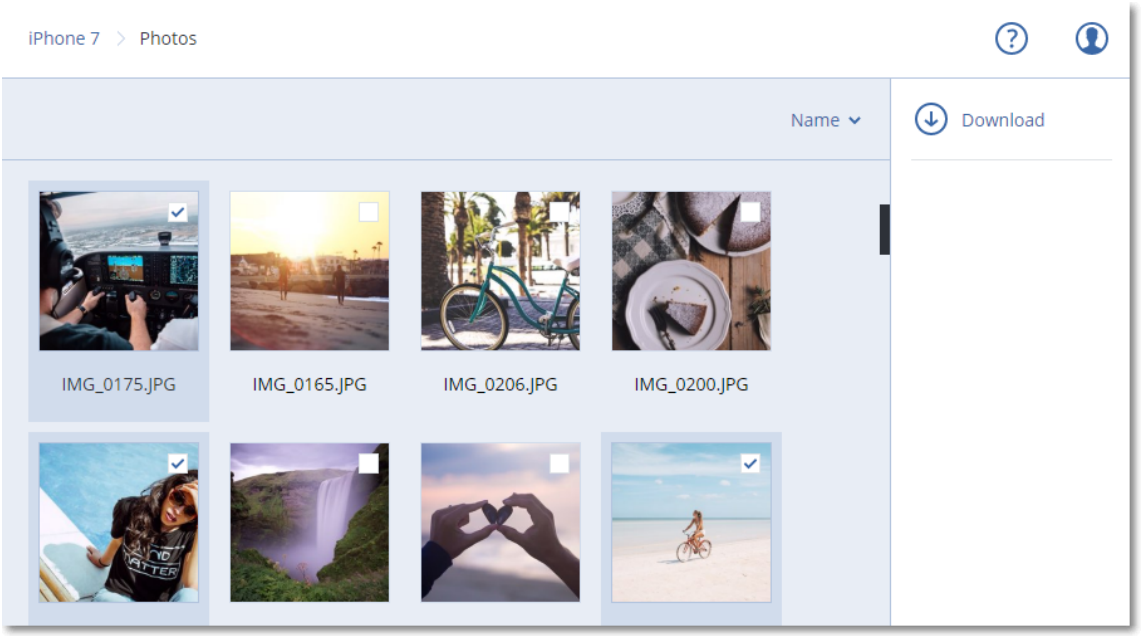
1. Sur un ordinateur, ouvrez un navigateur et saisissez l'URL de la console Cyber Protect.
2. Connectez-vous à votre compte.
3. Dans **Tous les terminaux**, cliquez sur **Restaurer** sous le nom de votre terminal mobile.
4. Effectuez l'une des actions suivantes :
   - Pour télécharger l'ensemble des photos, vidéos, contacts, calendriers ou rappels, sélectionnez les catégories de données correspondantes. Cliquez sur **Télécharger**.



   - Pour télécharger des photos, vidéos, contacts, calendriers ou rappels particuliers, cliquez sur les catégories de données correspondantes, puis sélectionnez les éléments de données

© Acronis International GmbH, 2003-2026

requis. Cliquez sur **Télécharger**.



- Pour afficher l'aperçu d'une photo ou d'un contact, cliquez sur le nom de la catégorie de données correspondante, puis sélectionnez l'élément de données requis.

Protection des données Microsoft 365

Les sauvegardes régulières des données Microsoft 365 offrent une couche de protection supplémentaire contre les erreurs des utilisateurs et les actions malveillantes intentionnelles. Vous pouvez restaurer les éléments supprimés d'une sauvegarde, même après expiration de la période de rétention de Microsoft 365. Par ailleurs, pour des raisons de conformité à d'éventuelles réglementations, il est possible de conserver une copie locale des boîtes aux lettres Exchange Online.

Vous pouvez sauvegarder les données Microsoft 365 en utilisant les solutions suivantes fournies par Cyber Protect Cloud :

- **Microsoft 365 Business – Sauvegarde**
- **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**
- **Agent pour Office 365** (agent installé localement)

Pour plus d'informations sur ces solutions, voir "Comparaison des solutions de sauvegarde pour les données Microsoft 365" (p. 845).

© Acronis International GmbH, 2003-2026

Important
Actions concernant les ressources de cloud à cloud telles que l'affichage du contenu d'e-mails sauvegardés, le téléchargement de pièces jointes ou de fichiers, la restauration d'e-mails sur des boîtes aux lettres autres que les boîtes aux lettres d'origine, ou l'envoi de tels contenus par e-mail pouvant constituer une violation de la confidentialité des utilisateurs. Ces actions sont consignées dans le portail de gestion, dans **Surveillance** > **Journal d'audit**.

Comparaison des solutions de sauvegarde pour les données Microsoft 365

Selon les services activés pour le tenant du client, les solutions de sauvegarde suivantes sont disponibles :

- **Microsoft 365 Business – Sauvegarde**
- **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**
- **Agent pour Office 365** (agent installé localement)

Remarque
Pour les tenants en mode de conformité, seul l'agent installé localement est disponible. Ces tenants ne peuvent sauvegarder que les boîtes aux lettres Microsoft 365. Ils ne peuvent pas utiliser les fonctionnalités étendues fournies par l'agent cloud.

Azure Information Protection (AIP) est pris en charge par toutes les solutions.

Le tableau suivant récapitule les fonctionnalités des solutions de sauvegarde.

Solution	Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365	Agent pour Office 365
Type d'agent	Agent cloud • L'agent cloud fournit des fonctionnalités de sauvegarde étendues, directement accessibles dans la console Cyber Protect • Aucune installation n'est nécessaire	Agent cloud • L'agent cloud fournit des fonctionnalités de sauvegarde étendues, directement accessibles dans la console Cyber Protect • Aucune installation n'est nécessaire	Agent local • L'agent installé localement permet de sauvegarder uniquement des boîtes aux lettres Exchange en ligne • L'agent doit être installé sur un ordinateur Windows connecté à Internet

© Acronis International GmbH, 2003-2026

Solution	Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365	Agent pour Office 365
Éléments de données qui peuvent être sauvegardés	• **Exchange Online** : ◦ boîtes aux lettres utilisateur et partagées (y compris les boîtes aux lettres des utilisateurs possédant un plan Kiosk et les boîtes aux lettres bloquées pour cause de litige) ◦ boîtes aux lettres de groupe ◦ dossiers publics • **OneDrive :** fichiers et dossiers utilisateur • **SharePoint Online** : ◦ sites de communication classiques ◦ sites d'équipe modernes ◦ éléments de données • **Microsoft 365 Teams** : ◦ équipes complètes ◦ canaux d'équipe ◦ fichiers de canal ◦ boîtes aux lettres d'équipe ◦ fichiers et e-mails dans les boîtes aux lettres d'équipe ◦ réunions ◦ sites d'équipe • **Bloc-notes OneNote** : dans le cadre de sauvegardes OneDrive,	• **Exchange Online** : ◦ boîte aux lettres de l'utilisateur • **OneDrive :** fichiers et dossiers utilisateur • **SharePoint Online** : ◦ sites de communication classiques ◦ sites d'équipe modernes	**Exchange Online** : boîtes aux lettres utilisateur et partagées (y compris les boîtes aux lettres des utilisateurs possédant un plan Kiosk et les boîtes aux lettres bloquées pour cause de litige)

© Acronis International GmbH, 2003-2026

Solution	Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365	Agent pour Office 365
	SharePoint Online et Microsoft 365 Teams		
Sauvegarde de boîtes aux lettres d'archive (**Archives permanentes**)	Oui	Oui	Non
Planification de sauvegarde	Jusqu'à six fois par jour*	Toutes les 10 minutes	Définie par l'utilisateur
Rétention de la sauvegarde	Flexible : par date ou par nombre de sauvegardes, ou illimité	Fixe • Pour les boîtes aux lettres : une année de sauvegardes fréquentes • Pour les comptes OneDrive et les sites SharePoint : un an, avec une période de deux semaines de sauvegardes fréquentes, puis des sauvegardes hebdomadaires pour le reste de la période	Flexible : par date ou par nombre de sauvegardes, ou illimité
Emplacements de sauvegardes	Stockage dans le Cloud (stockage hébergé par le partenaire compris)	Stockage de sauvegarde de Microsoft 365	Stockage dans le Cloud, dossier local, dossier réseau
Résilience de la sauvegarde	Fournie en standard : les centres de données de stockage dans le cloud ne sont pas situés dans les mêmes emplacements que les centres de données Microsoft	Réplication automatique vers d'autres conteneurs de stockage dans le réseau Microsoft	Non
Protection automatique des nouveaux utilisateurs, groupes,	Oui, en appliquant un plan de protection aux	Oui, en appliquant un plan de protection à	Non

© Acronis International GmbH, 2003-2026

Solution	Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365	Agent pour Office 365
sites et équipes Microsoft 365	groupes **Tous les utilisateurs**, **Tous les groupes**, **Tous les sites**, **Toutes les équipes**	**Tous les utilisateurs**, **Tous les groupes** et **Tous les sites**	
Protection de plus d'une organisation Microsoft 365	Oui	Oui	Non
Restauration granulaire	Oui	Non	Oui
Restauration vers un autre utilisateur dans la même organisation Microsoft 365 au sein de la même solution de sauvegarde	Oui	Non	Oui
Restauration vers une autre organisation Microsoft 365 du même tenant, dans la même solution de sauvegarde	Oui	Non	Non
Restauration vers un serveur Microsoft Exchange Server sur site	Non	Non	Non
Nombre maximum d'éléments pouvant être sauvegardés sans dégradation des performances	Jusqu'à 50 000 ressources protégées par entreprise**	Sans Objet	Lors d'une sauvegarde dans le stockage dans le cloud : 5 000 boîtes aux lettres par entreprise Lorsque vous effectuez une sauvegarde vers d'autres destinations : 2 000 boîtes aux lettres par plan de

© Acronis International GmbH, 2003-2026

Solution	Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365	Agent pour Office 365
			protection (aucune limite de nombre de boîtes aux lettres par entreprise)
Nombre maximal d'exécutions de sauvegardes manuelles	10 exécutions manuelles en une heure	Sans Objet	Illimité
Nombre maximal d'opérations de restauration simultanées	10 opérations, y compris les opérations de restauration Google Workspace	Sans Objet	Illimité
Performance	Vitesses types de la sauvegarde et de la restauration de cloud à cloud	Sauvegarde et restauration plus rapides, sans limitation des données	Vitesses types de sauvegarde et de restauration

* L'option par défaut est **Une fois par jour**. Vous pouvez planifier jusqu'à six sauvegardes par jour. Les sauvegardes démarrent à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud, qui dessert plusieurs clients dans un centre de données. Cela garantit une charge uniforme tout au long de la journée et une qualité de service équivalente pour tous les clients.

Remarque
La planification de la protection peut être affectée par le fonctionnement de services tiers, par exemple, l'accessibilité des serveurs Microsoft 365, les paramètres de limitation sur les serveurs Microsoft, etc. Voir également Conseils de limitation sur Microsoft Graph.

** Le nombre maximal de ressources dépend de leur type : 50 000 boîtes aux lettres Exchange, 10 000 équipes, 10 000 sites SharePoint ou 5 000 comptes OneDrive.

Pour calculer les combinaisons prises en charge, utilisez la formule suivante :

```
10 mailboxes = 2 teams = 2 sites = 1 OneDrive account
```

Par exemple :

- 50 000 boîtes aux lettres
- 40 000 boîtes aux lettres et 1 000 comptes OneDrive
- 40 000 boîtes aux lettres et 2 000 sites

© Acronis International GmbH, 2003-2026

- 40 000 boîtes aux lettres et 2 000 équipes
- 30 000 boîtes aux lettres, 1 000 comptes OneDrive, 1 000 sites et 1 000 équipes
- 30 000 boîtes aux lettres, 2 000 sites et 2 000 équipes

Nous vous recommandons de sauvegarder les ressources de manière séquentielle et dans l'ordre suivant :

1. Boîtes aux lettres
2. Comptes OneDrive
3. Teams
4. Sites SharePoint

La première sauvegarde complète peut prendre plusieurs jours, selon le nombre d'éléments protégés et leur taille. Ne démarrez pas la sauvegarde suivante avant la fin de la précédente.

Limites

- Tous les utilisateurs ayant une boîte aux lettres ou un compte OneDrive s'affichent dans la console Cyber Protect, y compris les utilisateurs qui ne possèdent pas de licence Microsoft 365 et les utilisateurs dont la connexion aux services Microsoft 365 est bloquée.
- Une sauvegarde de boîte aux lettres inclut uniquement des dossiers visibles pour les utilisateurs. Le dossier **Éléments récupérables** et ses sous-dossiers (**Suppressions**, **Versions**, **Purges**, **Audits**, **DiscoveryHold**, **Journalisation du calendrier**) ne sont pas inclus dans une sauvegarde de boîte aux lettres.
- La création automatique d'utilisateurs, de dossiers publics, de groupes ou de sites lors d'une restauration est impossible. Par exemple, si vous souhaitez restaurer un site SharePoint Online supprimé, commencez par créer un site manuellement, puis choisissez-le en tant que site cible lors d'une restauration.
- Vous ne pouvez pas simultanément restaurer des éléments depuis différents points de restauration, même si vous pouvez sélectionner ces éléments dans les résultats de recherche.
- Lors d'une sauvegarde, toute étiquette de confidentialité appliquée au contenu sera préservée. Par conséquent, le contenu sensible ne s'affichera peut-être pas s'il est restauré vers un emplacement autre que l'emplacement d'origine et si l'utilisateur dispose de droits d'accès différents.
- [Pour **Microsoft 365 Business – Sauvegarde**] Vous ne pouvez appliquer à une ressource qu'un seul plan de sauvegarde individuel.
- [Pour **Microsoft 365 Business – Sauvegarde**] Lorsqu'un plan de sauvegarde individuel et un plan de sauvegarde de groupe sont appliqués à la même ressource, les paramètres du plan individuel sont prioritaires.
- [Pour **une sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**] Vous pouvez créer et appliquer un plan de sauvegarde par type de données (boîtes aux lettres Exchange, sites SharePoint ou comptes OneDrive).
- **Direct Backup to Public Cloud** n’est pas pris en charge.

© Acronis International GmbH, 2003-2026

Droits utilisateurs requis

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde** et à **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**.

L'utilisation de l'agent cloud nécessite les droits d'utilisateur suivants dans Cyber Protect Cloud et dans Microsoft 365.

Dans Cyber Protect Cloud

- Avec **Microsoft 365 Business – Sauvegarde**, l'agent cloud peut être utilisé à la fois au niveau du tenant du client et au niveau de l'unité. Pour plus d'informations sur ces niveaux et leurs administrateurs respectifs, voir "Administration d'organisations Microsoft 365 organisations ajoutées à différents niveaux" (p. 854).
- Avec **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, l'agent cloud peut être utilisé au niveau du tenant du client.
- L'agent local doit être enregistré sous un compte d'administrateur d'entreprise et utilisé au niveau du tenant client. Les administrateurs d'entreprise agissant au niveau de l'unité, les administrateurs d'unité et les utilisateurs ne peuvent pas sauvegarder ou récupérer les données Microsoft 365.

Dans Microsoft 365

- Votre compte doit bénéficier du rôle d'administrateur global dans Microsoft 365.
- Pour découvrir, sauvegarder et restaurer des dossiers publics Microsoft 365, au moins un de vos comptes d'administrateur Microsoft 365 doit disposer d'une boîte aux lettres et de droits d'accès en lecture/écriture aux dossiers publics que vous souhaitez sauvegarder.
  - L'agent local se connectera à Microsoft 365 en utilisant ce compte. Pour permettre à l'agent d'accéder au contenu de toutes les boîtes aux lettres, ce compte se verra attribuer le rôle de gestion **ApplicationImpersonation**. Si vous modifiez le mot de passe du compte, mettez-le à jour dans la console Cyber Protect, comme décrit dans "Modification des identifiants de Microsoft 365" (p. 914).
  - L'agent cloud ne se connecte pas à Microsoft 365. Pour accorder à l'agent cloud les autorisations nécessaires à son fonctionnement, vous devez vous connecter à Microsoft 365 en tant qu'administrateur général.

    Le tableau suivant récapitule les autorisations nécessaires.

Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365
▪ Se connecter et lire le profil utilisateur ▪ Lire et écrire des fichiers dans toutes les	▪ Utiliser les services Web d'Exchange avec un accès complet à toutes les boîtes aux lettres

© Acronis International GmbH, 2003-2026

Microsoft 365 Business – Sauvegarde	Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365
collections de sites ▪ Lire et écrire les profils complets de tous les utilisateurs ▪ Lire et écrire tous les groupes ▪ Lire les données du répertoire ▪ Lire tous les messages du canal ▪ Lire et écrire des métadonnées gérées ▪ Lire et écrire des éléments et des listes dans toutes les collections de sites ▪ Avoir un contrôle total de toutes les collections de sites ▪ Utiliser les services Web d'Exchange avec un accès complet à toutes les boîtes aux lettres	▪ Lire et écrire des éléments dans toutes les collections de sites ▪ Lire et écrire des éléments et des listes dans toutes les collections de sites ▪ Avoir un contrôle total de toutes les collections de sites ▪ Lire toutes les stratégies de configuration de sauvegarde ▪ Lire et modifier toutes les stratégies de configuration de sauvegarde ▪ Lire toutes les sessions de restauration ▪ Lire et restaurer toutes les sessions, et démarrer la restauration des sessions à partir des sauvegardes ▪ Lire toutes les informations de surveillance, de quota et de facturation pour le tenant ▪ Rechercher les propriétés de métadonnées dans tous les instantanés de sauvegarde ▪ Mettre à jour ou lire le statut du service de sauvegarde M365 ▪ Lire le statut du service de sauvegarde M365 ▪ Lire les profils complets de tous les utilisateurs ▪ Lire les informations de l'organisation ▪ Mettre à jour ou lire le statut du service de sauvegarde M365 ▪ Se connecter et lire le profil utilisateur ▪ Lire et écrire les profils complets de tous les utilisateurs ▪ Lire des fichiers dans toutes les collections de sites ▪ Lire tous les groupes ▪ Lire les données du répertoire

- L'agent cloud ne stocke pas les identifiants de votre compte et ne les utilise pas pour effectuer des sauvegardes et des restaurations. La modification des identifiants, la désactivation ou la suppression du compte n'affectent pas le fonctionnement de l'agent cloud.

© Acronis International GmbH, 2003-2026

Ajout d'une organisation Microsoft 365

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde** et à **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**.

Avec **Microsoft 365 Business – Sauvegarde**, vous pouvez ajouter une organisation Microsoft 365 à un tenant ou à une unité de client.

Avec **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, vous pouvez ajouter une organisation Microsoft 365 à un tenant de client.

Pour ajouter une organisation Microsoft 365, vous devez disposer des droits d'administrateur pour le tenant ou l'unité du client.

Vous pouvez ajouter plusieurs organisations Microsoft 365 dans le tenant, mais vous ne pouvez pas ajouter la même organisation Microsoft 365 dans **Microsoft 365 Business – Sauvegarde** et **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**.

Pour ajouter une organisation Microsoft 365

1. [Pour ajouter une organisation Microsoft 365 dans le tenant du client] Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. [Pour ajouter une organisation Microsoft 365 dans une unité, uniquement pour **Microsoft 365 Business – Sauvegarde**] Selon votre rôle, procédez comme suit :
   a. [Pour les administrateurs d'unité] Connectez-vous à la console Cyber Protect en tant qu'administrateur d'unité.
   b. [Pour les administrateurs d'entreprise agissant au niveau de l'unité] Accédez à l'unité dans laquelle vous souhaitez ajouter l'organisation.
3. Cliquez sur **Terminaux** > **Ajouter**.
4. Sélectionnez la solution de sauvegarde.
   En fonction des services activés pour votre tenant, vous pouvez choisir l'une des options suivantes :
   - **Microsoft 365 Business – Sauvegarde**
   - **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**
   - **Microsoft 365**
     Cette option est affichée lorsque **Microsoft 365 Business – Sauvegarde** et **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365** sont activés pour votre tenant. Pour plus d'informations sur les différences entre ces solutions, voir "Comparaison des solutions de sauvegarde pour les données Microsoft 365" (p. 845).
5. [Si vous avez sélectionné **Microsoft 365**] Sélectionnez **Microsoft 365 Business – Sauvegarde** ou **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, puis cliquez sur **Continuer**.

© Acronis International GmbH, 2003-2026

6. Sur la page de connexion de Microsoft 365, connectez-vous avec les identifiants d'administrateur global Microsoft 365.

   Remarque
   Ce compte est utilisé uniquement pour ajouter l'organisation Microsoft 365 à la console Cyber Protect. Pour des raisons de sécurité, vous pouvez utiliser un compte d'administrateur global dédié pour cette opération. Après avoir ajouté l'organisation, vous pouvez supprimer le compte dédié, qui n'est plus nécessaire.

   Microsoft 365 affiche une liste des permissions nécessaires pour sauvegarder et restaurer les données de votre organisation.
7. Confirmez que vous accordez les autorisations requises.

En fonction de la solution sélectionnée, vous verrez l'organisation Microsoft 365 dans la console Cyber Protect, dans l'onglet **Terminaux** > **Microsoft 365** ou **Terminaux** > **Sauvegarde directe pour Microsoft 365**.

Administration d'organisations Microsoft 365 organisations ajoutées à différents niveaux

Remarque
Avec **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, vous pouvez ajouter des organisations uniquement au niveau tenant du client.

Les administrateurs d'entreprise disposent d'un accès complet aux organisations Microsoft 365 ajoutées au niveau tenant client.

Les administrateurs d'entreprise disposent d'un accès limité aux organisations ajoutées à une unité. Dans ces organisations, qui s'affichent avec le nom d'unité entre crochets, ils peuvent effectuer les opérations suivantes :

- Restaurer des données à partir de sauvegardes
  Les administrateurs d'entreprise peuvent restaurer des données dans toutes les organisations du tenant, quel que soit le niveau auquel ces organisations sont ajoutées.
- Parcourir des sauvegardes et des points de restauration dans des sauvegardes
- Supprimer des sauvegardes et des points de restauration dans des sauvegardes
- Afficher les alertes et les activités

Les administrateurs d'entreprise, lorsqu'ils agissent au niveau tenant client, ne peuvent effectuer les tâches suivantes :

- Ajouter des organisations Microsoft 365 à des unités
- Supprimer des organisations Microsoft 365 dans des unités
- Synchroniser des organisations Microsoft 365 qui ont été ajoutées une unité

© Acronis International GmbH, 2003-2026

- Afficher, créer, modifier, supprimer, appliquer, exécuter ou révoquer des plans de protection pour des éléments de données d'organisations Microsoft 365 qui ont été ajoutées à une unité.

Les administrateurs d'unité et les administrateurs d'entreprise agissant au niveau unité disposent d'un accès complet aux organisations ajoutées à une unité. Toutefois, ils n'ont pas accès aux éventuelles ressources provenant du tenant client parent, y compris aux plans de protection créés au sein de ce dernier.

Découverte de ressources Microsoft 365

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde** et à **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**.

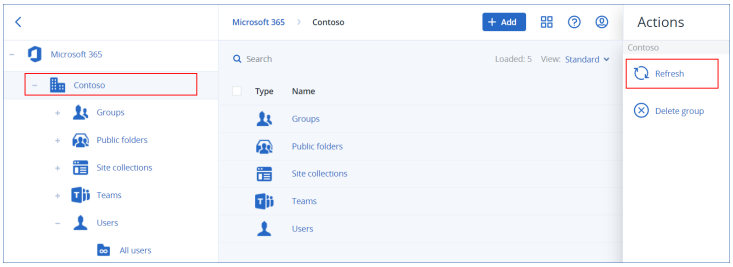
Lorsque vous ajoutez à Cyber Protect Cloud une organisation Microsoft 365, les ressources de cette organisation (boîtes aux lettres Exchange, comptes OneDrive ou sites SharePoint, par exemple) sont synchronisées avec la console Cyber Protect. Cette opération est appelée découverte et elle est consignée dans **Surveillance** > **Activités**.

Une fois la découverte terminée, vous pouvez voir les ressources de l'organisation Microsoft 365 dans la console Cyber Protect et pouvez leur appliquer des plans de sauvegarde.

Une opération de découverte automatique est exécutée une fois par jour afin que la liste des ressources dans la console Cyber Protect soit à jour. Vous pouvez synchroniser cette liste à la demande en réexécutant une opération de découverte manuellement.

Pour exécuter une opération de découverte manuellement

1. [Pour **Microsoft 365 Business – Sauvegarde**] Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft 365**.
2. [Pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**] Dans la console Cyber Protect, accédez à **Terminaux** > **Sauvegarde directe pour Microsoft 365**.
3. Sélectionnez l'organisation Microsoft 365, puis cliquez dans le panneau **Actions** sur **Actualiser**.



Remarque
Vous pouvez exécuter manuellement jusqu'à 10 découvertes par heure. Lorsque ce nombre est atteint, le nombre d'exécutions autorisé est réinitialisé à un par heure, puis une exécution supplémentaire est alors disponible toutes les heures jusqu'à ce qu'un total de 10 exécutions par heure soit atteint.

© Acronis International GmbH, 2003-2026

Conseils utiles

- L'agent cloud se synchronise avec Microsoft 365 toutes les 24 heures, à compter du moment où l'organisation est ajoutée au service Cyber Protection. Si vous ajoutez ou supprimez un utilisateur, un groupe ou un site, ce changement ne sera pas immédiatement visible dans la console Cyber Protect. Pour synchroniser la modification immédiatement, exécutez une opération de découverte manuellement.
- Si vous appliquez un plan de sauvegarde à **Tous les groupes**, **Tous les dossiers publics**, **Toutes les collections de sites**, **Toutes les équipes** ou **Tous les utilisateurs**, les éléments qui viennent d'être ajoutés seront inclus dans la sauvegarde après synchronisation.
- Conformément à la politique de Microsoft, lorsqu'un utilisateur, un groupe ou un site est supprimé de l'interface graphique de Microsoft 365, il reste disponible pendant quelques jours via une API. Pendant cette période, l'élément supprimé est inactif (grisé) dans la console Cyber Protect et n'est pas sauvegardé. Lorsque l'élément supprimé devient indisponible via l'API, il disparaît de la console Cyber Protect. Vous trouverez, le cas échéant, les sauvegardes de l'utilisateur supprimé dans la console Cyber Protect, dans l'onglet **Stockage de sauvegarde** > **Sauvegardes d'applications cloud**.

Suppression d'une organisation Microsoft 365

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde** et à **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**.

La suppression d'une organisation Microsoft 365 n'affecte pas les sauvegardes existantes des données de cette organisation. Si vous n'avez plus besoin de ces sauvegardes, commencez par les supprimer, puis supprimez l'organisation Microsoft 365. Sinon, les sauvegardes utiliseront toujours de l'espace de stockage dans le cloud, qui est susceptible de vous être facturé. Pour plus d'informations sur la suppression des sauvegardes, voir "Pour supprimer des sauvegardes ou des archives de sauvegarde" (p. 738).

Pour supprimer une organisation Microsoft 365

1. [Pour supprimer une organisation Microsoft 365 au niveau tenant d'un client] Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. [Pour supprimer une organisation Microsoft 365 au niveau d'une unité] Selon votre rôle, procédez comme suit :
   a. [Pour les administrateurs d'unité] Connectez-vous à la console Cyber Protect en tant qu'administrateur d'unité.
   b. [Pour les administrateurs d'entreprise agissant au niveau de l'unité] Accédez à l'unité dans laquelle l'organisation est ajoutée.
3. Accédez à **Terminaux**, puis sélectionnez la solution de sauvegarde utilisée par cette organisation :

© Acronis International GmbH, 2003-2026

- **Microsoft 365 Business – Sauvegarde**
- **Sauvegarde directe pour Microsoft 365**

4. Sélectionnez l'organisation, puis cliquez sur **Supprimer**.

Par conséquent, les plans de sauvegarde appliqués à cette organisation seront révoqués et les ressources qu'elle contient ne seront plus protégées.

Révoquez ensuite les droits d'accès accordés à l'application de service de sauvegarde. Pour plus d'informations, voir "Révocation des droits d'accès de l'application de service de sauvegarde" (p. 857).

Révocation des droits d'accès de l'application de service de sauvegarde

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde** et à **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**.

Lorsque vous ajoutez une organisation Microsoft 365 à la console Cyber Protect, vous accordez les droits d'accès de l'application **Service de sauvegarde** à l'organisation Microsoft 365. Après avoir supprimé l'organisation Microsoft 365 de la console Cyber Protect, vous devez révoquer ces droits d'accès.

Pour plus d'informations sur la suppression d'une organisation, voir "Suppression d'une organisation Microsoft 365" (p. 856).

Pour révoquer les droits d'accès

1. Connectez-vous à Microsoft 365 en tant qu'administrateur général.
2. Accédez au **centre d'administration Microsoft Entra** > **Identité** > **Applications** > **Applications d'entreprise** > **Toutes les applications**.
3. Sélectionnez l'application **Service de sauvegarde**.
4. Accédez à l'onglet **Propriétés**, puis cliquez sur **Supprimer** dans le menu vertical.
5. Confirmez la suppression.

L'application **Service de sauvegarde** est supprimée et les droits d'accès aux données de l'organisation Microsoft 365 sont révoqués.

Rapport des licences de poste Microsoft 365

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde**. Avec **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**, cette fonctionnalité n'est pas disponible.

© Acronis International GmbH, 2003-2026

Les administrateurs d'entreprise peuvent télécharger un rapport au sujet des postes Microsoft 365 protégés et de leurs licences. Le rapport est au format CSV, et comprend des informations sur la licence d'un poste ainsi que sur la raison de l'utilisation d'une licence. Il inclut aussi le nom du poste protégé, l'e-mail associé, le groupe, l'organisation Microsoft 365, le nom et le type de la ressource protégée.

Ce rapport est disponible uniquement pour les tenants dans lesquels une organisation Microsoft 365 a été enregistrée.

Pour télécharger le rapport des licences de poste Microsoft 365

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur de l'entreprise.
   Vous pouvez télécharger un reporting uniquement pour le niveau de tenant où vous travaillez actuellement. Par exemple, au niveau du tenant client, vous pouvez télécharger un reporting pour le tenant client. Au niveau de l'unité, vous pouvez télécharger un reporting pour une unité spécifique.
2. [Pour télécharger un reporting pour une unité] Passez au niveau de l'unité.
3. Cliquez sur l'icône de compte dans l'angle supérieur droit.
4. Cliquez sur le **rapport des licences de poste Microsoft 365**.

Configuration de la fréquence des sauvegardes Microsoft 365

Remarque
Cette rubrique s'applique à **Microsoft 365 Business – Sauvegarde**. Avec **Sauvegarde directe dans le stockage de sauvegarde de Microsoft**, cette fonctionnalité n'est pas disponible.

Avec les fonctionnalités standard incluses, les sauvegardes de Microsoft 365 s'exécutent par défaut une fois par jour et aucune option de planification supplémentaire n'est disponible.

Si la fonctionnalité de sauvegarde est activée dans votre tenant, l'option **Une fois par jour** est activée par défaut, et d'autres fréquences sont disponibles à la sélection.

Vous pouvez sélectionner le nombre de sauvegardes par jour, mais vous ne pouvez pas configurer l'heure de leur démarrage. Les sauvegardes démarrent automatiquement à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud desservant les nombreux clients d'un centre de données. De cette manière, la charge est égale toute la journée, ce qui garantit une qualité de service équivalente pour tous les clients.

Les options suivantes sont disponibles.

Planification des options	Intervalle approximatif entre chaque sauvegarde
Une fois par jour (par défaut)	24 heures
Deux fois par jour	12 heures

© Acronis International GmbH, 2003-2026

Planification des options	Intervalle approximatif entre chaque sauvegarde
Trois fois par jour	8 heures
Six fois par jour	4 heures

Remarque
Selon la charge sur l'agent cloud et les limitations possibles côté Microsoft 365, une sauvegarde peut démarrer plus tard ou prendre plus de temps que prévu. Si une sauvegarde est plus longue que l'intervalle moyen entre deux sauvegardes, la sauvegarde suivante est replanifiée, ce qui peut avoir pour résultat un nombre de sauvegardes quotidiennes inférieur au nombre sélectionné. Par exemple, il est possible que deux sauvegardes par jour seulement puissent s'effectuer, même si vous en avez sélectionné six.

Les sauvegardes de boîtes aux lettres de groupe ne peuvent être exécutées qu'une fois par jour.

Microsoft 365 Business – Sauvegarde

Remarque
Cette fonctionnalité est disponible dans les tenants de clients pour les **postes Microsoft 365** (**boîtes aux lettres**, **OneDrive**) et **Microsoft 365 SharePoint Online** sélectionnés dans **Protection standard** sur le portail de gestion.

Si certaines des cases ne sont pas cochées, la fonctionnalité sera disponible partiellement.

Les données sauvegardées sont compressées automatiquement et utilisent moins d'espace dans l'emplacement de sauvegarde que dans leur emplacement d'origine. Le niveau de compression des sauvegardes de cloud à cloud est fixe et correspond au niveau **Normal** des sauvegardes non-cloud à cloud. Pour en savoir plus sur ces niveaux, voir "Niveau de compression" (p. 618).

Plans de sauvegarde appliqués et planifiés pour les ressources Microsoft 365

Vous pouvez appliquer un seul plan de sauvegarde par service à une ressource Microsoft 365 individuelle. Pour plus d'informations sur les services disponibles par ressource, voir "Affichage de l'état de protection d'une ressource Microsoft 365 par service" (p. 860).

Par exemple, vous pouvez appliquer un seul plan de sauvegarde de boîte aux lettres à un utilisateur Microsoft 365. Vous pouvez également appliquer le même type de plan (sauvegarde de boîte aux lettres) à un ou plusieurs groupes dynamiques ou groupes statiques contenant cette ressource. Dans ce cas, la boîte aux lettres de l'utilisateur peut être sauvegardée par plus d'un plan de sauvegarde.

© Acronis International GmbH, 2003-2026

Important
Seul le plan qui est appliqué en premier s'exécutera automatiquement selon la planification. Les autres plans seront appliqués avec succès à la ressource, mais ne pourront être exécutés que manuellement.

Par exemple :

- Vous appliquez le plan A (sauvegarde de boîte aux lettres) à l'utilisateur John Doe. Vous ne pouvez pas appliquer un autre plan de sauvegarde de boîte aux lettres (plan B) au même utilisateur car le plan A est déjà appliqué.
- Vous appliquez le plan B (sauvegarde de boîte aux lettres) à un groupe dynamique ou groupe statique qui contient John Doe. Vous ne pouvez pas appliquer un autre plan de boîte aux lettres (plan C) au même groupe dynamique car le plan B est déjà appliqué.
- Vous appliquez le plan C (sauvegarde de boîte aux lettres) à **Tous les groupes**, ou à un autre groupe dynamique ou groupe statique qui contient John Doe.

En conséquence, le plan A, le plan B et le plan C peuvent sauvegarder la boîte aux lettres de John Doe, mais seul le plan A s'exécutera selon la planification pour cet utilisateur, car il a été appliqué en premier. Vous pouvez exécuter manuellement le plan B et le plan C pour John Doe. Le plan B et le plan C s'exécuteront selon la planification pour les utilisateurs ou groupes sur lesquels chacun de ces plans est le premier appliqué.

Affichage de l'état de protection d'une ressource Microsoft 365 par service

En fonction du type de ressource Microsoft 365, vous pouvez protéger les services suivants :

Ressource	Services
Groupes*	Boîte de réception
	Site
Dossiers publics	Boîte de réception
Collections de sites	Site
Teams	Canaux d'équipe
Utilisateurs	Boîte de réception
	OneDrive

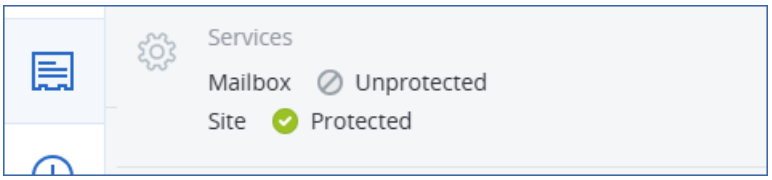
* Les groupes contiennent des sites modernes (d'équipe) et des boîtes aux lettres de groupe. Les groupes qui font partie d'une équipe peuvent être sauvegardés deux fois s'ils sont protégés à la fois en tant que groupe et en tant que partie de l'équipe. Pour plus d'informations, voir "Éviter les sauvegardes en double des groupes Microsoft 365" (p. 862).

© Acronis International GmbH, 2003-2026

Si plusieurs services sont disponibles pour une ressource mais qu'un seul est protégé, la ressource est partiellement protégée. Par exemple, si la boîte aux lettres d'un utilisateur est sauvegardée mais que les fichiers OneDrive ne le sont pas, cet utilisateur est partiellement protégé.

Pour vérifier l'état de protection par service

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Terminaux** > **Microsoft 365** > Organisation Microsoft 365.
3. Sélectionnez une ressource, puis cliquez sur **Détails**.
4. Vérifiez la section **Services**.
   Par exemple :



Révocation d'un plan de sauvegarde pour Microsoft 365 Business – Sauvegarde

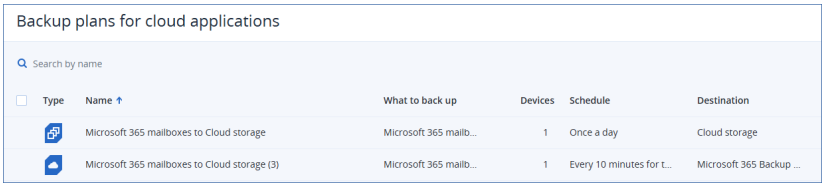
Vous pouvez révoquer un plan de sauvegarde dans l'onglet **Gestion** > **Sauvegardes d'applications cloud** ou dans l'onglet **Terminaux**.

Vous pouvez révoquer un plan de sauvegarde à partir d'une ressource individuelle ou d'un groupe de terminaux.

Révoquer un plan de sauvegarde

Gestion > Sauvegarde d'applications cloud

1. Dans la console Cyber Protect, accédez à **Gestion**, puis cliquez sur **Sauvegardes d'applications cloud**.
2. Sélectionnez un plan de sauvegarde pour **Microsoft 365 Business – Sauvegarde**, puis cliquez sur **Modifier**.
   Vous pouvez distinguer les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** et **Microsoft 365 Business – Sauvegarde** en comparant leurs icônes et la destination de la sauvegarde. Les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** ne peuvent utiliser que le stockage de sauvegarde Microsoft 365.



© Acronis International GmbH, 2003-2026

a. Cliquez sur **Terminaux**.

b. Sélectionnez les ressources ou les groupes de terminaux pour lesquels vous souhaitez révoquer le plan, puis cliquez sur **Supprimer**.

c. Cliquez sur **Terminé**.

3. Cliquez sur **Enregistrer**.

En conséquence, le plan de sauvegarde est révoqué pour toutes les ressources qui ont été supprimées.

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux**, puis cliquez sur **Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. [Pour les ressources individuelles] Sélectionnez une ressource à partir de laquelle vous souhaitez révoquer un plan de sauvegarde, puis cliquez sur **Sauvegarde**.

   Les plans de sauvegarde appliqués à un groupe dynamique ou statique sont verrouillés. Vous pouvez les révoquer au niveau du groupe.
4. [Pour les groupes de terminaux] Sélectionnez un groupe à partir duquel vous souhaitez révoquer un plan de sauvegarde, puis cliquez sur **Sauvegarde de groupe**.
5. Cliquez sur l'icône en forme d'engrenage située à côté du nom du plan de sauvegarde, puis sur **Retirer**.

Éviter les sauvegardes en double des groupes Microsoft 365

Des sauvegardes en double peuvent se produire lorsqu'un groupe Microsoft 365 qui fait partie d'une équipe Microsoft est sauvegardé à la fois sous **Teams** et **Groupes** :

- Sauvegarde Teams

  Dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Teams**, vous pouvez configurer une sauvegarde d'équipe. Celle-ci inclut le site SharePoint, la boîte aux lettres de groupe et d'autres données associées à l'équipe.
- Sauvegarde des groupes

  Dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**, vous pouvez configurer une sauvegarde pour le site SharePoint et la boîte aux lettres de groupe.

Groupe		Groupes apparaît dans Terminaux > Microsoft 365 > Groupes	Possibilité de sauvegardes en double
Groupe n'appartenant pas à une équipe	Un plan de groupe* est appliqué	Oui	Non
	Un plan de groupe n'est pas appliqué	Oui	Non

© Acronis International GmbH, 2003-2026

Groupe		Groupes apparaît dans Terminaux > Microsoft 365 > Groupes	Possibilité de sauvegardes en double
Groupe dans une équipe	Un plan de groupe est appliqué	Oui Ces groupes sont marqués avec une icône d'avertissement  , car ils pourraient être sauvegardés deux fois, à la fois sous **Groupes** et **Teams**. Si vous ne sauvegardez pas un tel groupe dans le cadre d'une équipe, vous pouvez ignorer cet avertissement. Si vous sauvegardez un tel groupe dans le cadre d'une équipe, évitez les sauvegardes en double en configurant la protection uniquement dans l'équipe concernée.	Oui
	Un plan de groupe n'est pas appliqué	Non À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).	Non

* Un plan de groupe est un plan de sauvegarde pour les sites SharePoint ou les boîtes aux lettres qui est appliqué sous **Groupes**.

Pour éviter les sauvegardes en double d'un groupe Microsoft 365

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes** > **Tous les groupes**.
3. Vérifiez la colonne **Équipe**.

© Acronis International GmbH, 2003-2026

- Si la colonne est vide, le groupe ne fait pas partie d'une équipe.
- Si la colonne montre un nom d'équipe, le groupe fait partie d'une équipe.

  Une icône d'avertissement  indique que ce groupe pourrait avoir des sauvegardes en double, à la fois sous **Groupes** et **Teams**.

4. [Si la sauvegarde est configurée à la fois sous **Groupes** et **Teams**] Configurez la sauvegarde uniquement au niveau de l'équipe.
   - Accédez à **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Teams** > **Toutes les équipes**, puis assurez-vous qu'un plan de sauvegarde est appliqué à l'équipe qui inclut ce groupe.
   - Accédez à **Terminaux** > **Microsoft 365** > organisation Microsoft 365 > **Groupes** > **Tous les groupes**, puis révoquez les plans de sauvegarde de groupe. Pour plus d'informations, voir "Révocation d'un plan de sauvegarde pour Microsoft 365 Business – Sauvegarde" (p. 861).

   Remarque
   Les plans appliqués au niveau d'un groupe ne peuvent être révoqués qu'au niveau du groupe. Par exemple, vous ne pouvez pas révoquer un plan appliqué à **Tous les groupes** en modifiant le paramètre de protection pour une ressource spécifique dans le groupe. Pour plus d'informations, voir "Révoquer un plan de sauvegarde" (p. 861) > Terminaux > étape 4.

Protection des données Exchange Online

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des boîtes aux lettres utilisateur, communes et de groupe. (Facultatif) Vous pouvez également choisir de sauvegarder les boîtes aux lettres d'archive en ligne (**Archives permanentes**) des boîtes aux lettres sélectionnées.

À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

Si votre organisation Microsoft 365 a été ajoutée avant Cyber Protect 8.0, vous devez répéter les étapes décrites dans "Ajout d'une organisation Microsoft 365" (p. 853) pour pouvoir sauvegarder les dossiers publics. Vous n'avez pas besoin de supprimer l'organisation avant de l'ajouter à nouveau.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers de courriers électroniques
- Messages de courriers électroniques

© Acronis International GmbH, 2003-2026

- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Les éléments suivants peuvent être restaurés à partir d'une sauvegarde de dossier public :

- Sous-dossiers
- Publications
- Messages de courriers électroniques

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Lorsque vous restaurez des boîtes aux lettres, des éléments de boîte aux lettres, des dossiers publics et des éléments de dossiers publics, vous pouvez choisir d'écraser ou non les éléments de l'emplacement de destination.

Sélection de boîtes aux lettres

Sélectionnez les boîtes aux lettres que vous souhaitez protéger, puis appliquez-leur un plan de sauvegarde.

Vous pouvez créer un nouveau plan ou sélectionner un plan existant.

Pour sélectionner des boîtes aux lettres Exchange Online et appliquer un plan de sauvegarde

Nouveau plan

1. Dans la console Cyber Protect, sous **Terminaux**, cliquez sur **Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
   - [Pour sauvegarder les boîtes aux lettres de tous les utilisateurs et toutes les boîtes aux lettres communes, y compris celles qui seront créées à l'avenir] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sauvegarder des boîtes aux lettres d'utilisateurs ou des boîtes aux lettres partagées] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez les boîtes aux lettres que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.
   - [Pour sauvegarder toutes les boîtes aux lettres de groupe, y compris celles des groupes qui seront créés à l'avenir] Développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.

© Acronis International GmbH, 2003-2026

Remarque
À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

Remarque
Au moins un des propriétaires du groupe doit être un utilisateur Microsoft 365 sous licence disposant d'une boîte aux lettres. Si le groupe est privé ou si son appartenance est masquée, le propriétaire doit également être membre du groupe.

- [Pour sauvegarder des boîtes aux lettres de groupe en particulier] Développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez les boîtes aux lettres que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.

Remarque
À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

Remarque
Au moins un des propriétaires du groupe doit être un utilisateur Microsoft 365 sous licence disposant d'une boîte aux lettres. Si le groupe est privé ou si son appartenance est masquée, le propriétaire doit également être membre du groupe.

4. Pour créer un plan de sauvegarde, cliquez sur **Créer**.
5. Dans le plan de sauvegarde, configurez les options suivantes :
   - [Si disponible] Dans **Quoi sauvegarder**, sélectionnez **Boîtes aux lettres Microsoft 365**.
     Si certains des utilisateurs sélectionnés individuellement n'ont pas le service Exchange inclus dans leur plan Microsoft 365, vous ne pourrez pas sélectionner cette option.
     Si certains des utilisateurs sélectionnés pour la sauvegarde de groupe n'ont pas le service Exchange inclus dans leur plan Microsoft 365, vous pourrez sélectionner cette option, mais le plan de sauvegarde ne sera pas appliqué à ces utilisateurs.
   - Dans **Planifier**, sélectionnez la fréquence de sauvegarde.
   - Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.
   - [Facultatif] Pour inclure les boîtes aux lettres d'archivage dans la sauvegarde, activez le paramètre **Boîte aux lettres d'archivage**.
   - Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.

© Acronis International GmbH, 2003-2026

- Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
- Cliquez sur **OK**.

- [Facultatif] Pour activer l'analyse antimalware, activez le paramètre **Analyse des sauvegardes à la recherche de malwares**.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour plus d'informations, voir "Analyse antimalware des boîtes aux lettres" (p. 869).

6. Cliquez sur **Appliquer**.

Plan existant

1. Dans la console Cyber Protect, sous **Terminaux**, cliquez sur **Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
   - [Pour sauvegarder les boîtes aux lettres de tous les utilisateurs et toutes les boîtes aux lettres communes, y compris celles qui seront créées à l'avenir] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sauvegarder des boîtes aux lettres d'utilisateurs ou des boîtes aux lettres partagées] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez les boîtes aux lettres que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.
   - [Pour sauvegarder toutes les boîtes aux lettres de groupe, y compris celles des groupes qui seront créés à l'avenir] Développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.

     Remarque
     À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

     Remarque
     Au moins un des propriétaires du groupe doit être un utilisateur Microsoft 365 sous licence disposant d'une boîte aux lettres. Si le groupe est privé ou si son appartenance est masquée, le propriétaire doit également être membre du groupe.

   - [Pour sauvegarder des boîtes aux lettres de groupe en particulier] Développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez les boîtes aux lettres que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.

© Acronis International GmbH, 2003-2026

Remarque
À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

Remarque
Au moins un des propriétaires du groupe doit être un utilisateur Microsoft 365 sous licence disposant d'une boîte aux lettres. Si le groupe est privé ou si son appartenance est masquée, le propriétaire doit également être membre du groupe.

4. Sélectionnez un plan de sauvegarde existant.
5. Cliquez sur **Appliquer**.

Sélection de dossiers publics

Sélectionnez les dossiers publics comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Remarque
Les dossiers publics utilisent les licences de votre quota de sauvegarde pour les postes Microsoft 365.

Pour sélectionner des dossiers publics Exchange Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, développez l'organisation pour laquelle vous souhaitez restaurer les données. Sinon, ignorez cette étape.
3. Étendez le nœud **Dossiers publics**, puis sélectionnez **Tous les dossiers publics**.
4. Effectuez l'une des actions suivantes :
   - Pour sauvegarder tous les dossiers publics (y compris les dossiers publics qui seront créés à l'avenir), cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des dossiers publics en particulier, sélectionnez ceux que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarder**.
5. Dans le plan de sauvegarde, configurez les options suivantes :
   - Dans **Planifier**, sélectionnez la fréquence de sauvegarde.
   - Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.
   - Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
     - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.

© Acronis International GmbH, 2003-2026

- Cliquez sur **OK**.

- [Facultatif] Pour activer l'analyse antimalware, activez le paramètre **Analyse des sauvegardes à la recherche de malwares**.

  Remarque
  La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

  Pour plus d'informations, voir "Analyse antimalware des boîtes aux lettres" (p. 869).

Analyse antimalware des boîtes aux lettres

L'analyse antimalware des boîtes aux lettres Microsoft 365 recherche dans les e-mails sauvegardés des adresses URL et fichiers malveillants, et vous informe en cas de détection de menaces.

Cette fonctionnalité nécessite le pack **Advanced Security + XDR** dans lequel le quota de **postes Microsoft 365** doit être activé. L'analyse antimalware des boîtes aux lettres Microsoft 365 est fournie dans le cadre du pack Advanced, sans frais supplémentaires.

Remarque
Dans la version 24.11, le quota de **postes Microsoft 365** dans le pack **Advanced Security + XDR** est activé automatiquement pour les clients existants qui utilisent le pack **Advanced Security + XDR** avec son quota de **ressources** et dont le quota de **postes Microsoft 365** se trouve dans la **protection standard**.

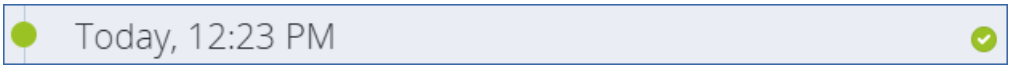
Pour ces clients, l'analyse antimalware est automatiquement activée dans les plans de sauvegarde existants pour les boîtes aux lettres Microsoft 365.

Vous pouvez activer les analyses antimalware lorsque vous configurez un plan de sauvegarde pour les boîtes aux lettres Microsoft 365. Pour plus d'informations, voir "Sélection de boîtes aux lettres" (p. 865).

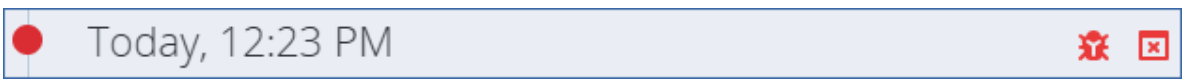
Les analyses s'exécutent automatiquement après chaque nouvelle sauvegarde. Vous ne pouvez ni planifier ni exécuter d'analyse manuellement.

Une fois l'analyse effectuée, la sauvegarde (point de restauration) dans l'archive de sauvegarde est marquée comme suit :

- Si aucun malware n'est trouvé, la sauvegarde est marquée d'un point vert et d'une icône verte.

- Si un malware est détecté, la sauvegarde est marquée d'un point rouge, et d'une ou de deux icônes rouges, selon le type de menace détectée (fichier malveillant ou adresse URL suspecte).

  Pour plus d'informations sur la consultation des informations sur ces menaces, voir "Vérification des détails sur une menace détectée" (p. 870).

© Acronis International GmbH, 2003-2026

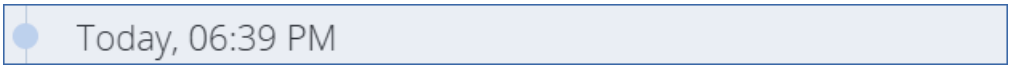
Important

Soyez prudent lors de la récupération de sauvegardes : l'analyse antimalware des boîtes aux lettres vous informe de la menace détectée, mais ne vous empêche pas de restaurer une sauvegarde infectée.

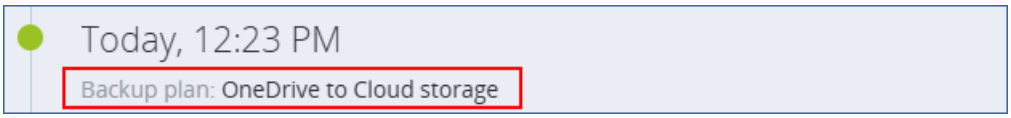
Pour nettoyer une sauvegarde infectée, accédez à la boîte aux lettres Microsoft 365, puis supprimez la pièce jointe malveillante ou l'intégralité de l'e-mail. De cette manière, la prochaine sauvegarde sera intègre.

Vous pouvez améliorer votre protection en activant Advanced Email Security. Avec ce pack Advanced, les e-mails suspects sont détectés avant d'atteindre la boîte de réception. Pour plus d'informations, voir Advanced Email Security.

Si une sauvegarde n'a pas encore été analysée, elle est marquée d'un point gris et aucune autre icône n'est affichée.



Une sauvegarde pour laquelle aucune analyse antimalware n'est disponible (par exemple, une sauvegarde OneDrive), est marquée d'un point vert et ne comporte aucune icône supplémentaire.



Limites

- L'analyse antimalware n'est pas prise en charge pour les types de fichiers suivants :
  - RAR
  - 7z
  - ISO
- Si une tâche d'analyse échoue, elle est retentée le jour suivant.
- L'analyse antimalware n'est pas prise en charge pour les composants Boucle dans les e-mails. Toute menace éventuelle dans un composant Boucle ne sera pas détectée.
- L'analyse antimalware est prise en charge uniquement sur le stockage cloud par défaut. Les stockages locaux, les stockages hébergés par des partenaires et les stockages dans le cloud public ne sont pas pris en charge.
- L'analyse antimalware n'est pas prise en charge pour les tenants en mode de Conformité.

Vérification des détails sur une menace détectée

Vous pouvez en savoir plus sur les menaces détectées en consultant l'archive de sauvegarde, l'e-mail infecté ou l'onglet **Alertes** dans la console Cyber Protect.

Pour vérifier les détails d'une menace détectée

© Acronis International GmbH, 2003-2026

Dans l'archive de sauvegarde

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Sauvegardes**, puis sélectionnez **Stockage d'application cloud**.
2. Sélectionnez l'archive de sauvegarde que vous souhaitez modifier, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez une sauvegarde marquée d'une icône rouge pour un fichier infecté ou une adresse URL malveillante.
4. Pour plus d'informations sur la menace, cliquez sur le lien **Fichiers infectés** ou **URL malveillantes**.

Dans un e-mail sauvegardé

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Sauvegardes**, puis sélectionnez **Stockage d'application cloud**.
2. Sélectionnez l'archive de sauvegarde que vous souhaitez modifier, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez une sauvegarde marquée d'une icône rouge pour un fichier infecté ou une adresse URL malveillante.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. [Si un avertissement de confidentialité s'affiche] Dans la boîte de dialogue **Avertissement de confidentialité**, cliquez sur **Poursuivre**.
6. Sélectionnez un e-mail marqué d'une icône rouge pour les fichiers infectés ou les URL malveillantes, puis cliquez sur **Afficher le contenu**.
7. Dans la zone **Des menaces malveillantes ont été détectées dans cet e-mail**, cliquez sur **Détails**.

Dans Surveillance > Alertes

1. Dans la console Cyber Protect, accédez à **Surveillance** > **Alertes**, puis sélectionnez **Stockage d'applications dans le cloud**.
2. Triez les alertes par niveau de gravité.
3. Sous **Avertissement**, recherchez les options **Une adresse URL malveillante est détectée** ou **Un malware est détecté**.
4. [Si une URL malveillante est détectée] Vérifiez la ligne **URL** au bas de l'alerte.
5. [Si un malware est détecté] Vérifiez la ligne **Nom de la menace** au bas de l'alerte.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Microsoft 365**.

© Acronis International GmbH, 2003-2026

2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   - Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des boîtes aux lettres, sélectionnez **Boîtes aux lettres** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Intégralité de la boîte aux lettres**.
6. Si plusieurs organisations Microsoft 365 sont ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
7. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
   Vous ne pouvez pas créer une nouvelle boîte aux lettres cible pendant la restauration. Pour restaurer une boîte aux lettres vers une nouvelle, vous devez d'abord créer la boîte aux lettres cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser le changement. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
8. Cliquez sur **Démarrer la restauration**.
9. Sélectionnez l'une des options d'écrasement :

© Acronis International GmbH, 2003-2026

- **Écraser les éléments existants**
- **Ne pas écraser les éléments existants**

10. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer des éléments d'une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer les éléments d'une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune qui contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer des éléments d'une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des boîtes aux lettres, sélectionnez **Boîtes aux lettres** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les e-mails : recherche par objet, expéditeur, destinataire, nom de la pièce jointe et date. Vous pouvez sélectionner une date de début ou une date de fin (toutes deux incluses), ou les deux dates pour effectuer une recherche dans un intervalle de temps.
   - Pour les événements : recherche par titre et date.

© Acronis International GmbH, 2003-2026

- Pour les tâches : recherche par sujet et date.
- Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Vous ne pouvez pas créer de nouvelle boîte aux lettres cible pendant la restauration. Pour restaurer un nouvel élément de boîte aux lettres vers une nouvelle boîte aux lettres, vous devez d'abord créer le nouvel élément de boîte aux lettres cible dans l'organisation Microsoft 365, puis laisser l'agent cloud synchroniser la modification. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :

   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier joint pour le télécharger.
   - Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.

8. Cliquez sur **Restaurer**.
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

    Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
11. [Uniquement lors de la restauration vers une boîte aux lettres utilisateur ou commune] Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Par défaut, le dossier **Éléments restaurés** est sélectionné.

    Les éléments d'une boîte aux lettres de groupe sont toujours restaurés dans le dossier **Boîte de réception**.
12. Cliquez sur **Démarrer la restauration**.
13. Sélectionnez l'une des options d'écrasement :

© Acronis International GmbH, 2003-2026

- **Écraser les éléments existants**
- **Ne pas écraser les éléments existants**

14. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration de l'intégralité de boîtes aux lettres dans des fichiers de données PST

Remarque
Vous pouvez restaurer des e-mails ou des dossiers de l'archive de boîte aux lettres en place en tant qu'éléments de boîte aux lettres distincts en utilisant l'option **Restauration > Messages électroniques**. Pour plus d'informations, voir "Restauration d'éléments de boîte aux lettres" (p. 873). L'archive de boîte aux lettres en place n'est pas restaurée lorsque vous utilisez les options **Restauration > Boîte aux lettres entière** ou **Restauration > En tant que fichiers PST**.

Restaurer une boîte aux lettres

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer une boîte aux lettres utilisateur dans un fichier de données PST, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres partagée dans un fichier de données PST, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer une boîte aux lettres de groupe dans un fichier de données PST, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.

   Si le fichier de données Outlook utilisateur, de groupe ou partagées a été supprimé, sélectionnez l'élément dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
4. Cliquez sur **Restaurer** > **En tant que fichiers PST**.
5. Définissez le mot de passe pour chiffrer l'archive avec le fichier PST.

   Le mot de passe doit contenir au moins un symbole.
6. Confirmez le mot de passe et cliquez sur **Terminé**.
7. Les éléments de boîte aux lettres sélectionnés seront restaurés sous la forme de fichiers de données PST et archivés au format ZIP. La taille maximale d'un fichier PST est limitée à 2 Go. Si la quantité de données que vous restaurez dépasse 2 Go, les données seront divisées en plusieurs fichiers PST. L'archive ZIP sera protégée par le mot de passe que vous avez défini.

© Acronis International GmbH, 2003-2026

8. Vous recevrez un e-mail avec un lien vers l'archive ZIP contenant les fichiers PST créés.
9. L'administrateur recevra une notification par e-mail l'informant que vous avez exécuté la procédure de restauration.

Remarque
La restauration d'une boîte aux lettres dans des fichiers PST peut prendre du temps, car elle suppose non seulement le transfert de données, mais également leur transformation à l'aide d'algorithmes complexes.

Télécharger l'archive contenant les fichiers PST et effectuer la restauration

1. Effectuez l'une des actions suivantes :
   - Pour télécharger l'archive à partir de l'e-mail, suivez le lien **Télécharger des fichiers**.
     L'archive est disponible pendant 96 heures. Pour télécharger l'archive après ces 96 heures, répétez la procédure de restauration.
   - Télécharger l'archive à partir de la console Cyber Protect :
     a. Accédez à **Stockage de sauvegarde** > **Fichiers PST**.
     b. Sélectionnez la dernière archive mise en évidence.
     c. Cliquez sur **Télécharger** dans le volet de droite.

   L'archive sera téléchargée dans le répertoire de téléchargement par défaut sur votre ordinateur.
2. Extrayez les fichiers PST depuis l'archive à l'aide du mot de passe que vous avez défini pour chiffrer l'archive.
3. Ouvrez les fichiers PST avec Microsoft Outlook.
   Les fichiers PST résultants peuvent être beaucoup plus petits que la boîte aux lettres d'origine. C'est un comportement normal.

   Important
   N'importez pas ces fichiers dans Microsoft Outlook à l'aide de l'**assistant d'importation et d'exportation**.
   Ouvrez les fichiers en double-cliquant dessus, ou en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Ouvrir avec...** > **Microsoft Outlook** dans le menu contextuel.

Restauration d'éléments de boîte aux lettres vers des fichiers PST

Remarque
Vous pouvez restaurer des e-mails ou des dossiers de l'archive de boîte aux lettres en place en tant qu'éléments de boîte aux lettres distincts en utilisant l'option **Restauration > Messages électroniques**. Pour plus d'informations, voir "Restauration d'éléments de boîte aux lettres" (p. 873). L'archive de boîte aux lettres en place n'est pas restaurée lorsque vous utilisez les options **Restauration > Boîte aux lettres entière** ou **Restauration > En tant que fichiers PST**.

Restaurer des éléments de boîte aux lettres

© Acronis International GmbH, 2003-2026

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour restaurer des éléments d'une boîte aux lettres utilisateur, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer les éléments d'une boîte aux lettres commune, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez la boîte aux lettres commune qui contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer des éléments d'une boîte aux lettres de groupe, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si la boîte aux lettres utilisateur, de groupe ou commune a été supprimée, sélectionnez-la dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
6. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.

© Acronis International GmbH, 2003-2026

- Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.

7. Cliquez sur **Restaurer en tant que fichiers PST**.
8. Définissez le mot de passe pour chiffrer l'archive avec le fichier PST.
   Le mot de passe doit contenir au moins un symbole.
9. Confirmez le mot de passe et cliquez sur **TERMINÉ**.

Les éléments de boîte aux lettres sélectionnés seront restaurés sous la forme de fichiers de données PST et archivés au format ZIP. La taille maximale d'un fichier PST est limitée à 2 Go. Si la quantité de données que vous restaurez dépasse 2 Go, les données seront divisées en plusieurs fichiers PST. L'archive ZIP sera protégée par le mot de passe que vous avez défini.

Vous recevrez un e-mail avec un lien vers l'archive ZIP contenant les fichiers PST créés.

L'administrateur recevra une notification par e-mail l'informant que vous avez exécuté la procédure de restauration.

Télécharger l'archive contenant les fichiers PST et effectuer la restauration

1. Effectuez l'une des actions suivantes :
   - Pour télécharger l'archive à partir de l'e-mail, suivez le lien **Télécharger des fichiers**.
     L'archive est disponible pendant 96 heures. Pour télécharger l'archive après ces 96 heures, répétez la procédure de restauration.
   - Télécharger l'archive à partir de la console Cyber Protect :
     a. Accédez à **Stockage de sauvegarde** > **Fichiers PST**.
     b. Sélectionnez la dernière archive mise en évidence.
     c. Cliquez sur **Télécharger** dans le volet de droite.

   L'archive sera téléchargée dans le répertoire de téléchargement par défaut sur votre ordinateur.
2. Extrayez les fichiers PST depuis l'archive à l'aide du mot de passe que vous avez défini pour chiffrer l'archive.
3. Ouvrez les fichiers PST avec Microsoft Outlook.
   Les fichiers PST résultants peuvent être beaucoup plus petits que la boîte aux lettres d'origine. C'est un comportement normal.

Important
N'importez pas ces fichiers dans Microsoft Outlook à l'aide de l'**assistant d'importation et d'exportation**.
Ouvrez les fichiers en double-cliquant dessus, ou en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Ouvrir avec...** > **Microsoft Outlook** dans le menu contextuel.

© Acronis International GmbH, 2003-2026

Restauration de dossiers publics et d'éléments de dossier

Pour restaurer un dossier public ou des éléments de dossier public, au moins un administrateur de l'organisation Microsoft 365 cible doit posséder les droits **Propriétaire** pour le dossier public cible. Si la restauration échoue en affichant une erreur concernant un accès refusé, affectez ces droits dans les propriétés du dossier cible, sélectionnez l'organisation cible dans la console Cyber Protect, cliquez sur **Actualiser**, puis répétez la restauration.

Pour restaurer un dossier public ou des éléments de dossier

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 sont ajoutées au service Cyber Protection, développez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Développez le nœud **Dossiers publics**, sélectionnez **Tous les dossiers publics**, sélectionnez le dossier public que vous souhaitez restaurer ou qui contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si le dossier public a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher des dossiers publics par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Récupérer des données**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Vous pouvez rechercher les e-mails et publications par sujet, expéditeur, destinataire et date. Les caractères génériques ne sont pas pris en charge.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un e-mail ou une publication est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un e-mail ou une publication est sélectionné, cliquez sur **Envoyer sous forme d'e-mail** pour l'envoyer aux adresses e-mail spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez

© Acronis International GmbH, 2003-2026

choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.

8. Cliquez sur **Restaurer**.
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer dans un dossier public**, affichez, modifiez ou spécifiez le dossier public cible.
    Le dossier d'origine est sélectionné par défaut. Si ce dossier n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier le dossier cible.
    Vous ne pouvez pas créer de nouveau dossier public pendant la restauration. Pour restaurer un dossier public vers un nouveau, vous devez d'abord créer le dossier public cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser la modification. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
11. Dans **Chemin d'accès**, affichez ou modifiez le sous-dossier cible dans le dossier public cible. Par défaut, le chemin d'accès d'origine sera recréé.
12. Cliquez sur **Démarrer la restauration**.
13. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser les éléments existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés.
Ne pas écraser les éléments existants	Si l'emplacement de destination comporte un fichier de même nom, ce fichier n'est pas écrasé et le fichier source n'est pas enregistré dans l'emplacement de destination.

14. Cliquez sur **Poursuivre** pour confirmer votre choix.

Protection des fichiers OneDrive

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder l'intégralité de OneDrive, ou des fichiers et dossiers en particulier.

Une option distincte dans le plan de sauvegarde permet de sauvegarder des blocs-notes OneNote.

Les fichiers sont sauvegardés avec les permissions de partage associées. Les niveaux de permission avancés (**Création**, **Complet**, **Contribution**) ne sont pas sauvegardés.

Certains fichiers sont susceptibles de contenir des informations sensibles, et l'accès à ces derniers peut être bloqué par une règle DLP (prévention de perte de données) dans Microsoft 365. Ces

© Acronis International GmbH, 2003-2026

fichiers ne sont pas sauvegardés, et aucun avertissement n'est affiché une fois l'opération de sauvegarde terminée.

Limites

La sauvegarde de contenu OneDrive Contenu n'est pas prise en charge pour les boîtes aux lettres partagées. Pour sauvegarder ce contenu, convertissez la boîte aux lettres partagée en compte utilisateur standard et vérifiez que OneDrive est activé pour ce compte.

Quels éléments de données peuvent être restaurés ?

Vous pouvez restaurer l'intégralité de OneDrive, ou tout fichier ou dossier sauvegardé.

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les fichiers hériter des permissions du dossier vers lequel ils sont restaurés.

Les liens de partage des fichiers et des dossiers ne sont pas restaurés.

Sélection de fichiers OneDrive

Sélectionnez les fichiers comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Sélection de fichiers OneDrive

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les fichiers de tous les utilisateurs (y compris des utilisateurs qui seront créés à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder les fichiers d'utilisateurs en particulier, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les fichiers, puis cliquez sur **Sauvegarde**.
4. Dans le plan de sauvegarde, configurez les options suivantes :
   - [Si disponible] Dans **Quoi sauvegarder**, sélectionnez **OneDrive**.

     Si certains des utilisateurs sélectionnés individuellement n'ont pas le service OneDrive inclus dans leur plan Microsoft 365, vous ne pourrez pas sélectionner cette option.

     Si certains des utilisateurs sélectionnés pour la sauvegarde de groupe n'ont pas le service OneDrive inclus dans leur plan Microsoft 365, vous pourrez sélectionner cette option, mais le plan de protection ne sera pas appliqué à ces utilisateurs.
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :

© Acronis International GmbH, 2003-2026

  - Conservez le paramètre par défaut **[Tous]** (tous les fichiers).
  - Spécifiez les fichiers et dossiers à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

    Vous pouvez utiliser des caractères génériques (*, ** et ?). Pour plus de détails sur la spécification des chemins et l'utilisation des caractères génériques, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 620).
  - Spécifiez les fichiers et dossiers à sauvegarder en cliquant sur Parcourir.

    Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul utilisateur.
- Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
  - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
  - Cliquez sur **OK**.
- [Facultatif] Dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions** pour spécifier les fichiers et dossiers à ignorer lors de la sauvegarde.

  Les exclusions de fichiers ont priorité sur la sélection de fichiers. Si vous spécifiez le même fichier dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.
- [Facultatif] Pour sauvegarder des blocs-notes OneNote, activez l'interrupteur **Inclure OneNote**.

Restauration de OneDrive et de fichiers OneDrive

Restauration de l'intégralité de OneDrive

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer le OneDrive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des fichiers OneDrive, sélectionnez **OneDrive** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer** > **Intégralité de OneDrive**.

© Acronis International GmbH, 2003-2026

6. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
   Vous ne pouvez pas créer une nouvelle cible OneDrive pendant la restauration. Pour restaurer un OneDrive sur un nouveau, vous devez d'abord créer le OneDrive cible dans l'organisation Microsoft 365, puis laisser l'agent cloud synchroniser le changement. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
7. Dans **Restaurer vers le lecteur**, affichez, modifiez ou spécifiez l'utilisateur cible.
   L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible.
8. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
9. Cliquez sur **Démarrer la restauration**.
10. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser un fichier existant s'il est plus ancien** et **Écraser les fichiers existants** remplaceront les blocs-notes OneNote existants.

11. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration de fichiers OneDrive

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.

© Acronis International GmbH, 2003-2026

3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer les fichiers OneDrive, puis cliquez sur **Restauration**.
   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des fichiers OneDrive, sélectionnez **OneDrive** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
6. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.
7. Sélectionnez les fichiers que vous voulez restaurer.
   Si la sauvegarde n'est pas chiffrée et que vous avez sélectionné un seul fichier, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version du fichier à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.
8. Si vous souhaitez télécharger un fichier, sélectionnez-le, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Sauvegarder**. Sinon, ignorez cette étape.
9. Cliquez sur **Restaurer**.
10. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
    Vous ne pouvez pas créer de nouveau OneDrive pendant la restauration. Pour restaurer un fichier vers un nouveau OneDrive, vous devez d'abord créer le OneDrive cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser la modification. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
11. Dans **Restaurer vers le lecteur**, affichez, modifiez ou spécifiez l'utilisateur cible.
    L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible.
12. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans le OneDrive de l'utilisateur cible. L'emplacement d'origine est sélectionné par défaut.
13. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
14. Cliquez sur **Démarrer la restauration**.

© Acronis International GmbH, 2003-2026

15. Sélectionnez l'une des options d'écrasement de fichier :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser un fichier existant s'il est plus ancien** et **Écraser les fichiers existants** remplaceront les blocs-notes OneNote existants.

16. Cliquez sur **Poursuivre** pour confirmer votre choix.

Protection de sites SharePoint Online

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder les collections de sites classiques, les sites de groupe (équipe moderne) et les sites de communication de SharePoint. Vous pouvez également sélectionner des sous-sites, listes et bibliothèques particuliers pour les sauvegarder.

À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

Une option distincte dans le plan de sauvegarde permet de sauvegarder des blocs-notes OneNote.

Les éléments suivants sont *exclus* lors d'une sauvegarde :

- Les paramètres de **Vue d'ensemble** du site (à l'exception du **titre, de la description et du logo**).
- Les commentaires des pages du site et les paramètres de commentaire des pages (commentaires **Activés**/**Désactivés**).
- Le **Site comprend** les paramètres du site.
- Les pages de composants WebPart et les composants WebPart intégrés aux pages wiki (en raison des limitations de l'API de SharePoint Online).

© Acronis International GmbH, 2003-2026

- Fichiers extraits : fichiers extraits manuellement pour être modifiés, et tous les fichiers créés ou transférés dans des bibliothèques et pour lesquels l'option **Nécessite une extraction** a été activée. Pour sauvegarder ces fichiers, vous devez d'abord les archiver.
- Les types de colonnes Données externes et Métadonnées gérées.
- La collection de sites par défaut « domain-my.sharepoint.com ». Il s'agit d'une collection dans laquelle sont stockés les fichiers OneDrive de tous les utilisateurs de l'organisation.
- Le contenu de la corbeille.

Limites

- Les titres et descriptions des sites/sous-sites/listes/colonnes sont tronqués lors d'une sauvegarde si leur taille dépasse 10 000 octets.
- Vous ne pouvez pas sauvegarder des versions précédentes de fichiers créés dans SharePoint Online. Seules les dernières versions des fichiers sont protégées.
- Vous ne pouvez pas sauvegarder la bibliothèque de conservation.
- Vous ne pouvez pas sauvegarder les sites créés dans Business Productivity Online Suite (BPOS), le prédécesseur de Microsoft 365.
- Vous ne pouvez pas sauvegarder les paramètres des sites qui utilisent le chemin d'accès géré/les `/portals` gérés (par exemple, `https://<tenant>.sharepoint.com/portals/...`).
- Vous pouvez restaurer les paramètres de gestion des droits relatifs à l'information (Information Rights Gestion – IRM) d'une liste ou d'une bibliothèque uniquement si l'IRM est activée dans l'organisation Microsoft 365 cible.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de site :

- Site entier
- Sous-sites
- Listes
- Éléments de liste
- Bibliothèques de documents
- Documents
- Pièces jointes d'éléments de liste
- Pages de site et pages de Wiki

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Les éléments peuvent être restaurés vers le site d'origine ou vers un autre site. Le chemin d'accès à un élément restauré est identique au chemin d'accès d'origine. Si le chemin d'accès n'existe pas, il sera créé.

© Acronis International GmbH, 2003-2026

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les éléments hériter des permissions de l'objet parent après la restauration.

Quels éléments ne peuvent pas être restaurés ?

- Sous-sites basés sur le modèle de **Référentiel de processus dans Visio**.
- Les listes de types suivants : **Liste de sondages**, **Liste de tâches**, **Bibliothèque d'images**, **Liens**, **Calendrier**, **Forum de discussion**, **Externe** et **Feuilles de calcul d'import**.
- Les listes pour lesquelles plusieurs types de contenu sont activés.

Sélection de données SharePoint Online

Sélectionnez les données comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des données SharePoint Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder tous les sites SharePoint classiques de l'organisation, y compris les sites qui seront créés à l'avenir, développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des sites classiques en particulier, développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, sélectionnez les sites que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.
   - Pour sauvegarder tous les sites de groupe (équipe moderne), y compris les sites qui seront créés à l'avenir, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.

     Remarque
     À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

   - Pour sauvegarder des sites de groupe (équipe moderne) en particulier, développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez les groupes dont vous souhaitez sauvegarder les sites, puis cliquez sur **Sauvegarde**.

© Acronis International GmbH, 2003-2026

Remarque
À partir de Cyber Protect Cloud 25.06, les groupes non protégés qui font partie d'une équipe ne sont pas affichés dans **Terminaux** > **Microsoft 365** > Organisation Microsoft 365 > **Groupes**. Vous pouvez protéger le site SharePoint et la boîte aux lettres de groupe de ces groupes en appliquant un plan de sauvegarde à l'ensemble de l'équipe. Pour plus d'informations, voir "Protection des données Microsoft 365 Teams" (p. 890).

4. Dans le plan de sauvegarde, configurez les options suivantes :
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :
     - Conservez le paramètre par défaut **[Tous]** (tous les éléments des sites sélectionnés).
     - Spécifiez les sous-sites, listes, et bibliothèques à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

       Pour sauvegarder un sous-site ou une liste/bibliothèque de sites de premier niveau, spécifiez son nom affiché au format suivant : `/nom affiché/**`

       Pour sauvegarder une liste/bibliothèque de sous-sites, spécifiez son nom affiché au format suivant : `/nom affiché du sous-site/nom affiché de la liste/**`

       Le nom affiché des sous-sites, des listes et des bibliothèques est disponible à la page **Contenu du site** du site ou sous-site SharePoint.
     - Spécifiez les sous-sites à sauvegarder en cliquant sur Parcourir.

       Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul site.
   - [Facultatif] Dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions** pour spécifier les sous-sites, les listes et les bibliothèques à ignorer lors de la sauvegarde.

     Les exclusions ont la priorité sur la sélection d'éléments, c'est-à-dire que si vous spécifiez le même sous-site dans les deux champs, ce sous-site sera ignoré lors de la sauvegarde.
   - Dans **Planifier**, sélectionnez la fréquence de sauvegarde.
   - Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.
   - Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
     - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
     - Cliquez sur **OK**.
   - [Facultatif] Pour sauvegarder des blocs-notes OneNote, activez l'interrupteur **Inclure OneNote**.

Restauration de données de SharePoint Online

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.

© Acronis International GmbH, 2003-2026

3. Effectuez l'une des actions suivantes :
   - Pour restaurer des données depuis un site de groupe (équipe moderne), développez le nœud **Groupes**, sélectionnez **Tous les groupes**, sélectionnez le groupe dont le site contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Pour restaurer des données depuis un site classique, développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, sélectionnez le groupe dont le site contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.
   - Si le site a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les groupes et les sites par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des sites SharePoint, sélectionnez **Sites SharePoint** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer les fichiers SharePoint**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments de données requis.
7. Sélectionnez les éléments que vous souhaitez restaurer.

   Si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.
8. [Facultatif] Pour télécharger un élément, sélectionnez-le, cliquez sur **Télécharger**, sélectionner l'emplacement dans lequel vous souhaitez le sauvegarder, puis cliquez sur **Enregistrer**.
9. Cliquez sur **Restaurer**.
10. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
11. Dans **Restaurer vers le site**, affichez, modifiez ou spécifiez le site cible.

    Vous ne pouvez pas créer de nouveau site SharePoint pendant la restauration. Pour restaurer un site SharePoint vers un nouveau site, vous devez d'abord créer le site cible dans l'organisation Microsoft 365 souhaitée, puis laisser l'agent cloud synchroniser le changement. L'agent cloud se synchronise automatiquement avec Microsoft 365 toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez dans la console Cyber Protect l'organisation sur la page **Microsoft 365**, puis cliquez sur **Actualiser**.
12. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.

    Les autorisations de partage pour les utilisateurs internes et externes sont restaurées.

© Acronis International GmbH, 2003-2026

13. Cliquez sur **Démarrer la restauration**.
14. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser un fichier existant s'il est plus ancien** et **Écraser les fichiers existants** remplaceront les blocs-notes OneNote existants.

15. Cliquez sur **Poursuivre** pour confirmer votre choix.

Protection des données Microsoft 365 Teams

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des équipes entières. Cela inclut le nom de l'équipe, la liste des membres de l'équipe, les canaux d'équipe et leur contenu, la boîte aux lettres et les réunions de l'équipe, et le site de l'équipe.

Une option distincte dans le plan de sauvegarde permet de sauvegarder des blocs-notes OneNote.

Quels éléments de données peuvent être restaurés ?

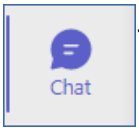
- Toute l'équipe
- Canaux d'équipe
- Fichiers de canal
- Boîte aux lettres d'équipe
- Dossiers d'e-mail dans la boîte aux lettres de l'équipe
- E-mails dans la boîte aux lettres de l'équipe
- Réunions
- Site d'équipe

© Acronis International GmbH, 2003-2026

Il est impossible de restaurer des conversations dans les canaux d'équipe, mais vous pouvez les télécharger en tant que fichier html unique.

Limites

Les éléments suivants ne sont pas sauvegardés :

- Les paramètres du canal général (préférence de modération), en raison d'une restriction de l'API bêta de Microsoft Teams.
- Les paramètres des canaux personnalisés (préférence de modération), en raison d'une restriction de l'API bêta de Microsoft Teams.
- Notes de réunion.
- Messages de la section de chat 

. Cette section contient des chats privés en tête-à-tête et des chats de groupe.
- Badges et éloges.

La sauvegarde et la restauration sont prises en charge pour les onglets de canal suivants :

- Word
- Excel
- PowerPoint
- PDF
- Bibliothèque de documents

Sélection des équipes

Sélectionnez les équipes comme décrit ci-dessous, puis indiquez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des équipes

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les équipes. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder toutes les équipes de l'organisation (y compris les équipes qui seront créées à l'avenir), développez le nœud **Teams**, sélectionnez **Toutes les équipes**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des équipes individuelles, développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez les équipes que vous souhaitez sauvegarder, puis cliquez sur **Sauvegarde**.

© Acronis International GmbH, 2003-2026

Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.

4. Dans le plan de sauvegarde, configurez les options suivantes :
   - Dans **Planifier**, sélectionnez la fréquence de sauvegarde.
   - Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.
   - Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
     - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
     - Cliquez sur **OK**.
   - [Facultatif] Pour sauvegarder des blocs-notes OneNote, activez l'interrupteur **Inclure OneNote**.

Restauration de l'intégralité d'une équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe que vous souhaitez restaurer, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Toute l'équipe**.

   Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
6. Dans **Restaurer vers l'équipe**, consultez l'équipe cible ou sélectionnez-en une autre.

   L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas (par exemple, si elle a été supprimée) ou si vous avez sélectionné une organisation qui ne contient pas l'équipe d'origine, vous devez sélectionner une équipe cible dans la liste déroulante.

   Vous pouvez restaurer une équipe uniquement dans une équipe existante. Vous ne pouvez pas créer d'équipes pendant les opérations de restauration.
7. Cliquez sur **Démarrer la restauration**.
8. Sélectionnez l'une des options d'écrasement :
   - **Écraser le contenu existant s'il est plus ancien**
   - **Écraser le contenu existant**
   - **Ne pas écraser le contenu existant**

© Acronis International GmbH, 2003-2026

Remarque
Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.

9. Cliquez sur **Poursuivre** pour confirmer votre choix.

Lorsque vous supprimez un canal d'une interface graphique de Microsoft Teams, il n'est pas immédiatement supprimé du système. Ainsi, lorsque vous restaurez l'intégralité de l'équipe, le nom de ce canal ne peut pas être utilisé et un suffixe y sera ajouté.

Les conversations sont restaurées en tant que fichier html unique dans l'onglet **Fichiers** du canal. Vous pouvez trouver ce fichier dans un dossier nommé selon le modèle suivant : `<Team name>_<Channel name>_conversations_backup_<date of recovery>T<time of recovery>Z`.

Remarque
Après avoir restauré une équipe ou des canaux d'équipe, accédez à Microsoft Teams, sélectionnez les canaux restaurés, puis cliquez sur leur onglet **Fichiers**. Autrement, les sauvegardes suivantes de ces canaux n'incluront pas le contenu de cet onglet, en raison d'une restriction de l'API bêta de Microsoft Teams.

Restaurer des canaux ou des fichiers d'équipe dans les canaux d'équipe

Pour restaurer des canaux d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer les canaux, puis cliquez sur **Restauration**.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Canaux**.
6. Sélectionnez les canaux que vous souhaitez restaurer, puis cliquez sur **Restaurer**. Pour sélectionner un canal dans le volet principal, sélectionnez la case en face de son nom.

   Les options de recherche suivantes sont disponibles :

   - Pour **Conversations** : expéditeur, objet, contenu, langue, nom de la pièce jointe, date ou plage de dates.
   - Pour **Fichiers** : nom du fichier ou nom du dossier, type de fichier, taille, date ou plage de dates de la dernière modification.

   Remarque
   Vous pouvez aussi télécharger les fichiers localement, au lieu de les restaurer.

© Acronis International GmbH, 2003-2026

7. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
8. Dans **Restaurer vers l'équipe**, affichez, modifiez ou indiquez l'équipe cible.
   L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez indiquer l'équipe cible.
9. Dans **Restaurer vers le canal**, affichez, modifiez ou indiquez le canal cible.
10. Cliquez sur **Démarrer la restauration**.
11. Sélectionnez l'une des options d'écrasement :
    - **Écraser le contenu existant s'il est plus ancien**
    - **Écraser le contenu existant**
    - **Ne pas écraser le contenu existant**

    Remarque
    Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
12. Cliquez sur **Poursuivre** pour confirmer votre choix.

Les conversations sont restaurées en tant que fichier html unique dans l'onglet **Fichiers** du canal. Vous pouvez trouver ce fichier dans un dossier nommé selon le modèle suivant : `<Team name>_<Channel name>_conversations_backup_<date of recovery>T<time of recovery>Z`.

Remarque
Après avoir restauré une équipe ou des canaux d'équipe, accédez à Microsoft Teams, sélectionnez les canaux restaurés, puis cliquez sur leur onglet **Fichiers**. Autrement, les sauvegardes suivantes de ces canaux n'incluront pas le contenu de cet onglet, en raison d'une restriction de l'API bêta de Microsoft Teams.

Restaurer des fichiers dans un canal d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer les canaux, puis cliquez sur **Restauration**.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Canaux**.
6. Sélectionnez le canal souhaité, puis ouvrez le dossier **Fichiers**.

© Acronis International GmbH, 2003-2026

Parcourez les éléments requis ou utilisez la fonction de recherche pour les obtenir. Les options de recherche suivantes sont disponibles : nom du fichier ou nom du dossier, type de fichier, taille, date ou plage de dates de la dernière modification.

7. [Facultatif] Pour télécharger un élément, sélectionnez-le, cliquez sur **Télécharger**, sélectionner l'emplacement dans lequel vous souhaitez le sauvegarder, puis cliquez sur **Enregistrer**.
8. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer**
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur Organisation Microsoft 365 pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers l'équipe**, affichez, modifiez ou indiquez l'équipe cible.
    L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez indiquer l'équipe cible.
11. Dans **Restaurer vers le canal**, affichez, modifiez ou indiquez le canal cible.
12. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
13. Cliquez sur **Démarrer la restauration**.
14. Sélectionnez l'une des options d'écrasement :
    - **Écraser le contenu existant s'il est plus ancien**
    - **Écraser le contenu existant**
    - **Ne pas écraser le contenu existant**

    Remarque
    Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
15. Cliquez sur **Poursuivre** pour confirmer votre choix.

Vous ne pouvez pas restaurer de conversations individuelles. Dans votre volet principal, vous pouvez uniquement parcourir le dossier **Conversation** ou télécharger son contenu en tant que fichier html unique. Pour cela, cliquez sur l'icône « Restaurer les dossiers »  , sélectionnez le dossier **Conversations** souhaité, puis cliquez sur **Télécharger**.

Vous pouvez rechercher les messages dans le dossier **Conversation** par :

- Expéditeur
- Contenu
- Nom de la pièce jointe
- Date

© Acronis International GmbH, 2003-2026

Restaurer une boîte aux lettres d'équipe

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Cliquez sur l'icône « Restaurer les dossiers »  , sélectionnez le dossier de boîte aux lettres racine, puis cliquez sur **Restaurer**.

   Remarque
   Vous pouvez également récupérer des dossiers individuels dans la boîte aux lettres sélectionnée.
7. Cliquez sur **Restaurer**.
8. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
9. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
10. Cliquez sur **Démarrer la restauration**.
11. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
12. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres d'équipe vers des fichiers PST

Restaurer des éléments de boîte aux lettres d'équipe

© Acronis International GmbH, 2003-2026

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez une équipe dont la boîte aux lettres contenait à l'origine les éléments que vous souhaitez restaurer, puis cliquez sur **Restauration**.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un message de courrier électronique ou un élément de calendrier est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
   - Lorsque la sauvegarde n'est pas chiffrée, que vous avez utilisé la recherche et que vous avez sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour afficher la version de l'élément. Vous pouvez sélectionner n'importe quelle version sauvegardée, qu'elle soit antérieure ou postérieure au point de restauration sélectionné.
8. Cliquez sur **Restaurer en tant que fichiers PST**.
9. Définissez le mot de passe pour chiffrer l'archive avec le fichier PST.

   Le mot de passe doit contenir au moins un symbole.
10. Confirmez le mot de passe et cliquez sur **TERMINÉ**.

© Acronis International GmbH, 2003-2026

Les éléments de boîte aux lettres sélectionnés seront restaurés sous la forme de fichiers de données PST et archivés au format ZIP. La taille maximale d'un fichier PST est limitée à 2 Go. Si la quantité de données que vous restaurez dépasse 2 Go, les données seront divisées en plusieurs fichiers PST. L'archive ZIP sera protégée par le mot de passe que vous avez défini.

Vous recevrez un e-mail avec un lien vers l'archive ZIP contenant les fichiers PST créés.

L'administrateur recevra une notification par e-mail l'informant que vous avez exécuté la procédure de restauration.

Télécharger l'archive contenant les fichiers PST et effectuer la restauration

1. Effectuez l'une des actions suivantes :
   - Pour télécharger l'archive depuis l'e-mail, suivez le lien **Téléchargement des fichiers**. L'archive est disponible au téléchargement sous 24 heures. Si le lien expire, répétez la procédure de restauration.
   - Télécharger l'archive à partir de la console Cyber Protect :
     a. Accédez à **Stockage de sauvegarde** > **Fichiers PST**.
     b. Sélectionnez la dernière archive mise en évidence.
     c. Cliquez sur **Télécharger** dans le volet de droite.

   L'archive sera téléchargée dans le répertoire de téléchargement par défaut sur votre ordinateur.
2. Extrayez les fichiers PST depuis l'archive à l'aide du mot de passe que vous avez défini pour chiffrer l'archive.
3. Dans Microsoft Outlook, ouvrez ou importez les fichiers PST. Pour savoir comment procéder, reportez-vous à la documentation Microsoft.

Restaurer les messages électroniques et les réunions

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer les e-mails ou les réunions, puis cliquez sur **Restauration**.

   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Parcourez l'élément requis ou utilisez la fonction de recherche pour l'obtenir.

   Les options de recherche suivantes sont disponibles :
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire et date.
   - Pour les réunions : recherchez par nom d'événement et date.

© Acronis International GmbH, 2003-2026

7. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

   Remarque
   Vous pouvez trouver les réunions dans le dossier **Calendrier**.

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Lorsqu'un e-mail ou une réunion sont sélectionnés, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer aux adresses électroniques spécifiées. Vous pouvez sélectionner l'expéditeur et rédiger un message qui sera ajouté à l'élément transféré.
8. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
9. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
10. Cliquez sur **Démarrer la restauration**.
11. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
12. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restaurer un site d'équipe ou des éléments précis d'un site

1. Cliquez sur **Microsoft 365**.
2. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les équipes sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Teams**, sélectionnez **Toutes les équipes**, sélectionnez l'équipe dont vous souhaitez restaurer le site, puis cliquez sur **Restauration**.
   Vous pouvez rechercher les équipes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Site d'équipe**.
6. Parcourez l'élément requis ou utilisez la fonction de recherche pour l'obtenir.
7. [Facultatif] Pour télécharger un élément, sélectionnez-le, cliquez sur **Télécharger**, sélectionner l'emplacement dans lequel vous souhaitez le sauvegarder, puis cliquez sur **Enregistrer**.

© Acronis International GmbH, 2003-2026

8. Sélectionnez les éléments que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
9. Si plusieurs organisations Microsoft 365 ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Microsoft 365** pour afficher, modifier ou indiquer l'organisation cible.
   L'organisation et l'équipe d'origine sont sélectionnées par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez spécifier l'organisation cible.
10. Dans **Restaurer vers l'équipe**, affichez, modifiez ou indiquez l'équipe cible.
    L'équipe d'origine est sélectionnée par défaut. Si cette équipe n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez indiquer le dossier cible.
11. Choisissez de restaurer ou non les permissions de partage associées aux éléments restaurés.
12. Cliquez sur **Démarrer la restauration**.
13. Sélectionnez l'une des options d'écrasement :
    - **Écraser le contenu existant s'il est plus ancien**
    - **Écraser le contenu existant**
    - **Ne pas écraser le contenu existant**

    Remarque
    Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
14. Cliquez sur **Poursuivre** pour confirmer votre choix.

Protection des blocs-notes OneNote

Par défaut, les blocs-notes OneNote sont inclus dans les sauvegardes de fichiers OneDrive, de Microsoft Teams et de sites SharePoint.

Pour exclure les blocs-notes OneNote de ces sauvegardes, désactivez l'interrupteur **Inclure OneNote** dans le plan de sauvegarde correspondant.

Restauration de blocs-notes OneNote sauvegardés

Pour apprendre à restaurer un bloc-notes OneNote sauvegardé, reportez-vous à la rubrique suivante :

- Pour les sauvegardes OneDrive, reportez-vous à "Restauration de l'intégralité de OneDrive" (p. 882) ou à "Restauration de fichiers OneDrive" (p. 883).
- Pour les sauvegardes Teams, reportez-vous à "Restauration de l'intégralité d'une équipe" (p. 892), à "Restaurer des canaux ou des fichiers d'équipe dans les canaux d'équipe" (p. 893) ou à "Restaurer un site d'équipe ou des éléments précis d'un site" (p. 899).
- Pour les sauvegardes de site SharePoint, reportez-vous à "Restauration de données de SharePoint Online" (p. 888).

© Acronis International GmbH, 2003-2026

Versions prises en charge

- OneNote (OneNote 2016 et versions ultérieures)
- OneNote pour Windows 10

Limitations et problèmes connus

- Les blocs-notes OneNote enregistrés dans OneDrive ou SharePoint sont limités à 2 Go. Vous ne pouvez pas restaurer des blocs-notes OneNote plus volumineux sur des cibles OneDrive ou SharePoint.
- Les blocs-notes OneNote comprenant des groupes de sections ne sont pas pris en charge.
- Dans les blocs-notes OneNote sauvegardés qui contiennent des sections avec des noms différents de ceux par défaut, la première section s'affiche avec le nom par défaut (comme `Nouvelle section` ou `Section sans titre`). Cela peut affecter l'ordre des sections dans les blocs-notes contenant plusieurs sections.
- Lorsque vous restaurez des blocs-notes OneNote, les options **Écraser le contenu existant s'il est plus ancien** et **Écraser le contenu existant** remplaceront les blocs-notes OneNote existants.
- Lorsque vous restaurez une équipe complète, un site d'équipe ou le dossier `SiteAssets` d'un site d'équipe, et que vous avez sélectionné l'option **Écraser le contenu existant s'il est plus ancien** ou **Écraser le contenu existant**, le bloc-notes OneNote par défaut de l'équipe n'est pas écrasé. La restauration réussit avec l'avertissement *Échec de la mise à jour des propriétés du fichier « /sites/<nom équipe>/SiteAssets/<nom bloc-notes OneNote> »*.

Protection des postes avec application de collaboration Microsoft 365

Vous pouvez utiliser le pack Advanced Email Security qui fournit une protection en temps réel pour vos boîtes aux lettres Microsoft 365, Google Workspace ou Open-Xchange :

- Antimalware et antispam
- Analyse d'URL dans les e-mails
- Analyse DMARC
- Anti-phishing
- Protection contre l'usurpation d'identité
- Analyse des pièces jointes
- Désarmement et reconstruction du contenu
- Schéma de confiance

Vous pouvez également activer les postes d'application de collaboration Microsoft 365, ce qui permet de protéger les applications de collaboration cloud Microsoft 365 contre les menaces de sécurité liées au contenu. Ces applications comprennent OneDrive, SharePoint et Teams.

© Acronis International GmbH, 2003-2026

Advanced Email Security peut être activé par ressource ou par gigaoctet, et aura un impact sur votre modèle de licence.

Pour accéder à l'intégration d'Advanced Email Security depuis la console Cyber Protect Cloud

1. Cliquez sur **Terminaux** > **Microsoft 365**.
2. Cliquez sur le nœud **Utilisateurs**, puis sur le lien **Accédez à Email Security** en haut à droite.

Pour en savoir plus sur Advanced Email Security dans la fiche solution Advanced Email Security.

Pour obtenir des instructions de configuration, consultez Advanced Email Security avec FortiMail Workspace Security (anciennement Perception Point).

Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365

Remarque
Cette fonctionnalité est disponible pour les tenants clients pour lesquels **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365** est sélectionnée dans la section **Protection Standard** d'un mode de licence basé sur le service dans le portail de gestion. Aucun abonnement Azure distinct n'est requis.

L'option **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365** fournit des sauvegardes fréquentes, une restauration rapide et des plans de sauvegarde simplifiés.

Les sauvegardes sont effectuées toutes les 10 minutes et restent toujours dans la limite de confiance des données Microsoft 365, car elles sont conservées dans le stockage des sauvegardes Microsoft 365.

L'option **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365** est disponible pour les types de données suivants :

- Boîtes aux lettres Exchange
  Toutes les sauvegardes sont disponibles pour la restauration pendant un an.
- Comptes OneDrive
  La période de rétention est d'un an, avec une durée de conservation de deux semaines pour les sauvegardes fréquentes. Pendant les deux dernières semaines, toutes les sauvegardes sont disponibles pour la restauration. Du 15e jour jusqu'à la fin de la période d'un an, une sauvegarde hebdomadaire est disponible pour la restauration.
- Sites SharePoint
  La période de rétention est d'un an, avec une durée de conservation de deux semaines pour les sauvegardes fréquentes. Pendant les deux dernières semaines, toutes les sauvegardes sont disponibles pour la restauration. Du 15e jour jusqu'à la fin de la période d'un an, une sauvegarde hebdomadaire est disponible pour la restauration.

© Acronis International GmbH, 2003-2026

Pour plus d'informations sur les différentes solutions de sauvegarde des données Microsoft 365, voir "Comparaison des solutions de sauvegarde pour les données Microsoft 365" (p. 845).

Création et application d'un nouveau plan de sauvegarde

Vous pouvez créer un plan de sauvegarde dans les onglets **Terminaux** ou **Gestion** > **Sauvegarde des applications dans le cloud**.

Remarque
Vous ne pouvez avoir qu'un seul plan de sauvegarde par type de données (boîtes aux lettres Exchange, comptes OneDrive ou sites SharePoint) dans un tenant de client.

Pour créer et appliquer un plan de sauvegarde

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Sauvegarde directe pour Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Sélectionnez les éléments que vous souhaitez sauvegarder.
   Vous pouvez sélectionner des boîtes aux lettres Exchange, OneDrive et des sites SharePoint.
   - [Pour sauvegarder les boîtes aux lettres ou les comptes OneDrive de tous les utilisateurs, y compris ceux qui seront créés à l'avenir] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sauvegarder des boîtes aux lettres ou des comptes OneDrive] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs** et des comptes d'utilisateurs, puis cliquez sur **Sauvegarde**.
   - [Pour sauvegarder tous les sites d'équipe modernes, y compris ceux qui seront créés à l'avenir] Développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sauvegarder des sites d'équipe modernes] Développez le nœud **Groupes**, sélectionnez **Tous les groupes** et des sites, puis cliquez sur **Sauvegarde**.
   - [Pour sauvegarder tous les sites de communication classiques, y compris ceux qui seront créés à l'avenir] Développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sauvegarder des sites de communication classiques] Développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites** et des sites, puis cliquez sur **Sauvegarde**.
4. Pour créer un plan de sauvegarde, cliquez sur **Créer**.

© Acronis International GmbH, 2003-2026

Remarque
Cette option est disponible uniquement s'il n'existe pas de plan pour le type de données sélectionné. Si un plan existe, vous ne pouvez appliquer que ce plan. Pour plus d'informations, voir "Application d'un plan de sauvegarde" (p. 906).

5. [Si plusieurs types de données sont disponibles] Dans le plan de sauvegarde, cliquez sur **Éléments à sauvegarder**, puis sélectionnez **Boîtes aux lettres Microsoft 365** ou **OneDrive**.
6. Cliquez sur **Appliquer**.

Remarque
L'application d'un plan de sauvegarde peut prendre jusqu'à 45 minutes en raison du temps de traitement nécessaire côté stockage des sauvegardes Microsoft 365.

Gestion > Sauvegarde d'applications dans le cloud

1. Dans la console Cyber Protect, accédez à **Gestion** > **Sauvegarde d'applications dans le cloud**.
2. Cliquez sur **Création d'un plan**.
3. Dans **Éléments à sauvegarder**, sélectionnez l'un des types de données suivants :
   - **Boîtes aux lettres Microsoft 365**
   - **OneDrive**
   - **Sites SharePoint**
4. Activez le commutateur situé à côté de l'option **Sauvegarde directe pour Microsoft 365**.

Remarque
L'interrupteur est activé uniquement si aucun plan de sauvegarde n'existe pour le même type de données. Si un plan de sauvegarde est déjà disponible, vous ne pouvez activer que ce plan. Pour plus d'informations, voir "Application d'un plan de sauvegarde" (p. 906).

5. Dans **Terminaux**, cliquez sur **Aucun terminal**, puis ajoutez les ressources que vous souhaitez sauvegarder :
   a. Cliquez sur **Ajouter**.
   b. Sélectionnez les ressources que vous souhaitez ajouter, puis cliquez sur **Ajouter**.
   c. Cliquez sur **Terminé**.
6. Cliquez sur **Appliquer**.

Remarque
L'application d'un plan de sauvegarde peut prendre jusqu'à 45 minutes en raison du temps de traitement nécessaire côté stockage des sauvegardes Microsoft 365.

Le plan de sauvegarde est créé et appliqué aux ressources sélectionnées. Les sauvegardes s'exécuteront automatiquement toutes les 10 minutes. Avec **Sauvegarde directe dans le stockage**

© Acronis International GmbH, 2003-2026

de sauvegarde de Microsoft 365, vous ne pouvez pas exécuter de plan de sauvegarde manuellement.

Modification d'un plan de sauvegarde

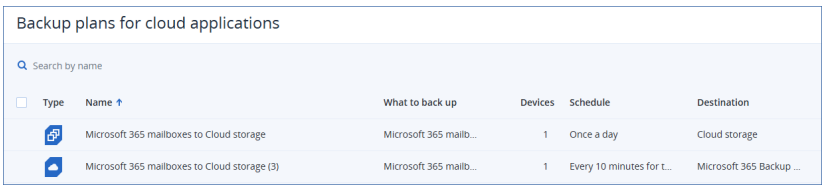
Vous pouvez modifier un plan de sauvegarde pour ajouter ou supprimer des ressources, ou modifier le nom du plan.

Vous ne pouvez pas convertir un plan de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365** en plan pour **Microsoft 365 Business - Sauvegarde**, ni inversement.

Pour modifier un plan de sauvegarde pour Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365

1. Dans la console Cyber Protect, accédez à **Gestion** > **Sauvegarde d'applications dans le cloud**.
2. Sélectionnez un plan pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, puis cliquez sur **Modifier**.

   Vous pouvez distinguer les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** et **Microsoft 365 Business – Sauvegarde** en comparant leurs icônes et la destination de la sauvegarde. Les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** ne peuvent utiliser que le stockage de sauvegarde Microsoft 365.

3. [Facultatif] Pour modifier le nom du plan :
   a. Cliquez sur l'icône représentant un crayon, puis modifiez le nom.
   b. Cliquez sur **OK**.
   c. Cliquez sur **Enregistrer**.
4. [Facultatif] Pour ajouter des ressources au plan :
   a. Cliquez sur **Terminaux**.
   b. Cliquez sur **Ajouter**.
   c. Sélectionnez les ressources, puis cliquez sur **Ajouter**.
   d. Cliquez sur **Terminé**.
   e. Cliquez sur **Enregistrer**.
5. [Facultatif] Pour supprimer des ressources du plan :
   a. Cliquez sur **Terminaux**.
   b. Sélectionnez les ressources, puis cliquez sur **Supprimer**.

© Acronis International GmbH, 2003-2026

c. Cliquez sur **Terminé**.

d. Cliquez sur **Enregistrer**.

Application d'un plan de sauvegarde

Vous pouvez avoir un plan de sauvegarde par type de données (boîtes aux lettres Exchange, sites SharePoint ou OneDrive). Si un plan de sauvegarde a déjà été créé, vous ne pouvez appliquer que ce plan et ne pourrez pas créer un nouveau plan.

Remarque
Si vous révoquez puis réappliquez un plan de sauvegarde à une ressource, les sauvegardes existantes (points de restauration) deviendront indisponibles lorsqu'une nouvelle sauvegarde sera créée.

Vous pouvez appliquer un plan de sauvegarde dans les onglets **Terminaux** ou **Gestion** > **Sauvegarde d'applications dans le Cloud**.

Pour appliquer un plan de sauvegarde

Terminaux

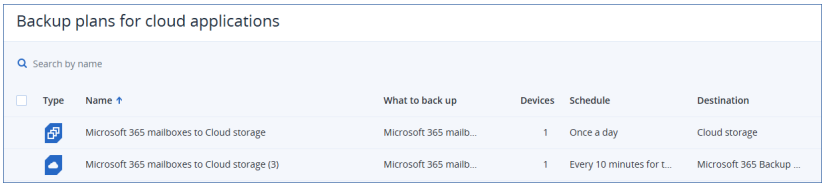
1. Dans la console Cyber Protect, accédez à **Terminaux** > **Sauvegarde directe pour Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Sélectionnez les éléments auxquels vous souhaitez appliquer un plan de sauvegarde.
   - Pour sélectionner les boîtes aux lettres ou les comptes OneDrive de tous les utilisateurs, y compris ceux qui seront créés à l'avenir, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sélectionner des boîtes aux lettres ou des comptes OneDrive] Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs** et des comptes d'utilisateurs, puis cliquez sur **Sauvegarde**.
   - [Pour sélectionner tous les sites d'équipe modernes, y compris les sites qui seront créés à l'avenir] Développez le nœud **Groupes**, sélectionnez **Tous les groupes**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sélectionner des sites d'équipe modernes] Développez le nœud **Groupes**, sélectionnez **Tous les groupes** et des sites, puis cliquez sur **Sauvegarde**.
   - [Pour sélectionner tous les sites de communication classiques, y compris les sites qui seront créés à l'avenir] Développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites**, puis cliquez sur **Sauvegarde de groupe**.
   - [Pour sélectionner des sites de communication classiques] Développez le nœud **Collections de sites**, sélectionnez **Toutes les collections de sites** et des sites, puis cliquez sur **Sauvegarde**.
4. Sélectionnez un plan de sauvegarde, puis cliquez sur **Appliquer**.

© Acronis International GmbH, 2003-2026

Remarque
L'application d'un plan de sauvegarde peut prendre jusqu'à 45 minutes en raison du temps de traitement nécessaire côté stockage des sauvegardes Microsoft 365.

Les plans de sauvegarde affichés dépendent du type de données. Par exemple, dans **Utilisateurs**, seuls les plans de sauvegarde de boîtes aux lettres ou de comptes OneDrive sont disponibles.

Gestion > Sauvegarde d'applications dans le cloud

1. Dans la console Cyber Protect, accédez à **Gestion** > **Sauvegarde d'applications dans le cloud**.
2. Sélectionnez un plan de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, puis cliquez sur **Modifier**.
   Vous pouvez distinguer les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** et **Microsoft 365 Business – Sauvegarde** en comparant leurs icônes et la destination de la sauvegarde. Les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** ne peuvent utiliser que le stockage de sauvegarde Microsoft 365.
   

3. Dans le plan de sauvegarde, cliquez sur **Terminaux**.
4. Cliquez sur **Ajouter**.
5. Sélectionnez les ressources ou les groupes de terminaux, puis cliquez sur **Ajouter**.
6. Cliquez sur **Terminé**.
7. Cliquez sur **Enregistrer**.

Remarque
L'application d'un plan de sauvegarde peut prendre jusqu'à 45 minutes en raison du temps de traitement nécessaire côté stockage des sauvegardes Microsoft 365.

Restauration d'éléments sauvegardés

Vous pouvez restaurer des boîtes aux lettres Exchange, des comptes OneDrive et des sites SharePoint complets vers leurs emplacements d'origine. Vous ne pouvez restaurer qu'une boîte aux lettres, un compte OneDrive ou un site SharePoint à la fois. Pour restaurer plusieurs éléments, répétez la procédure de restauration pour chaque élément.

Pour restaurer des éléments sauvegardés à partir de terminaux

Boîte aux lettres Exchange

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Sauvegarde directe pour Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Développez le nœud **Utilisateurs**, puis sélectionnez **Tous les utilisateurs**.
4. Sélectionnez un compte utilisateur, puis cliquez sur **Restauration**.

   Remarque
   Vous ne pouvez sélectionner qu'un seul compte utilisateur à la fois.

5. [Si la boîte aux lettres et le compte OneDrive sont sauvegardés] Dans **Filtrer par contenu**, sélectionnez **Boîtes aux lettres Microsoft 365**.
6. Sélectionnez une sauvegarde (point de restauration), puis cliquez sur **Restaurer l'intégralité de la boîte aux lettres**.
7. Cliquez sur **Démarrer la restauration**.

Les éléments modifiés ou supprimés de la boîte aux lettres sont remplacés par les éléments sauvegardés. Les nouveaux éléments et les éléments non modifiés ne sont pas écrasés. Vous ne pouvez pas modifier les paramètres d'écrasement, car ils dépendent de l'intégration Microsoft. Pour plus d'informations, consultez Restaurer des données dans Sauvegarde Microsoft 365 dans la documentation Microsoft.

Compte OneDrive

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Sauvegarde directe pour Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Développez le nœud **Utilisateurs**, puis sélectionnez **Tous les utilisateurs**.
4. Sélectionnez un compte utilisateur, puis cliquez sur **Restauration**.

   Remarque
   Vous ne pouvez sélectionner qu'un seul compte utilisateur à la fois.

5. [Si la boîte aux lettres et le compte OneDrive sont sauvegardés] Dans **Filtrer par contenu**, sélectionnez **OneDrive**.
6. Sélectionnez une sauvegarde (point de restauration), puis cliquez sur **Restaurer l'intégralité de OneDrive**.
7. Cliquez sur **Démarrer la restauration**.

Le contenu de OneDrive est complètement écrasé par le contenu sauvegardé. Toutes les modifications qui ne sont pas incluses dans la sauvegarde sont perdues. Vous ne pouvez pas modifier les paramètres d'écrasement, car ils dépendent de l'intégration Microsoft. Pour plus

© Acronis International GmbH, 2003-2026

d'informations, consultez Restaurer des données dans Sauvegarde Microsoft 365 dans la documentation Microsoft.

Site SharePoint

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Sauvegarde directe pour Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. [Pour restaurer des sites modernes] Développez le nœud **Groupes**, puis sélectionnez **Tous les groupes**.
4. [Pour restaurer des sites classiques] Développez le nœud **Collections de sites**, puis sélectionnez **Toutes les collections de sites**.
5. Sélectionnez un groupe ou une collection de sites, puis cliquez sur **Restauration**.

   Remarque
   Vous ne pouvez sélectionner qu'un élément à la fois.

6. Sélectionnez une sauvegarde (point de restauration), puis cliquez sur **Restaurer le site SharePoint complet**.
7. Cliquez sur **Démarrer la restauration**.

Le site SharePoint est complètement écrasé par le contenu sauvegardé. Toutes les modifications qui ne sont pas incluses dans la sauvegarde sont perdues. Vous ne pouvez pas modifier les paramètres d'écrasement, car ils dépendent de l'intégration Microsoft. Pour plus d'informations, consultez Restaurer des données dans Sauvegarde Microsoft 365 dans la documentation Microsoft.

Pour restaurer des éléments sauvegardés à partir du stockage des sauvegardes

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde**, puis sélectionnez **Stockage de sauvegarde de Microsoft 365**.
2. Sélectionnez une archive de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez une sauvegarde (point de restauration), puis cliquez sur **Restaurer le site SharePoint complet**, **Restaurer l'intégralité de OneDrive** ou **Restaurer l'intégralité de la boîte aux lettres**.
   Le nom du bouton dépend du type des données sauvegardées.
4. Cliquez sur **Démarrer la restauration**.

Lors de la restauration de boîtes aux lettres, les éléments modifiés ou supprimés sont remplacés par les éléments de la sauvegarde. Les nouveaux éléments et les éléments inchangés ne sont pas écrasés. Lors de la restauration de comptes OneDrive et de sites SharePoint, la sauvegarde écrase tous les fichiers existants. Toutes les modifications qui ne sont pas incluses dans la sauvegarde sont perdues.

© Acronis International GmbH, 2003-2026

Vous ne pouvez pas modifier les paramètres d'écrasement, car ils dépendent de l'intégration Microsoft. Pour plus d'informations, consultez Restaurer des données dans Sauvegarde Microsoft 365 dans la documentation Microsoft.

Révoquer un plan de sauvegarde pour la sauvegarde directe vers Microsoft 365

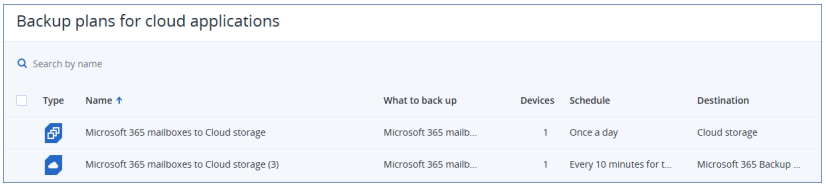
Vous pouvez révoquer un plan de sauvegarde dans l'onglet **Gestion** > **Sauvegardes d'applications cloud** ou dans l'onglet **Terminaux**.

Vous pouvez révoquer un plan de sauvegarde à partir d'une ressource individuelle ou d'un groupe de terminaux.

Pour révoquer un plan de sauvegarde

Gestion > Sauvegarde d'applications cloud

1. Dans la console Cyber Protect, accédez à **Gestion**, puis cliquez sur **Sauvegardes d'applications cloud**.
2. Sélectionnez un plan de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**, puis cliquez sur **Modifier**.
   Vous pouvez distinguer les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** et **Microsoft 365 Business – Sauvegarde** en comparant leurs icônes et la destination de la sauvegarde. Les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** ne peuvent utiliser que le stockage de sauvegarde Microsoft 365.



3. Dans le plan de sauvegarde, cliquez sur **Terminaux**.
4. Sélectionnez les ressources pour lesquelles vous souhaitez révoquer le plan, puis cliquez sur **Supprimer**.
5. Cliquez sur **Terminé**.
6. Cliquez sur **Enregistrer**.
   En conséquence, le plan de sauvegarde est révoqué pour toutes les ressources supprimées.

> **Remarque**
> La révocation d'un plan de sauvegarde peut prendre quelques minutes, en raison du temps de traitement requis du côté du stockage des sauvegardes Microsoft 365.

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux**, puis cliquez sur **Sauvegarde directe pour Microsoft 365**.

© Acronis International GmbH, 2003-2026

2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. [Pour les ressources individuelles] Sélectionnez une ressource à partir de laquelle vous souhaitez révoquer un plan de sauvegarde, puis cliquez sur **Sauvegarde**.
4. [Pour les groupes de terminaux] Sélectionnez un groupe à partir duquel vous souhaitez révoquer un plan de sauvegarde, puis cliquez sur **Sauvegarde de groupe**.
5. Cliquez sur l'icône en forme d'engrenage située à côté du nom du plan de sauvegarde, puis sur **Retirer**.

Remarque
La révocation d'un plan de sauvegarde peut prendre quelques minutes, en raison du temps de traitement nécessaire du côté du stockage des sauvegardes Microsoft 365.

Suppression d'un plan de sauvegarde

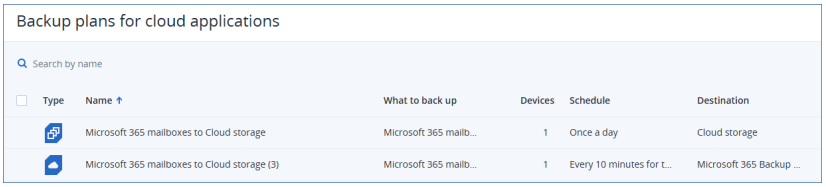
Vous pouvez supprimer un plan de sauvegarde dans l'onglet **Gestion** > **Sauvegardes d'applications dans le cloud** ou dans l'onglet **Terminaux**.

Remarque
Dans l'onglet **Terminaux**, vous ne pouvez pas supprimer les plans qui sont appliqués aux groupes de terminaux.

Pour supprimer un plan de sauvegarde

Gestion > Sauvegarde d'applications cloud

1. Dans la console Cyber Protect, accédez à **Gestion** > **Sauvegarde d'applications cloud**.
2. Sélectionnez un plan de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365**.
   Vous pouvez distinguer les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** et **Microsoft 365 Business – Sauvegarde** en comparant leurs icônes et la destination de la sauvegarde. Les plans de sauvegarde pour **Sauvegarde directe dans le stockage de sauvegarde de Microsoft** ne peuvent utiliser que le stockage de sauvegarde Microsoft 365.



3. Cliquez sur **Supprimer**.
4. Cochez la case pour confirmer votre décision, puis cliquez sur **Supprimer**.

Remarque
La suppression d'un plan de sauvegarde peut prendre quelques minutes, en raison du temps de traitement requis par le stockage des sauvegardes Microsoft 365.

© Acronis International GmbH, 2003-2026

Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** puis cliquez sur **Sauvegarde directe pour Microsoft 365**.
2. [Si plusieurs organisations Microsoft 365 sont ajoutées] Sélectionnez une organisation Microsoft 365.
3. Sélectionnez une ressource à laquelle le plan que vous souhaitez supprimer est appliqué, puis cliquez sur **Sauvegarde**.
4. Cliquez sur l'icône en forme d'engrenage située à côté du nom du plan de sauvegarde, puis sur **Supprimer**.
5. Cochez la case pour confirmer votre décision, puis cliquez sur **Supprimer**.

Remarque
La suppression d'un plan de sauvegarde peut prendre quelques minutes, en raison du temps de traitement requis par le stockage des sauvegardes Microsoft 365.

Agent pour Office 365 installé localement

Ajout d'une organisation Microsoft 365

Pour ajouter une organisation Microsoft 365

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur de l'entreprise.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit, puis cliquez sur **Téléchargements** > **Agent pour Office 365**.
3. Téléchargez l'agent et installez-le sur une machine Windows connectée à Internet.
4. Dans la console Cyber Protect, accédez à **Terminaux** > **Microsoft Office 365**.
5. Dans la fenêtre qui s'ouvre, saisissez l'identifiant et le secret de l'application, ainsi que l'identifiant du tenant Microsoft 365. Pour plus informations sur leur recherche, reportez-vous à "Obtention de l'identifiant et du secret d'application" (p. 912).
6. Cliquez sur **OK**.

Les données de votre organisation apparaissent dans la console Cyber Protect, dans l'onglet **Microsoft Office 365**.

Important
Il ne peut y avoir qu'un seul agent pour Office 365 installé localement au sein d'une organisation (groupe de sociétés).

Obtention de l'identifiant et du secret d'application

Pour utiliser l'authentification moderne pour Office 365, vous devez créer une application personnalisée dans le centre d'administration d'Entra et lui attribuer une permission d'API

© Acronis International GmbH, 2003-2026

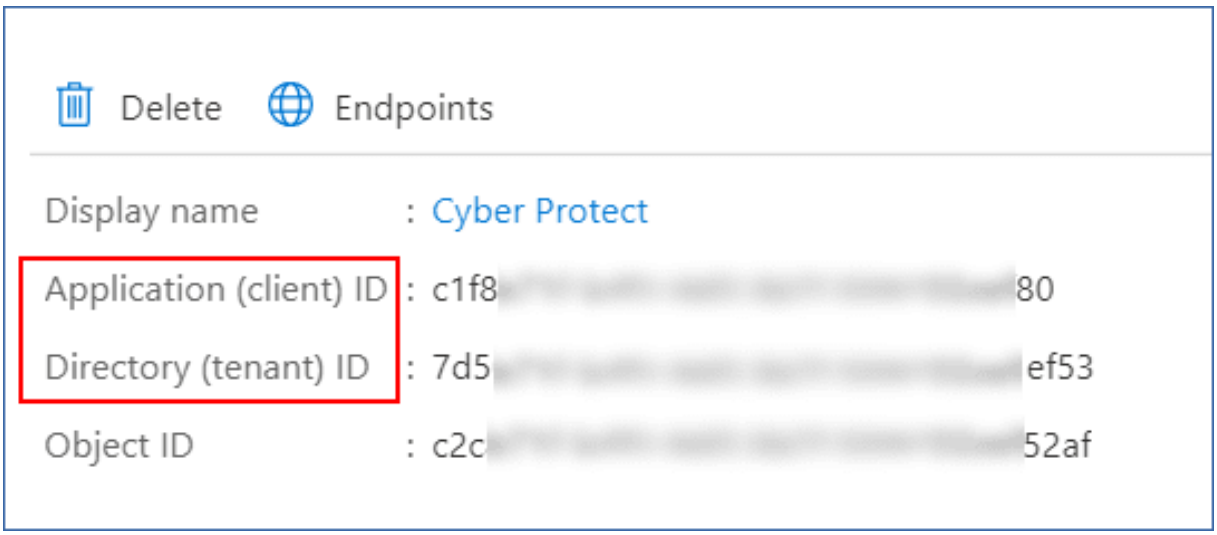
spécifiques. Vous obtiendrez ensuite l'**identifiant de l'application**, le **secret de l'application** et l'**identifiant du répertoire (tenant)** que vous devez saisir dans la console Cyber Protect.

Remarque
Sur l'ordinateur sur lequel Agent pour Office 365 est installé, vérifiez que vous autorisez l'accès à graph.microsoft.com par l'intermédiaire du port 443.

Pour créer une application dans le centre d'administration d'Entra

1. Connectez-vous au centre d'administration d'Entra en tant qu'administrateur.
2. Accédez à **Azure Active Directory** > **Inscriptions de l'application**, puis cliquez sur **Nouvelle inscription**.
3. Spécifiez un nom pour votre application personnalisée, par exemple Cyber Protection.
4. Dans **Types de comptes pris en charge**, sélectionnez **Comptes dans ce répertoire organisationnel uniquement**.
5. Cliquez sur **Enregistrer**.

Votre application est maintenant créée. Dans le centre d'administration d'Entra, accédez à la page d'**Vue d'ensemble** de l'application, puis vérifiez l'identifiant de votre application (client) et celui du répertoire (tenant).



Pour plus d'informations sur la création d'une application dans le centre d'administration d'Entra, référez-vous à la documentation Microsoft.

Pour accorder à l'application les permissions d'API nécessaires

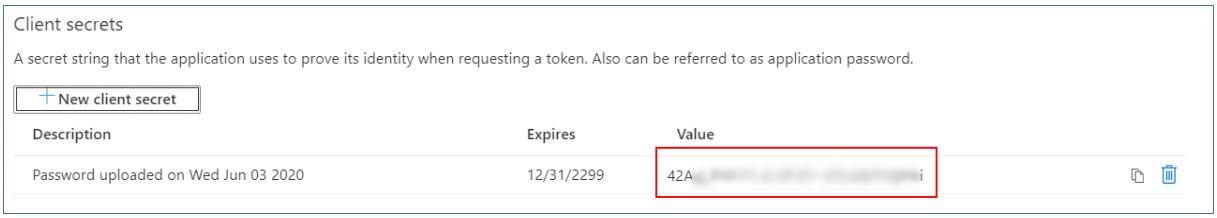
1. Dans le centre d'administration d'Entra, accédez aux **permissions API** de l'application, puis cliquez sur **Ajouter une autorisation**.
2. Sélectionnez l'onglet **API utilisées par mon organisation**, puis recherchez **Office 365 Exchange Online**.
3. Cliquez sur **Office 365 Exchange Online**, puis sur **Permissions d'application**.

© Acronis International GmbH, 2003-2026

4. Cochez la case **full_access_as_app**, puis cliquez sur **Ajouter des permissions**.
5. Dans **Permissions d'API**, cliquez sur **Ajouter une permission**.
6. Sélectionnez **Microsoft Graph**.
7. Sélectionnez **Permissions d'application**.
8. Développez l'onglet **Répertoire**, puis cochez la case **Directory.Read.All**. Cliquez sur **Ajouter des permissions**.
9. Vérifiez toutes les permissions, puis cliquez sur **Accorder des permissions d'administrateur pour <your application's name>**.
10. Confirmez votre choix en cliquant sur **Oui**.

Pour créer un secret d'application

1. Dans le centre d'administration d'Entra, accédez au **Certificats et secrets de** votre application > **Nouveau secret client**.
2. Dans la boîte de dialogue qui s'ouvre, sélectionnez Expire : **Jamais**, puis cliquez sur **Ajouter**.
3. Vérifiez le secret de votre application dans le champ **Valeur**, puis mémorisez-le.



Pour plus d'informations sur le secret d'application, reportez-vous à la documentation Microsoft.

Modification des identifiants de Microsoft 365

Vous pouvez modifier les identifiants de Microsoft 365 sans réinstaller l'agent.

Modification des identifiants de Microsoft 365

1. Cliquez sur **Terminaux** > **Microsoft Office 365**.
2. Sélectionnez l'organisation Microsoft 365.
3. Cliquez sur **Indiquer l'identifiant**.
4. Saisissez l'identifiant et le secret de l'application, ainsi que l'identifiant du tenant Microsoft 365. Pour plus informations sur leur recherche, reportez-vous à "Obtention de l'identifiant et du secret d'application" (p. 912).
5. Cliquez sur **OK**.

© Acronis International GmbH, 2003-2026

Protection des boîtes aux lettres Exchange Online

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder des boîtes aux lettres utilisateur et communes. Les boîtes aux lettres de groupe et les boîtes aux lettres d'archive (**Archives permanentes**) ne peuvent pas être sauvegardées.

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers de courriers électroniques
- Messages de courriers électroniques
- Événements de calendrier
- Tâches
- Contacts
- Entrées de journal
- Notes

Vous pouvez utiliser la fonction de recherche pour trouver l'emplacement des éléments.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres existante, les éléments existants dont les identifiants sont identiques sont écrasés.

La restauration des éléments de boîtes aux lettres n'écrase aucun élément. À la place, le chemin d'accès complet vers un élément de boîte aux lettres est recréé dans le dossier cible.

Sélection des boîtes aux lettres Microsoft 365

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des boîtes aux lettres

1. Cliquez sur **Microsoft Office 365**.
2. Sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
3. Cliquez sur **Sauvegarder**.

© Acronis International GmbH, 2003-2026

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Microsoft Office 365**.
2. Sélectionnez la boîte aux lettres à restaurer, puis cliquez sur **Restauration**.
   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.
   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Boîte aux lettres**.
5. Dans **Boîte aux lettres cible**, afficher, modifier ou spécifier la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas, vous devez spécifier la boîte aux lettres cible.
6. Cliquez sur **Démarrer la restauration**.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Microsoft Office 365**.
2. Sélectionnez la boîte aux lettres d'origine des éléments à restaurer, puis cliquez sur **Restauration**.
   Vous pouvez rechercher les boîtes aux lettres par nom. Les caractères génériques ne sont pas pris en charge.
   Si la boîte aux lettres a été supprimée, sélectionnez-la dans l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
4. Cliquez sur **Restaurer** > **Messages électroniques**.
5. Sélectionnez les éléments que vous souhaitez restaurer.
   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les messages de courrier électronique : recherche par sujet, expéditeur, destinataire, nom de la pièce jointe et date.
   - Pour les événements : recherche par titre et date.
   - Pour les tâches : recherche par sujet et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.

   Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes.

© Acronis International GmbH, 2003-2026

Remarque
Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.

Lorsqu'un message de courrier électronique est sélectionné, vous pouvez cliquer sur **Envoyer sous forme de message électronique** pour l'envoyer à une adresse électronique. Le message est envoyé à partir de l'adresse électronique de votre compte d'administrateur.

Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

6. Cliquez sur **Restaurer**.
7. Dans **Boîte aux lettres cible**, afficher, modifier ou spécifier la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas, vous devez spécifier la boîte aux lettres cible.
8. Cliquez sur **Démarrer la restauration**.
9. Confirmez votre choix.

Les éléments de boîte aux lettres sont toujours restaurés dans le dossier **Éléments restaurés** de la boîte aux lettres cible.

Protection des données Google Workspace

Remarque
Cette fonctionnalité n'est pas disponible pour les tenants en mode Conformité. Pour plus d'informations, voir "Mode de conformité" (p. 1615).

Que signifie la protection Google Workspace ?

- Service de sauvegarde et de restauration de Cloud à Cloud des données utilisateur de Google Workspace (boîtes aux lettres Gmail, Agendas, Contacts, Google Drives) et Drive partagés Google Workspace.
- Restauration granulaire d'e-mails, fichiers, contacts et autres éléments.
- Assistance pour plusieurs organisations Google Workspace et restauration entre les organisations.
- Notarisation facultative des fichiers sauvegardés au moyen de la base de données blockchain Ethereum. Lorsqu'elle est activée, elle vous permet de prouver qu'un fichier est authentique et inchangé depuis sa sauvegarde.
- Recherche en texte intégral facultative. Lorsque cette fonction est activée, vous pouvez rechercher du contenu dans les e-mails.
- Vous pouvez protéger jusqu'à 5 000 éléments (boîtes aux lettres, instances Google Drive et Drive partagé) par entreprise, sans dégradation des performances.
- Les données sauvegardées sont compressées automatiquement et utilisent moins d'espace dans l'emplacement de sauvegarde que dans leur emplacement d'origine. Le niveau de compression

© Acronis International GmbH, 2003-2026

des sauvegardes de cloud à cloud est fixe et correspond au niveau **Normal** des sauvegardes non-cloud à cloud. Pour en savoir plus sur ces niveaux, voir "Niveau de compression" (p. 618).

Droits utilisateurs requis

Dans Cyber Protection

Dans Cyber Protection, vous devez être un administrateur d'entreprise agissant au niveau tenant client. Les administrateurs d'entreprise agissant au niveau d'une unité, les administrateurs d'unité et les utilisateurs ne peuvent pas sauvegarder ou récupérer les données de Google Workspace.

Dans Google Workspace

Pour ajouter votre organisation Google Workspace au service Cyber Protection, vous devez être connecté en tant que super administrateur, avec l'accès aux API activé (**Security** > **Document de référence sur les API** > **Activer l'accès aux API** dans la console d'administration Google).

Le mot de passe du super administrateur n'est stocké nulle part et n'est pas utilisé pour effectuer la sauvegarde et la restauration. La modification de ce mot de passe dans Google Workspace n'affecte pas le fonctionnement du service Cyber Protection.

Si le super administrateur qui a ajouté l'organisation Google Workspace est supprimé de Google Workspace ou se voit attribuer un rôle avec des privilèges moindres, les sauvegardes échoueront avec une erreur telle que « Accès refusé ». Dans ce cas, répétez la procédure décrite à l'adresse "Ajouter une organisation Google Workspace" (p. 919) et indiquez des identifiants valides pour le super administrateur. Pour éviter ce problème, nous vous recommandons de créer un utilisateur super administrateur dédié à la sauvegarde et à la restauration.

Pour découvrir et sauvegarder des lecteurs partagés, l'utilisateur superadministrateur doit au moins disposer d'une licence Google Workspace Business Standard.

À propos de la planification de sauvegarde

Étant donné que l'agent Cloud sert plusieurs clients, il détermine seul l'heure de début de chaque plan de protection, pour garantir une charge égale dans une journée et une qualité de service égale pour tous les clients.

Chaque plan de protection s'exécute tous les jours à la même heure.

L’option par défaut est **Une fois par jour**. Vous pouvez planifier jusqu’à six sauvegardes par jour. Les sauvegardes démarrent à des intervalles approximatifs qui dépendent de la charge actuelle de l’agent cloud, qui dessert plusieurs clients dans un centre de données. Cela garantit une charge uniforme tout au long de la journée et une qualité de service équivalente pour tous les clients.

© Acronis International GmbH, 2003-2026

Limites

- La console Cyber Protect affiche uniquement les utilisateurs auxquels une licence Google Workspace a été affectée, et une boîte aux lettres ou un espace Google Drive.
- Les utilisateurs Google Workspace archivés ou suspendus s'affichent comme étant inactifs (grisés) dans la console Cyber Protect après l'opération de découverte qui suit le changement de leur statut. Vous ne pouvez pas appliquer de nouveaux plans de sauvegarde aux utilisateurs inactifs. Les plans de sauvegarde existants restent actifs pendant 72 heures.

  Après l'opération de découverte qui suit la période de 72 heures, les utilisateurs archivés ou suspendus sont supprimés de la console Cyber Protect et leurs données ne sont plus sauvegardées. Les sauvegardes existantes restent disponibles.
- Les sauvegardes des comptes utilisateur Google Workspace supprimés ne sont pas supprimées automatiquement du stockage dans le cloud. Ces sauvegardes sont facturées en fonction de l'espace de stockage qu'elles utilisent.
- Les documents aux formats Google natifs sont sauvegardés en tant que documents Office génériques et s'affichent avec une extension différente dans la console Cyber Protect, .docx ou .pptx par exemple. Ces documents sont reconvertis dans leur format d'origine lors de la restauration.
- Vous pouvez exécuter manuellement jusqu'à 10 sauvegardes par heure. Pour plus d'informations, voir "Exécution manuelle de sauvegardes de cloud à cloud" (p. 273).
- Vous pouvez exécuter simultanément jusqu'à 10 opérations de restauration de cloud à cloud. Ce nombre inclut les opérations de restauration de Microsoft 365 et de Google Workspace.
- Vous ne pouvez pas simultanément restaurer des éléments depuis différents points de restauration, même si vous pouvez sélectionner ces éléments dans les résultats de recherche.
- **Direct Backup to Public Cloud** is not supported.
- Vous ne pouvez appliquer à une ressource qu'un seul plan de sauvegarde.
- Lorsqu'un plan de sauvegarde individuel et un plan de sauvegarde de groupe sont appliqués à la même ressource, les paramètres du plan individuel sont prioritaires.

Important
Actions concernant les ressources de cloud à cloud telles que l'affichage du contenu d'e-mails sauvegardés, le téléchargement de pièces jointes ou de fichiers, la restauration d'e-mails sur des boîtes aux lettres autres que les boîtes aux lettres d'origine, ou l'envoi de tels contenus par e-mail pouvant constituer une violation de la confidentialité des utilisateurs. Ces actions sont consignées dans le portail de gestion, dans **Surveillance** > **Journal d'audit**.

Ajouter une organisation Google Workspace

Pour ajouter une organisation Google Workspace au service Cyber Protection, vous devez disposer d'un projet Google Cloud personnel dédié. Pour plus d'informations sur le processus de création et de configuration d'un tel projet, consultez "Création d'un projet Google Cloud personnel" (p. 921).

© Acronis International GmbH, 2003-2026

Pour ajouter une organisation Google Workspace en utilisant un projet Google Cloud personnel dédié

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur de l'entreprise.
2. Cliquez sur **Terminaux** > **Ajouter** > **Google Workspace**.
3. Saisissez l'adresse e-mail d'un super administrateur de votre compte Google Workspace.
   Pour cette procédure, il est utile de savoir si la vérification en 2 étapes est activée pour le compte e-mail de Super administrateur.
4. Recherchez le fichier JSON qui contient la clé privée du compte de service que vous avez créé dans votre projet Google Cloud.
   Vous pouvez également coller le contenu du fichier en tant que texte.
5. Cliquez sur **Confirmer**.

Votre organisation Google Workspace apparaît alors sous l'onglet **Terminaux** dans la console Cyber Protect.

Conseils utiles

- Après l'ajout d'une organisation Google Workspace, les données utilisateurs et les Drive partagés qui se trouvent dans le domaine principal et dans tous les domaines secondaires (s'il y en a) seront sauvegardés. Les ressources sauvegardées s'afficheront sous la forme d'une liste, et ne seront pas regroupées par domaine.
- L'agent Cloud se synchronise avec Google Workspace toutes les 24 heures, à compter du moment où l'organisation est ajoutée au service Cyber Protection. Si vous ajoutez ou supprimez un utilisateur ou un lecteur partagé, ce changement ne sera pas immédiatement visible dans la console Cyber Protect. Pour synchroniser la modification immédiatement, sélectionnez l'organisation sur la page **Google Workspace**, puis cliquez sur **Actualiser**.
  Pour plus d'informations sur la synchronisation des ressources d'une organisation Google Workspace et de la console Cyber Protect, voir "Découverte des ressources Google Workspace" (p. 924).
- Si vous avez appliqué un plan de protection au groupe **Tous les utilisateurs** ou **Tous les Drive partagés**, les éléments récemment ajoutés ne seront inclus dans la sauvegarde que lorsque la synchronisation aura été effectuée.
- Conformément à la politique de Google, lorsqu'un utilisateur ou un Drive partagé est supprimé de l'interface utilisateur graphique de Google Workspace, il reste encore disponible pendant quelques jours via l'API. Pendant cette période, l'élément supprimé est inactif (grisé) dans la console Cyber Protect et n'est pas sauvegardé. Lorsque l'élément supprimé ne sera plus disponible via l'API, il disparaîtra de la console Cyber Protect. Ses sauvegardes (s'il y en a) se trouvent sous **Stockage de sauvegarde** > **Sauvegardes d'applications Cloud**.

© Acronis International GmbH, 2003-2026

Création d'un projet Google Cloud personnel

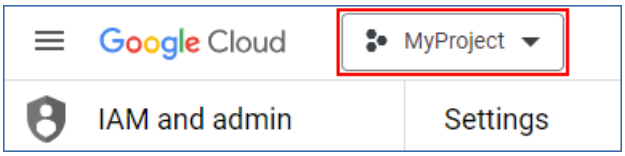
Pour ajouter votre organisation Google Workspace au service Cyber Protection à l'aide d'un projet Google Cloud personnel dédié, procédez comme suit :

1. Créez un nouveau projet Google Cloud.
2. Activez les API nécessaires pour ce projet.
3. Configurez les informations d'identification pour ce projet :
   a. Configurez l'écran d'autorisation OAuth.
   b. Créez et configurez le compte de service pour le service Cyber Protection.
4. Accordez à votre nouveau projet l'accès à votre compte Google Workspace.

Remarque
Cette rubrique contient une description d'une interface utilisateur tierce, susceptible d'être modifiée sans préavis.

Pour créer un nouveau projet Google Cloud

1. Connectez-vous à la plate-forme Google Cloud (console.cloud.google.com) en tant que super administrateur.
2. Dans la console de la plate-forme Google Cloud, cliquez sur le sélecteur de projets en haut à gauche.



3. Dans l'écran qui s'affiche, sélectionnez une organisation, puis cliquez sur **Nouveau projet**.



4. Spécifiez un nom pour votre nouveau projet.
5. Cliquez sur **Créer**.

Un nouveau projet Google Cloud est alors créé.

Pour activer les API nécessaires pour ce projet

1. Dans la console de la plate-forme Google Cloud, sélectionnez votre nouveau projet.
2. Dans le menu de navigation, sélectionnez **API et services** > **API et services activés**.
3. Désactivez toutes les API activées par défaut dans ce projet, une par une :
   a. Faites défiler la page **API et services activés** vers le bas, puis cliquez sur le nom d'une API activée.
   La page **Détails de l'API/du service** de l'API sélectionnée s'ouvre.

© Acronis International GmbH, 2003-2026

b. Cliquez sur **Désactiver l'API**, puis confirmez votre choix en cliquant sur **Désactiver**.

c. [Si vous y êtes invité] Confirmez votre choix en cliquant sur **Confirmer**.

d. Revenez à la page **API et services** > **API et services activés**, puis désactivez l'API suivante.

4. Dans le menu de navigation, sélectionnez **API et services** > **Bibliothèque**.
5. Dans la bibliothèque d'API, activez les API suivantes, une par une :
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - API Google Drive
   - Google People API

   Trouvez les API requises à l'aide de la barre de recherche. Pour activer une API, cliquez sur son nom, puis sur **Activer**. Pour rechercher l'API suivante, revenez à la bibliothèque d'API en sélectionnant **API et services** > **Bibliothèque** dans le menu de navigation.

Pour configurer l'écran d'autorisation OAuth

1. Dans le menu de navigation de Google Cloud Platform, sélectionnez **API et services** > **Écran d'autorisation OAuth**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le type d'utilisateur **Interne**, puis cliquez sur **Créer**.
3. Dans le champ **Nom de l'appli**, spécifiez un nom pour votre application.
4. Dans le champ **Adresse e-mail d'assistance utilisateur**, saisissez l'adresse e-mail du super administrateur.
5. Dans le champ **Coordonnées du développeur**, saisissez l'adresse e-mail du super administrateur.
6. Laissez tous les autres champs vides, puis cliquez sur **Enregistrer et continuer**.
7. Sur la page **Niveau d'accès**, cliquez sur **Enregistre et continuer**, sans rien modifier.
8. Sur la page **Résumé**, vérifiez vos paramètres, puis cliquez sur **Revenir au tableau de bord**.

Pour créer et configurer le compte de service pour le service Cyber Protection

1. Dans le menu de navigation de Google Cloud Platform, sélectionnez **API et services** > **Comptes de service**.
2. Cliquez sur **Créer un compte de service**.
3. Spécifiez un nom pour le compte de service.
4. [Facultatif] Spécifiez une description pour le compte de service.
5. Cliquez sur **Créer et continuer**.
6. Ne modifiez rien dans les étapes **Autoriser ce compte de service à accéder au projet** et **Autoriser les utilisateurs à accéder à ce compte de service**.
7. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

La page **Comptes de service** s'ouvre.

8. Sur la page **Comptes de service**, sélectionnez le nouveau compte de service, puis sous **Actions**, cliquez sur **Gérer les clés**.
9. Sous **Clés**, cliquez sur **Ajouter une clé** > **Créer clé**, puis sélectionnez le type de clé **JSON**.
10. Cliquez sur **Créer**.

    Un fichier JSON contenant la clé privée du compte de service est automatiquement téléchargé sur votre ordinateur. Conservez ce fichier précieusement, car vous en aurez besoin pour ajouter votre organisation Google Workspace au service Cyber Protection.

Pour accorder l'accès à votre compte Google Workspace à votre nouveau projet

1. Dans le menu de navigation de Google Cloud Platform, sélectionnez **IAM et Admin** > **Comptes de service**.
2. Dans la liste, recherchez le compte de service que vous avez créé, puis copiez l'identifiant client indiqué dans la colonne **ID client OAuth 2.0**.
3. Connectez-vous à la console d'administration de Google (admin.google.com) en tant que super administrateur.
4. Dans le menu de navigation, sélectionnez **Sécurité** > **Contrôles d'accès et de données** > **Contrôles d'API**.
5. Faites défiler la page **Contrôles d'API**, puis sous **Délégation au niveau du domaine**, cliquez sur **Gérer la délégation au niveau du domaine**.

   La page **Délégation au niveau du domaine** s'affiche.
6. Sur la page **Délégation au niveau du domaine**, cliquez sur **Ajouter nouveau**.

   La fenêtre **Ajouter un identifiant client** s'ouvre.
7. Dans le champ **Identifiant du client**, entrez l'ID du client de votre compte de service.
8. Dans le champ **Champs d'application OAuth**, copiez et collez la liste des champs d'application délimités par des virgules suivante :

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   Vous pouvez également ajouter des champs d'application, un par ligne :

   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. Cliquez sur **Autoriser**.

© Acronis International GmbH, 2003-2026

Votre nouveau projet Google Cloud peut alors accéder aux données de votre compte Google Workspace. Pour sauvegarder les données, vous devez lier ce projet au service Cyber Protection. Pour en savoir plus sur la façon de procéder, reportez-vous à "Pour ajouter une organisation Google Workspace en utilisant un projet Google Cloud personnel dédié" (p. 920).

Si vous devez révoquer l'accès de votre projet Google Cloud à votre compte Google Workspace, et respectivement, l'accès au service Cyber Protection, supprimez le client API que votre projet utilise.

Pour révoquer l'accès à votre compte Google Workspace

1. Dans la console d'administration de Google (admin.google.com), connectez-vous en tant que super administrateur.
2. Dans le menu de navigation, sélectionnez **Sécurité** > **Contrôles d'accès et de données** > **Contrôles d'API**.
3. Faites défiler la page **Contrôles d'API**, puis sous **Délégation au niveau du domaine**, cliquez sur **Gérer la délégation au niveau du domaine**.
   La page **Délégation au niveau du domaine** s'affiche.
4. Sur la page **Délégation au niveau du domaine**, sélectionnez le client API que votre projet utilise, puis cliquez sur **Supprimer**.
   Votre projet Google Cloud et le service Cyber Protection ne seront alors plus en mesure d'accéder à votre compte Google Workspace ni de sauvegarder les données qu'il contient.

Découverte des ressources Google Workspace

Lorsque vous ajoutez une organisation Google Workspace au service Cyber Protection, les ressources de cette organisation (boîtes aux lettres et services Google Drive, par exemple) sont synchronisées avec la console Cyber Protect. Cette opération est appelée découverte et elle est consignée dans **Surveillance** > **Activités**.

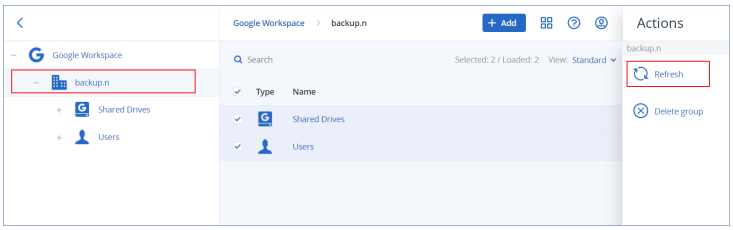
Une fois la découverte terminée, vous pouvez voir les ressources de l'organisation Google Workspace dans l'onglet **Terminaux** > **Google Workspace** de la console Cyber Protect et pouvez leur appliquer des plans de sauvegarde.

Une opération de découverte automatique est exécutée une fois par jour afin que la liste des ressources dans la console Cyber Protect soit à jour. Vous pouvez également synchroniser cette liste à la demande en réexécutant une opération de découverte manuellement.

Pour réexécuter une opération de découverte manuellement

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Google Workspace**.
2. Sélectionnez votre organisation Google Workspace, puis cliquez dans le panneau **Actions** sur **Actualiser**.

© Acronis International GmbH, 2003-2026



Remarque

Vous pouvez exécuter manuellement jusqu'à 10 découvertes par heure. Lorsque ce nombre est atteint, le nombre d'exécutions autorisé est réinitialisé à un par heure, puis une exécution supplémentaire est alors disponible toutes les heures jusqu'à ce qu'un total de 10 exécutions par heure soit atteint.

Configuration de la fréquence des sauvegardes Google Workspace

Par défaut, les sauvegardes Google Workspace s'exécutent une fois par jour et aucune autre option de planification n'est disponible.

Si la fonctionnalité de sauvegarde est activée dans votre tenant, l'option **Une fois par jour** est activée par défaut, et d'autres fréquences sont disponibles à la sélection.

Vous pouvez sélectionner le nombre de sauvegardes par jour, mais vous ne pouvez pas configurer l'heure de leur démarrage. Les sauvegardes démarrent automatiquement à des intervalles approximatifs qui dépendent de la charge actuelle de l'agent cloud desservant les nombreux clients d'un centre de données. De cette manière, la charge est égale toute la journée, ce qui garantit une qualité de service équivalente pour tous les clients.

Les options suivantes sont disponibles.

Planification des options	Intervalle approximatif entre chaque sauvegarde
Une fois par jour (par défaut)	24 heures
Deux fois par jour	12 heures
Trois fois par jour	8 heures
Six fois par jour	4 heures

Remarque

Selon la charge sur l'agent cloud et les limitations possibles côté Google Workspace, une sauvegarde peut démarrer plus tard ou prendre plus de temps que prévu. Si une sauvegarde est plus longue que l'intervalle moyen entre deux sauvegardes, la sauvegarde suivante est replanifiée, ce qui peut avoir pour résultat un nombre de sauvegardes quotidiennes inférieur au nombre sélectionné. Par exemple, il est possible que deux sauvegardes par jour seulement puissent s'effectuer, même si vous en avez sélectionné six.

© Acronis International GmbH, 2003-2026

Protéger des données Gmail

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder les boîtes aux lettres des utilisateurs Gmail. Une sauvegarde de boîte aux lettres inclut également des données d'Agenda et de Contacts. Vous pouvez également choisir de sauvegarder les agendas partagés.

Les éléments suivants sont *exclus* lors d'une sauvegarde :

- Les agendas **Anniversaires**, **Rappels**, **Tâches**
- Dossiers joints aux événements d'agenda
- Le dossier **Répertoire** des Contacts

Les éléments d'Agenda suivants sont *ignorés,* en raison des restrictions de l'API Google Agenda :

- Plages de rendez-vous
- Le champ Conférence d'un événement
- Le paramètre d'agenda **Notifications des événements « Toute la journée »**
- Le paramètre d'agenda **Accepter automatiquement les invitations** (dans les agendas pour les salons ou les espaces partagés)

Les éléments de Contacts suivants sont *ignorés,* en raison des restrictions de l'API Google People :

- Le dossier **Autres contacts**
- Les profils externes d'un contact (**Profil du répertoire**, **Profil Google**)
- Le champ de contact **Classer en tant que**

Quels éléments de données peuvent être restaurés ?

Les éléments suivants peuvent être restaurés à partir de sauvegardes de boîte aux lettres :

- Boîtes aux lettres
- Dossiers d'e-mail (selon la terminologie Google, « libellés ». Les **libellés** sont présentés dans le logiciel de sauvegarde en tant que dossiers, pour être cohérents avec la présentation d'autres données.)
- Messages de courriers électroniques
- Événements de calendrier
- Contacts

Vous pouvez utiliser la recherche pour localiser des éléments dans une sauvegarde.

Lorsque vous restaurez des boîtes aux lettres et des éléments de boîte aux lettres, vous pouvez choisir d'écraser ou non les éléments de l'emplacement de destination.

© Acronis International GmbH, 2003-2026

Limites

- Les photos des contacts ne peuvent pas être restaurées
- L'élément d'agenda **Absent du bureau** est restauré en tant qu'événement d'agenda régulier, en raison des restrictions de l'API Google Agenda

Sélection des boîtes aux lettres Gmail

Sélectionnez les boîtes aux lettres comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des boîtes aux lettres Gmail

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les boîtes aux lettres de tous les utilisateurs (y compris celles qui seront créés à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder des boîtes aux lettres utilisateur en particulier, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les boîtes aux lettres, puis cliquez sur **Sauvegarde**.
4. Dans le plan de sauvegarde, configurez les options suivantes :
   - [Si disponible] Dans **Quoi sauvegarder**, sélectionnez **Gmail**.
   - [Facultatif] Si vous souhaitez sauvegarder les calendriers partagés avec les utilisateurs sélectionnés, activez le commutateur **Inclure les calendriers partagés**.
   - Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.
   - Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
     - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
     - Cliquez sur **OK**.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.

© Acronis International GmbH, 2003-2026

3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer la boîte aux lettres, puis cliquez sur **Restauration**.
   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des boîtes aux lettres, sélectionnez **Gmail** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Intégralité de la boîte aux lettres**.
6. Si plusieurs organisations Google Workspace sont ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
7. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.
   Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
   Vous ne pouvez pas créer de nouvelle boîte aux lettres cible pendant la restauration. Pour restaurer une boîte aux lettres vers une nouvelle, vous devez d'abord créer la boîte aux lettres cible dans l'organisation Google Workspace souhaitée, puis laisser l'agent synchroniser le changement. L'agent Cloud se synchronise automatiquement avec Google Workspace toutes les 24 heures. Pour synchroniser la modification immédiatement, sélectionnez l'organisation sur la page **Google Workspace** de la console Cyber Protect, puis cliquez sur **Actualiser**.
8. Cliquez sur **Démarrer la restauration**.
9. Sélectionnez l'une des options d'écrasement :
   - **Écraser les éléments existants**
   - **Ne pas écraser les éléments existants**
10. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration d'éléments de boîte aux lettres

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.

© Acronis International GmbH, 2003-2026

3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont la boîte aux lettres contenait à l'origine les éléments à restaurer, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs et les groupes par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des boîtes aux lettres, sélectionnez **Gmail** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. Accédez au dossier requis. Si la sauvegarde n'est pas chiffrée, vous pouvez utiliser la recherche pour obtenir la liste des éléments requis.

   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.
   - Pour les e-mails : recherche par sujet, expéditeur, destinataire, date, nom de pièce jointe et contenu du message.

     Lors d'une recherche par date, vous pouvez sélectionner une date de début ou une date de fin (toutes deux incluses), ou les deux dates pour effectuer une recherche dans un intervalle de temps.

     La recherche par nom de pièce jointe ou dans le contenu du message ne donne des résultats que si l'option de **Recherche en texte intégral** a été activée lors de la sauvegarde. Vous pouvez spécifier la langue du fragment de message qui sera recherché en tant que paramètre supplémentaire.
   - Pour les événements : recherche par titre et date.
   - Pour les contacts : recherche par nom, adresse e-mail et numéro de téléphone.
7. Sélectionnez les éléments que vous souhaitez restaurer. Pour pouvoir sélectionner les dossiers, cliquez sur l'icône des dossiers à restaurer : 

   Par ailleurs, vous pouvez effectuer l'une des opérations suivantes :
   - Lorsqu'un élément est sélectionné, cliquez sur **Afficher le contenu** pour afficher son contenu, y compris les pièces jointes. Cliquez sur le nom d'un fichier de pièce jointe pour le télécharger.
   - Uniquement si la sauvegarde n'est pas chiffrée, que vous avez utilisé la fonction de recherche et que vous avec sélectionné un seul élément dans les résultats de recherche : cliquez sur **Afficher les versions** pour sélectionner la version de l'élément à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.
8. Cliquez sur **Restaurer**.

© Acronis International GmbH, 2003-2026

9. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
10. Dans **Restaurer vers la boîte aux lettres**, affichez, modifiez ou spécifiez la boîte aux lettres cible.

    Par défaut, la boîte aux lettres d'origine est sélectionnée. Si cette boîte aux lettres n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier la boîte aux lettres cible.
11. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans la boîte aux lettres cible. Le dossier d'origine est sélectionné par défaut.
12. Cliquez sur **Démarrer la restauration**.
13. Sélectionnez l'une des options d'écrasement :
    - **Écraser les éléments existants**
    - **Ne pas écraser les éléments existants**
14. Cliquez sur **Poursuivre** pour confirmer votre choix.

Protéger des fichiers Google Drive

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder l'intégralité d'une instance Google Drive, ou des fichiers et dossiers en particulier. Les fichiers sont sauvegardés avec les permissions de partage associées.

Important
Les éléments suivants ne sont pas sauvegardés :

- Dossier **Partagé avec moi**
- Le dossier **Ordinateurs** (créé par le client Sauvegarde et synchronisation)

Limites

De tous les formats de fichiers spécifiques à Google, les formats Google Docs, Google Sheets et Google Slides sont totalement pris en charge pour la sauvegarde et la restauration. Les autres formats propres à Google risquent de n'être pris en charge que partiellement, voire pas du tout. Par exemple, les fichiers Google Drawings sont restaurés sous forme de fichiers `.svg`, les fichiers Google Sites, sous forme de fichiers `.txt` et les fichiers Google Jamboard, sous forme de fichiers `.pdf`. Quant aux fichiers Google My Maps, ils sont ignorés pendant la sauvegarde.

Remarque
Les formats de fichiers qui ne sont pas propres à Google, par exemple, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, sont totalement pris en charge pour la sauvegarde et la restauration.

© Acronis International GmbH, 2003-2026

Quels éléments de données peuvent être restaurés ?

Vous pouvez restaurer l'intégralité d'une instance Google Drive, ou tout fichier ou dossier sauvegardé.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les fichiers hériter des permissions du dossier vers lequel ils sont restaurés.

Limites

- Les commentaires des fichiers ne sont pas restaurés.
- Les liens de partage des fichiers et des dossiers ne sont pas restaurés.
- Les **paramètres de propriété** en lecture seule pour les fichiers partagés (**Empêcher les éditeurs de modifier l'accès et d'ajouter des personnes** et **Désactiver les options permettant de télécharger, imprimer et copier pour les commentateurs et les lecteurs**) ne peuvent pas être modifiés lors d'une restauration.
- Vous ne pouvez pas modifier la propriété d'un dossier partagé lors de la restauration si l'option **Empêcher les éditeurs de modifier l'accès et d'ajouter des personnes** est activée pour ce dossier. Ce paramètre empêche l'API Gogle Drive de lister les permissions de dossiers. La propriété des fichiers de ce dossier est correctement restaurée.

Sélectionner des fichiers Google Drive

Sélectionnez les fichiers comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des fichiers Google Drive

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les fichiers de tous les utilisateurs (y compris des utilisateurs qui seront créés à l'avenir), développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder les fichiers d'utilisateurs en particulier, développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez sauvegarder les fichiers, puis cliquez sur **Sauvegarde**.
4. Dans le plan de sauvegarde, configurez les options suivantes :
   - [Si disponible] Dans **Quoi sauvegarder**, sélectionnez **Google Drive**.
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :

© Acronis International GmbH, 2003-2026

  - Conservez le paramètre par défaut **[Tous]** (tous les fichiers).
  - Spécifiez les fichiers et dossiers à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

    Vous pouvez utiliser des caractères génériques (*, ** et ?). Pour plus de détails sur la spécification des chemins et l'utilisation des caractères génériques, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 620).
  - Spécifiez les fichiers et dossiers à sauvegarder en cliquant sur Parcourir.

    Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul utilisateur.
- [Facultatif] Pour spécifier les fichiers et dossiers qui seront ignorés lors de la sauvegarde, dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions**.

  Les exclusions de fichiers ont priorité sur la sélection de fichiers. Si vous spécifiez le même fichier dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.
- Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.
- Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
  - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
  - Cliquez sur **OK**.

Restaurer une instance et des fichiers Google Drive

Restauration de l'intégralité d'une instance Google Drive

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer les fichiers Google Drive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des fichiers Google Drive, sélectionnez **Google Drive** dans **Filtre par contenu**.
5. Cliquez sur **Restaurer** > **Tout le Drive**.

© Acronis International GmbH, 2003-2026

6. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
7. Dans **Restaurer vers un Drive**, affichez, modifiez ou spécifiez l'utilisateur ou le Drive partagé cibles.

   L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible ou le Drive partagé cible.

   Si la sauvegarde contient des fichiers partagés, ces derniers seront restaurés vers le dossier racine du Drive cible.
8. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
9. Cliquez sur **Démarrer la restauration**.
10. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

11. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration de fichiers Google Drive

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Utilisateurs**, sélectionnez **Tous les utilisateurs**, sélectionnez l'utilisateur dont vous souhaitez restaurer les fichiers Google Drive, puis cliquez sur **Restauration**.

   Si l'utilisateur a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les utilisateurs par nom. Les caractères génériques ne sont pas pris en charge.

© Acronis International GmbH, 2003-2026

4. Sélectionnez un point de restauration.

   Remarque
   Pour afficher uniquement les points de restauration qui contiennent des fichiers Google Drive, sélectionnez **Google Drive** dans **Filtre par contenu**.

5. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
6. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.
7. Sélectionnez les fichiers que vous voulez restaurer.

   Si la sauvegarde n'est pas chiffrée et que vous avez sélectionné un seul fichier, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version du fichier à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.
8. Si vous souhaitez télécharger un fichier, sélectionnez-le, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Sauvegarder**. Sinon, ignorez cette étape.
9. Cliquez sur **Restaurer**.
10. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
11. Dans **Restaurer vers un Drive**, affichez, modifiez ou spécifiez l'utilisateur ou le Drive partagé cibles.

    L'utilisateur d'origine est sélectionné par défaut. Si cet utilisateur n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier l'utilisateur cible ou le Drive partagé cible.
12. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans l'instance Google Drive de l'utilisateur cible ou dans le Drive partagé cible. L'emplacement d'origine est sélectionné par défaut.
13. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
14. Cliquez sur **Démarrer la restauration**.
15. Sélectionnez l'une des options d'écrasement de fichier :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.

© Acronis International GmbH, 2003-2026

Option	Description
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

16. Cliquez sur **Poursuivre** pour confirmer votre choix.

Protection des fichiers de Drive partagés

Quels éléments peuvent être sauvegardés ?

Vous pouvez sauvegarder l'intégralité d'un Drive partagé, ou des fichiers et dossiers en particulier. Les fichiers sont sauvegardés avec les permissions de partage associées.

Important
Le dossier **Partagé avec moi** n'est pas sauvegardé.

Limites

- Un Drive partagé qui ne comprend aucun membre ne peut pas être sauvegardé, en raison des restrictions de l'Google Drive API.
- De tous les formats de fichiers spécifiques à Google, les formats Google Docs, Google Sheets et Google Slides sont totalement pris en charge pour la sauvegarde et la restauration. Les autres formats propres à Google risquent de n'être pris en charge que partiellement, voire pas du tout. Par exemple, les fichiers Google Drawings sont restaurés sous forme de fichiers `.svg`, les fichiers Google Sites, sous forme de fichiers `.txt` et les fichiers Google Jamboard, sous forme de fichiers `.pdf`. Quant aux fichiers Google My Maps, ils sont ignorés pendant la sauvegarde.

  Remarque
  Les formats de fichiers qui ne sont pas propres à Google, par exemple, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`, sont totalement pris en charge pour la sauvegarde et la restauration.

Quels éléments de données peuvent être restaurés ?

Vous pouvez restaurer l'intégralité d'un Drive partagé, ou tout fichier ou dossier sauvegardé.

Vous pouvez choisir de restaurer les permissions de partage ou de laisser les fichiers hériter des permissions du dossier vers lequel ils sont restaurés.

Les éléments suivants ne sont pas restaurés :

- Les permissions de partage d'un fichier ayant été partagé avec un utilisateur externe à l'organisation ne sont pas restaurées si le partage en dehors de l'organisation est désactivé dans le Drive partagé cible.

© Acronis International GmbH, 2003-2026

- Les permissions de partage d'un fichier ayant été partagé avec un utilisateur qui n'est pas membre du Drive partagé cible ne sont pas restaurées si **Partage avec des non-membres** est désactivé dans le Drive partagé cible.

Limites

- Les commentaires des fichiers ne sont pas restaurés.
- Les liens de partage des fichiers et des dossiers ne sont pas restaurés.

Sélection de fichiers de Drive partagés

Sélectionnez les fichiers comme décrit ci-dessous, puis spécifiez d'autres paramètres du plan de protection au besoin.

Pour sélectionner des fichiers de Drive partagés

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez sauvegarder les données utilisateur. Sinon, ignorez cette étape.
3. Effectuez l'une des actions suivantes :
   - Pour sauvegarder les fichiers de tous les Drive partagés (y compris des Drive partagés qui seront créés à l'avenir), développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, puis cliquez sur **Sauvegarde de groupe**.
   - Pour sauvegarder les fichiers de Drive partagés individuels, développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, sélectionnez les Drive partagés à sauvegarder, puis cliquez sur **Sauvegarde**.
4. Dans le plan de sauvegarde, configurez les options suivantes :
   - Dans **Éléments à sauvegarder**, effectuez l'une des actions suivantes :
     - Conservez le paramètre par défaut **[Tous]** (tous les fichiers).
     - Spécifiez les fichiers et dossiers à sauvegarder en ajoutant leur nom ou leur chemin d'accès.

       Vous pouvez utiliser des caractères génériques (*, ** et ?). Pour en savoir plus sur la définition de chemin d'accès et sur l'utilisation de caractères génériques, consultez la section « Filtres de fichiers ».
     - Spécifiez les fichiers et dossiers à sauvegarder en cliquant sur Parcourir.

       Le lien **Parcourir** est disponible uniquement lors de la création d'un plan de protection pour un seul Drive partagé.
   - [Facultatif] Pour spécifier les fichiers et dossiers qui seront ignorés lors de la sauvegarde, dans **Éléments à sauvegarder**, cliquez sur **Afficher les exclusions**.

     Les exclusions de fichiers ont priorité sur la sélection de fichiers. Si vous spécifiez le même fichier dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.
   - Dans **Durée de conservation**, configurez les règles de rétention des sauvegardes.

© Acronis International GmbH, 2003-2026

- Dans **Chiffrement**, cliquez sur **Spécifier le mot de passe**.
  - Spécifiez et confirmez le mot de passe de chiffrement, puis sélectionnez l'algorithme de chiffrement.
  - Cliquez sur **OK**.

Restauration des Drives partagés et des fichiers de Drive partagés

Restauration de l'intégralité d'un Drive partagé

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, sélectionnez le Drive partagé que vous souhaitez restaurer, puis cliquez sur **Restauration**.
   Si le Drive partagé a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.
   Vous pouvez rechercher les Drive partagés par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Drive partagé complet**.
6. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.
   L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
7. Dans **Restaurer vers le Drive**, affichez, modifiez ou spécifiez le Drive partagé ou l'utilisateur cibles. Si vous précisez un utilisateur, les données seront restaurées vers l'instance Google Drive de cet utilisateur.
   Le Drive partagé d'origine est sélectionné par défaut. Si ce Drive partagé n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier le Drive partagé cible ou l'utilisateur cible.
8. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
9. Cliquez sur **Démarrer la restauration**.

© Acronis International GmbH, 2003-2026

10. Sélectionnez l'une des options d'écrasement :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

11. Cliquez sur **Poursuivre** pour confirmer votre choix.

Restauration des fichiers de Drive partagés

1. Cliquez sur **Google Workspace**.
2. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, sélectionnez l'organisation dont vous souhaitez restaurer les données sauvegardées. Sinon, ignorez cette étape.
3. Développez le nœud **Drive partagé**, sélectionnez **Tous les Drive partagés**, sélectionnez le Drive partagé qui contenait à l'origine les fichiers que vous souhaitez restaurer, puis cliquez sur **Restauration**.

   Si le Drive partagé a été supprimé, sélectionnez-le dans la section **Sauvegardes d'applications Cloud** de l'onglet Stockage de sauvegarde, puis cliquez sur **Afficher les sauvegardes**.

   Vous pouvez rechercher les Drive partagés par nom. Les caractères génériques ne sont pas pris en charge.
4. Sélectionnez un point de restauration.
5. Cliquez sur **Restaurer** > **Fichiers/dossiers**.
6. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.
7. Sélectionnez les fichiers que vous voulez restaurer.

   Si la sauvegarde n'est pas chiffrée et que vous avez sélectionné un seul fichier, vous pouvez cliquer sur **Afficher les versions** pour sélectionner la version du fichier à restaurer. Vous pouvez choisir n'importe quelle version sauvegardée, avant ou après le point de restauration sélectionné.
8. Si vous souhaitez télécharger un fichier, sélectionnez-le, cliquez sur **Télécharger**, sélectionnez l'emplacement dans lequel le sauvegarder, puis cliquez sur **Sauvegarder**. Sinon, ignorez cette étape.
9. Cliquez sur **Restaurer**.

© Acronis International GmbH, 2003-2026

10. Si plusieurs organisations Google Workspace ont été ajoutées au service Cyber Protection, cliquez sur **Organisation Google Workspace** pour afficher, modifier ou spécifier l'organisation cible.

    L'organisation d'origine est sélectionnée par défaut. Si cette organisation n'est plus enregistrée dans le service Cyber Protection, vous devez sélectionner une nouvelle organisation cible parmi les organisations enregistrées disponibles.
11. Dans **Restaurer vers le Drive**, affichez, modifiez ou spécifiez le Drive partagé ou l'utilisateur cibles. Si vous précisez un utilisateur, les données seront restaurées vers l'instance Google Drive de cet utilisateur.

    Le Drive partagé d'origine est sélectionné par défaut. Si ce Drive partagé n'existe pas ou si une organisation non d'origine est sélectionnée, vous devez spécifier le Drive partagé cible ou l'utilisateur cible.
12. Dans **Chemin d'accès**, affichez ou modifiez le dossier cible dans le Drive partagé cible ou dans le Google Drive de l'utilisateur cible. L'emplacement d'origine est sélectionné par défaut.
13. Choisissez de restaurer ou non les permissions de partage associées aux fichiers.
14. Cliquez sur **Démarrer la restauration**.
15. Sélectionnez l'une des options d'écrasement de fichier :

Option	Description
Écraser un fichier existant s'il est plus ancien	Si l'emplacement de destination comporte un fichier de même nom, mais plus ancien que le fichier source, le fichier source est enregistré dans l'emplacement de destination et remplace l'ancienne version.
Écraser les fichiers existants	Tous les fichiers existants dans l'emplacement de destination sont remplacés, quelle que soit la date de leur dernière modification.
Ne pas écraser les fichiers existants	Si l'emplacement de destination comporte un fichier de même nom, aucune modification ne lui est appliquée et le fichier source n'est pas enregistré dans l'emplacement de destination.

16. Cliquez sur **Poursuivre** pour confirmer votre choix.

Notarisation

La notarisation vous permet de prouver qu'un fichier est authentique et inchangé depuis sa sauvegarde. Nous vous recommandons d'activer la notarisation lors de la sauvegarde de vos fichiers juridiques ou tout autre fichier requérant une authentification.

La notarisation est disponible uniquement pour les sauvegardes de fichiers Google Drive et de Drive partagés Google Workspace.

© Acronis International GmbH, 2003-2026

Comment utiliser la notarisation

Pour activer la notarisation de tous les fichiers sélectionnés pour la sauvegarde, activez le commutateur **Notarisation** lors de la création d'un plan de protection.

Lors de la configuration de la restauration, les fichiers notariés seront marqués d'une icône spéciale. Vous pourrez ainsi vérifier l'authenticité du fichier.

Fonctionnement

Lors d'une sauvegarde, l'agent calcule les code de hachage des fichiers sauvegardés, crée un arbre de hachage (basé sur la structure du dossier), enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données blockchain Ethereum pour s'assurer que cette valeur ne change pas.

Lors de la vérification de l'authenticité d'un fichier, l'agent calcule le hachage du fichier, puis le compare avec le hachage stocké dans l'arbre de hachage sauvegardé. Si ces hachages ne correspondent pas, le fichier n'est pas authentique. Sinon, l'authenticité du fichier est garantie par l'arbre de hachage.

Pour vérifier que l'arbre de hachage n'a pas été compromis, l'agent envoie la racine de l'arbre de hachage au service Notary. Le service Notary la compare avec celle stockée dans la base de données blockchain. Si les hachages correspondent, le fichier sélectionné est authentique. Sinon, le logiciel affiche un message indiquant que le fichier n'est pas authentique.

Vérification de l'authenticité d'un fichier grâce à Notary Service

Si la notarisation a été activée lors de la sauvegarde, vous pouvez vérifier l'authenticité d'un fichier sauvegardé.

Pour vérifier l'authenticité d'un fichier

1. Effectuez l'une des actions suivantes :
   - Pour vérifier l'authenticité d'un fichier Google Drive, sélectionnez le fichier tel que décrit dans les étapes 1 à 7 de la section « Restaurer des fichiers Google Drive ».
   - Pour vérifier l'authenticité d'un fichier de Drive partagé Google Workspace, sélectionnez le fichier tel que décrit dans les étapes 1 à 7 de la section « Restaurer des fichiers de Drive partagés ».
2. Assurez-vous que le fichier sélectionné possède l'icône suivante :  . Cela signifie que le fichier est notarié.
3. Effectuez l'une des actions suivantes :
   - Cliquez sur **Vérifier**.
     Le logiciel vérifie l'authenticité du fichier et affiche le résultat.
   - Cliquez sur **Obtenir certificat**.

© Acronis International GmbH, 2003-2026

Un certificat confirmant la notarisation du fichier est ouvert dans une fenêtre de navigateur Web. La fenêtre contient également les instructions qui vous permettent de vérifier l'authenticité d'un fichier manuellement.

Recherche dans les sauvegardes cloud à cloud

Lors de la restauration des données, vous pouvez effectuer une recherche d'éléments spécifiques sauvegardés au lieu de parcourir l'archive de sauvegarde.

Les fonctionnalités de recherche dépendent des éléments suivants :

- Type de recherche : améliorée (indexée) ou type (non indexée)
  La recherche basée sur l'index est plus rapide et offre des options supplémentaires telles que l'affichage des versions des éléments sauvegardés, la recherche dans les noms des pièces jointes et la recherche en texte intégral dans les sauvegardes Gmail.
- Type d'archive : chiffrée ou non chiffrée
  - Dans les sauvegardes non chiffrées, la recherche est toujours disponible. Seule la recherche améliorée (basée sur l'index) est prise en charge.
  - Dans les sauvegardes chiffrées, la recherche améliorée (indexée) est disponible en option.
    Si vous n'activez pas la recherche améliorée, la recherche de base sera disponible pour les sauvegardes des boîtes aux lettres Microsoft 365. Pour toutes les autres ressources, la recherche ne sera pas disponible. Le tableau ci-dessous récapitule les options disponibles pour les sauvegardes chiffrées.

Type de ressource	Quoi restaurer	La recherche améliorée est désactivée	La recherche améliorée est activée
Ressources Microsoft 365			
Boîte de réception	Messages de courriers électroniques	La recherche de base (non basée sur l'index) est disponible	La recherche améliorée (basée sur l'index) est disponible
OneDrive	Fichiers/dossiers	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Site SharePoint	Fichiers SharePoint	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Teams	Canaux	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
	Messages de courriers électroniques	La recherche de base (non basée sur l'index) est disponible	La recherche améliorée (basée sur l'index) est disponible

© Acronis International GmbH, 2003-2026

Type de ressource	Quoi restaurer	La recherche améliorée est désactivée	La recherche améliorée est activée
	Site d'équipe	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Ressources Google Workspace			
Boîte de réception	Messages de courriers électroniques	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Google Drive	Fichiers/dossiers	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible
Lecteurs partagés	Fichiers/dossiers	La recherche n'est pas disponible	La recherche améliorée (basée sur l'index) est disponible

Recherche en texte intégral

La recherche en texte intégral est disponible uniquement pour les sauvegardes Gmail et est activée par défaut. Elle vous permet d'effectuer des recherches dans le corps du texte des e-mails sauvegardés. Si cette option est désactivée, vous ne pouvez effectuer des recherches que par objet, expéditeur, destinataire et date.

Un index de recherche en texte intégral utilise entre 10 et 30 pour cent de l'espace de stockage occupé par la sauvegarde de Gmail. Un index sans données de recherche en texte intégral est nettement plus petit. Pour économiser de l'espace de stockage, vous pouvez désactiver la recherche en texte intégral et effacer la partie de l'index qui contient les données de recherche en texte intégral.

Index de recherche

Les index de recherche permettent d'effectuer des recherches améliorées dans les archives de sauvegarde cloud à cloud.

Les archives sont indexées automatiquement après chaque opération de sauvegarde. Le processus d'indexation n'a aucune incidence sur les performances de sauvegarde, car l'indexation et la sauvegarde sont effectuées par des composants logiciels distincts.

Les résultats de recherche sont disponibles une fois l'opération d'indexation terminée, ce qui peut prendre jusqu'à 24 heures. L'indexation de la première sauvegarde, qui est complète, prend généralement plus de temps que l'indexation des sauvegardes incrémentielles successives.

© Acronis International GmbH, 2003-2026

Tous les index contiennent des métadonnées qui prennent en charge la fonctionnalité de recherche principale : recherche par objet, expéditeur, destinataire ou date. Les index des sauvegardes Gmail contiennent des données supplémentaires si la recherche en texte intégral est activée.

Vérification de la taille d'un index de recherche

La taille des index de recherche augmente avec le temps. Les index des archives de sauvegarde dans lesquelles la recherche en texte intégral est activée peuvent occuper jusqu'à 30 pour cent de la taille de l'archive.

Pour vérifier la taille d'un index de recherche

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Dans l'onglet **Stockage de sauvegarde**, cliquez sur **Sauvegarde d'applications dans le Cloud**.
3. Vérifiez la valeur figurant dans la colonne **Taille de l'index**.

Mise à jour, reconstruction ou suppression des index

Pour résoudre les problèmes liés à la recherche dans les sauvegardes cloud à cloud, vous pouvez mettre à jour, reconstruire ou supprimer les index de recherche.

Remarque
Les opérations avec les Index ne sont pas prises en charge dans les sauvegardes chiffrées.

Ces opérations peuvent être longues et ne sont disponibles que pour les administrateurs, comme suit :

Type de tenant	Rôle	Peut mettre à jour l'index	Peut reconstruire l'index	Peut supprimer l'index
Tenant partenaire	Administrateur d'entreprise	+	+	+
	Administrateur de cyberprotection	+	-	-
	Administrateur de protection	+	-	-
	Administrateur de protection en lecture seule	-	-	-
Tenant client	Administrateur d'entreprise	+	-	-
	Administrateur de protection	+	-	-
	Administrateur de protection en lecture seule	-	-	-

© Acronis International GmbH, 2003-2026

Type de tenant	Rôle	Peut mettre à jour l'index	Peut reconstruire l'index	Peut supprimer l'index
Unité	Administrateur de l'unité	+	-	-
	Administrateur de protection	+	-	-
	Administrateur de protection en lecture seule	-	-	-

Pour mettre à jour, reconstruire ou supprimer un index

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Dans l'onglet **Stockage de sauvegarde**, cliquez sur **Sauvegarde d'applications dans le Cloud**.
3. Sélectionnez l'archive pour laquelle vous souhaitez mettre à jour, reconstruire ou supprimer l'index.
4. Dans le volet **Actions**, sélectionnez l'action à effectuer :
   - **Mettre à jour l'index** : les points de restauration dans l'archive sont vérifiés et les index manquants sont ajoutés.
   - **Reconstruire l'index** : les index de tous les points de restauration de l'archive sont supprimés, puis sont recréés.
   - **Supprimer l'index** : les index de tous les points de restauration de l'archive sont supprimés.
5. Sélectionnez le champ d'application de l'action, puis cliquez sur **OK**.
   En fonction de l'archive et de l'action sélectionnée, une ou plusieurs des options suivantes sont disponibles :
   - **Métadonnées uniquement**
   - **Contenu seulement**
   - **Métadonnées et recherche de contenu**

Activation de la recherche améliorée dans les sauvegardes chiffrées

Vous pouvez activer la recherche améliorée (indexée) dans un nouveau plan de sauvegarde ou dans un plan de sauvegarde existant.

Si vous n'activez pas la recherche améliorée, la recherche de base est disponible pour les sauvegardes des boîtes aux lettres Microsoft 365. Pour toutes les autres ressources, la recherche n'est pas disponible. Pour plus d'informations sur les options disponibles, voir "Recherche dans les sauvegardes cloud à cloud" (p. 941).

Pour activer la recherche améliorée

Dans un nouveau plan de sauvegarde

1. Dans la console Cyber Protect, accédez à **Gestion** > **Sauvegardes d'applications cloud**.
2. Cliquez sur **Création d'un plan**.

© Acronis International GmbH, 2003-2026

3. Activez le commutateur **Chiffrement**, puis spécifiez et confirmez le mot de passe de chiffrement.
4. Sélectionnez l'algorithme de chiffrement.
5. Cochez la case **Autoriser la recherche améliorée dans les sauvegardes chiffrées**.
6. Configurez les autres options du plan de sauvegarde, puis cliquez sur **Terminé**.

Remarque
Vous ne pourrez pas désactiver le chiffrement, modifier le mot de passe de chiffrement ou désactiver la recherche améliorée ultérieurement. Pour créer une sauvegarde non chiffrée, modifier le mot de passe de chiffrement ou créer une sauvegarde dans laquelle la recherche améliorée est désactivée, créez un nouveau plan de sauvegarde.

Dans un plan de sauvegarde existant

1. Dans la console Cyber Protect, accédez à **Gestion** > **Sauvegardes d'applications cloud**.
2. Sélectionnez le plan de sauvegarde dans lequel vous souhaitez activer la recherche améliorée, puis cliquez sur **Modifier**.
3. Cliquez sur l'icône en forme d'engrenage à côté du nom du plan, puis sélectionnez l'onglet **Options de recherche**.
4. Activez le commutateur, puis cliquez sur **Terminé**.
5. Cliquez sur **Enregistrer les paramètres**.

Une opération d'indexation démarrera après la prochaine sauvegarde.

Remarque
Vous ne pourrez pas désactiver la recherche améliorée ultérieurement. Pour créer une sauvegarde dans laquelle la recherche améliorée est désactivée, créez un nouveau plan de sauvegarde.

Désactivation de la recherche en texte intégral pour les sauvegardes Gmail

Vous souhaiterez peut-être désactiver la recherche en texte intégral si la taille de l'index de recherche doit rester à son niveau minimal.

Si vous réactivez ultérieurement la recherche en texte intégral, toutes les archives créées par ce plan de sauvegarde seront réindexées. Cette opération prend un certain temps.

Pour désactiver la recherche en texte intégral

1. Lors de la création ou de la modification d'un plan de sauvegarde, cliquez sur l'icône d'engrenage dans l'angle supérieur droit.
2. Dans l'onglet **Recherche en texte intégral**, désactivez le commutateur.
3. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

4. [Lors de la création d'un plan] Cliquez sur **Appliquer**.
5. [Lors de la modification d'un plan] Cliquez sur **Enregistrer les paramètres**.

Sauvegarde d'Oracle Database

La protection d'Oracle Database est décrite dans un autre document, disponible à l'adresse https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

Protection de SAP HANA

La protection de SAP HANA est décrite dans un document distinct disponible à cette adresse : https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

Protection des données MySQL et MariaDB

Vous pouvez protéger les données MySQL ou MariaDB à l'aide d'une sauvegarde reconnaissant les applications. Elle collecte les métadonnées des applications et permet une restauration granulaire au niveau de l'instance, de la base de données ou de la table.

Pour protéger une machine physique ou virtuelle qui exécute des instances MySQL ou MariaDB avec la sauvegarde reconnaissant les applications, vous devez installer l'agent pour MySQL/MariaDB sur cette machine. L'agent pour MySQL/MariaDB est fourni avec l'agent pour Linux (64 bits) ; par conséquent, il ne peut être installé que sur des systèmes d'exploitation Linux 64 bits. Consultez "Systèmes d'exploitation et environnements pris en charge pour la sauvegarde et la restauration" (p. 513).

Télécharger le fichier d'installation de l'agent pour Linux (64 bits)

1. Connectez-vous à la console Cyber Protect.
2. Cliquez sur l'icône de compte dans l'angle supérieur droit, puis sélectionnez **Téléchargements**.
3. Cliquez sur **Agent pour Linux (64 bits)**.

Le fichier d'installation est téléchargé sur votre ordinateur. Pour installer l'agent, procédez tel que décrit dans les sections "Installation des agents de protection sous Linux" (p. 69) ou "Installation et désinstallation d'agents de protection sous Linux" (p. 92). Veillez à sélectionner Agent pour MySQL/MariaDB, qui est un composant optionnel.

Pour restaurer des bases de données et des tables vers une instance active, l'agent pour MySQL/MariaDB a besoin d'un stockage temporaire pour fonctionner. Par défaut, le répertoire `/tmp` est utilisé. Vous pouvez modifier ce répertoire en configurant la variable d'environnement `ACRONIS_MYSQL_RESTORE_DIR`.

© Acronis International GmbH, 2003-2026

Limites

- Les clusters MySQL ou MariaDB ne sont pas pris en charge.
- Les instances MySQL ou MariaDB exécutées dans des conteneurs Docker ne sont pas prises en charge.
- Les instances MySQL ou MariaDB exécutées sur des systèmes d'exploitation utilisant le système de fichiers BTRFS ne sont pas prises en charge.
- Les bases de données système (`sys`, `mysql`, `information-schema` et `performance_schema`) et les bases de données qui ne contiennent aucune table ne peuvent pas être restaurées sur des instances actives. Toutefois, ces bases de données ne peuvent pas être restaurées en tant que fichiers lors de la restauration de l'instance complète.
- La restauration est prise en charge uniquement vers les instances cibles dont la version est identique à celle de l'instance sauvegardée, avec les restrictions suivantes :
  - La restauration d'instances MySQL 5.x vers des instances MySQL 8.x n'est pas prise en charge.
  - La restauration vers une version MySQL 5.x ultérieure (y compris les versions mineures) est prise en charge uniquement via une restauration de l'instance complète sous forme de fichiers. Avant de tenter une restauration, consultez le guide officiel de mise à niveau MySQL pour la version cible, par exemple, le Guide de mise à niveau MySQL 5.7.
- La restauration de sauvegardes stockées sur Secure Zone n'est pas prise en charge.
- Les bases de données et les tables ne peuvent pas être restaurées par l'agent pour MySQL/MariaDB qui est encore en cours d'exécution sur un ordinateur sur lequel AppArmor est installé. Vous pouvez toujours restaurer une instance sous forme de fichiers, ou bien la machine entière.
- La restauration vers des bases de données cibles configurées avec des liens symboliques n'est pas prise en charge. Vous pouvez restaurer les bases de données sauvegardées en tant que nouvelles bases de données en modifiant leur nom.

Problèmes connus

Si vous rencontrez des problèmes lors de la restauration de données depuis des partages Samba protégés par mot de passe, déconnectez-vous de la console Cyber Protect, puis reconnectez-vous à cette dernière. Sélectionnez le point de restauration désiré, puis cliquez sur **Bases de données MySQL/MariaDB**.Ne cliquez pas sur **Toute la machine** ni sur **Fichiers/dossiers**.

Configuration d'une sauvegarde reconnaissant les applications

Prérequis

- Au moins une instance MySQL ou MariaDB doit être en cours d'exécution sur l'ordinateur sélectionné.
- Sur l'ordinateur sur lequel l'instance MySQL ou MariaDB est en cours d'exécution, l'agent de protection doit être lancé à l'aide de l'utilisateur root (superutilisateur).

© Acronis International GmbH, 2003-2026

- La sauvegarde reconnaissant les applications n'est disponible que lorsque l'option **Toute la machine** est sélectionnée en tant que source de sauvegarde dans le plan de protection.
- L'option de sauvegarde **Secteur par secteur** doit être désactivée dans les options du plan de protection. Dans le cas contraire, la restauration des donnes d'application est impossible.

Configurer une sauvegarde reconnaissant les applications

1. Dans la console Cyber Protect, sélectionnez un ou plusieurs ordinateurs sur lesquels une instance MySQL ou MariaDB est en cours d'exécution.
   Vous pouvez disposer d'une ou plusieurs instances sur le même ordinateur.
2. Créez un plan de protection avec le module de sauvegarde activé.
3. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine**.
4. Cliquez sur **Sauvegarde d'applications**, puis activez l'interrupteur à côté de **MySQL/MariaDB Server**.
5. Sélectionnez comment spécifier les instances MySQL ou MariaDB :
   - **Pour toutes les ressources**
     Choisissez cette option si vous exécutez des instances dont la configuration est identique sur plusieurs serveurs. Les mêmes paramètres et identifiants de connexion seront utilisés pour toutes les instances.
   - **Pour des ressources spécifiques**
     Choisissez cette option pour spécifier les paramètres et identifiants de connexion pour chaque instance.
6. Cliquez sur **Ajouter une instance** pour configurer les paramètres et identifiants de connexion pour chaque instance.
   a. Sélectionnez le type de connexion, puis spécifiez les éléments suivants :
      - [Pour socket TCP] Adresse IP et port.
      - [Pour socket Unix] Chemin d'accès du socket.
   b. Spécifiez les identifiants d'un compte utilisateur possédant les autorisations suivantes pour l'instance :
      - `FLUSH_TABLES` OU `RELOAD` pour toutes les bases de données et tables (`*.*`)
      - `SELECT` pour `information_schema.tables`
   c. Cliquez sur **OK**.
7. Cliquez sur **Terminé**.

Restauration à partir d'une sauvegarde reconnaissant les applications

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des instances, bases de données et tables MySQL ou MariaDB. Vous pouvez aussi restaurer le serveur tout entier sur lequel ces instances sont en cours d'exécution, ou des fichiers et dossiers de ce serveur.

Le tableau ci-dessous résume toutes les options de restauration.

© Acronis International GmbH, 2003-2026

Quoi restaurer	Restaurer en tant que	Récupérer vers
Serveur MySQL Serveur MariaDB	Toute la machine	Machine* sur laquelle l'agent pour Linux est installé
Serveur MySQL Serveur MariaDB	Fichiers ou dossiers	Machine* sur laquelle l'agent pour Linux est installé
Instance	Fichiers	Machine* sur laquelle l'agent pour MySQL/MariaDB est installé
Base de données	La même base de données Nouvelle base de données	Machine* sur laquelle l'agent pour MySQL/MariaDB est installé • Instance d'origine • Une autre instance • Base de données d'origine • Nouvelle base de données
Table	La même table Une nouvelle table	Machine* sur laquelle l'agent pour MySQL/MariaDB est installé • Instance d'origine • Une autre instance • Base de données d'origine • La table d'origine • Une nouvelle table

* Une machine virtuelle contenant un agent est traitée comme une machine physique du point de vue de la sauvegarde.

Restauration du serveur tout entier

Pour apprendre à restaurer l'ensemble du serveur sur lequel s'exécutent des instances MySQL ou MariaDB, voir "Restauration" (p. 664).

Restauration d'instances

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des instances MySQL ou MariaDB sous la forme de fichiers.

Restaurer une instance

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.

© Acronis International GmbH, 2003-2026

3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :

   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner un ordinateur**, sélectionnez un ordinateur en ligne avec agent pour MySQL/MariaDB, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet **Stockage de sauvegarde**.

   La machine choisie pour la navigation avec l'une des actions ci-dessus devient une machine cible pour la restauration.
4. Cliquez sur **Restaurer** > **Bases de données MySQL/MariaDB**.
5. Sélectionnez l'instance à restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
6. Sous **Chemin d'accès**, sélectionnez le répertoire vers lequel les fichiers seront restaurés.
7. Cliquez sur **Démarrer la restauration**.

Restauration de bases de données

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des bases de données vers des instances MySQL ou MariaDB.

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :

   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner un ordinateur**, sélectionnez un ordinateur en ligne avec agent pour MySQL/MariaDB, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet **Stockage de sauvegarde**.

   La machine choisie pour la navigation avec l'une des actions ci-dessus devient une machine cible pour la restauration.
4. Cliquez sur **Restaurer** > **Bases de données MySQL/MariaDB**.
5. Cliquez sur le nom de l'instance désirée pour explorer ses bases de données.
6. Sélectionnez une ou plusieurs bases de données à restaurer.
7. Cliquez sur **Restaurer**.
8. Cliquez sur **Instance MySQL/MariaDB cible** pour spécifier les paramètres et identifiants de connexion pour l'instance cible.

© Acronis International GmbH, 2003-2026

- Vérifiez l'instance sur laquelle vous voulez restaurer les données. Par défaut, l'instance d'origine est sélectionnée.
- Spécifiez les identifiants d'un compte utilisateur capable d'accéder à l'instance cible. Les privilèges suivants doivent être attribués à ce compte utilisateur pour toutes les bases de données et tables (`*.*`) :
  - `INSERT`
  - `CREATE`
  - `DROP`
  - `LOCK_TABLES`
  - `ALTER`
  - `SELECT`
- Cliquez sur **OK**.

9. Vérifiez la base de données cible.

   Par défaut, la base de données d'origine est sélectionnée.

   Pour restaurer une base de données en tant que nouvelle base de données, cliquez sur le nom de la base de données cible et modifiez-le. Cette action n'est disponible que si vous restaurez une seule base de données.
10. Sous **Écraser les bases de données existantes**, sélectionnez le mode d'écrasement.

    Par défaut, l'écrasement est activé et la base de données sauvegardée remplace la base de données cible qui possède le même nom.

    Si l'écrasement est désactivé, la base de données sauvegardée est ignorée lors de l'opération de restauration et ne remplace pas la base de données cible qui possède le même nom.
11. Cliquez sur **Démarrer la restauration**.

Restauration de tables

À partir d'une sauvegarde reconnaissant les applications, vous pouvez restaurer des tables vers des instances MySQL ou MariaDB actives.

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel les données que vous souhaitez restaurer étaient initialement présentes.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :
   - Si la sauvegarde est située sur le Cloud ou à un emplacement de stockage partagé (c.-à-d. que d'autres agents peuvent y accéder), cliquez sur **Sélectionner un ordinateur**, sélectionnez un ordinateur en ligne avec agent pour MySQL/MariaDB, puis choisissez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet **Stockage de sauvegarde**.

© Acronis International GmbH, 2003-2026

La machine choisie pour la navigation avec l'une des actions ci-dessus devient une machine cible pour la restauration.

4. Cliquez sur **Restaurer** > **Bases de données MySQL/MariaDB**.
5. Cliquez sur le nom de l'instance désirée pour explorer ses bases de données.
6. Cliquez sur le nom de la base de données désirée pour explorer ses tables.
7. Sélectionnez une ou plusieurs tables à restaurer.
8. Cliquez sur **Restaurer**.
9. Cliquez sur **Instance MySQL/MariaDB cible** pour spécifier les paramètres et identifiants de connexion pour l'instance cible.
   - Vérifiez l'instance sur laquelle vous voulez restaurer les données. Par défaut, l'instance d'origine est sélectionnée.
   - Spécifiez les identifiants d'un compte utilisateur capable d'accéder à l'instance cible. Les privilèges suivants doivent être attribués à ce compte utilisateur pour toutes les bases de données et tables (`*.*`) :
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Cliquez sur **OK**.
10. Vérifiez la base cible.

    Par défaut, la table d'origine est sélectionnée.

    Pour restaurer une table en tant que nouvelle table, cliquez sur le nom de la table cible et modifiez-le. Cette action n'est disponible que si vous restaurez une seule table.
11. Sous **Écraser les tables existantes**, sélectionnez le mode d'écrasement.

    Par défaut, l'écrasement est activé et la table sauvegardée remplace la table cible qui possède le même nom.

    Si l'écrasement est désactivé, la table sauvegardée est ignorée lors de l'opération de restauration et ne remplace pas la table cible qui possède le même nom.
12. Cliquez sur **Démarrer la restauration**.

Récupération des routines stockées

Lorsque vous récupérez une instance MySQL complète, les routines stockées sont automatiquement restaurées.

Lorsque vous récupérez une base de données individuelle vers une instance non originale ou que vous la récupérez en tant que nouvelle base de données, les routines stockées ne sont pas

© Acronis International GmbH, 2003-2026

automatiquement restaurées. Vous pouvez les restaurer manuellement, en les exportant dans un fichier SQL, puis en les ajoutant à la base de données restaurée.

Pour exporter les routines stockées et les ajouter à une base de données restaurée

1. Sur la machine où se trouve l'instance MySQL d'origine, ouvrez Terminal.
2. Exécutez la commande suivante pour exporter les routines stockées.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data > [exported_db_routines.sql]
   ```
4. Sur la machine où la base de données est restaurée, ouvrez le client MySQL en ligne de commande .
5. Exécutez les commandes suivantes pour ajouter les routines à la base de données restaurée.
   ```
   mysql>  use [recovered_database_name];
   ```
   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```

Protection des machines virtuelles et des conteneurs Proxmox

Vous pouvez effectuer une sauvegarde sans agent des machines virtuelles et des conteneurs Proxmox en installant l'agent pour Proxmox sur l'hôte protégé.

L'agent pour Proxmox est inclus dans l'offre groupée avec l'agent pour Linux (64 bits) et nécessite que l'agent pour Linux soit également installé sur l'hôte. Pour plus d'informations sur la façon de télécharger le fichier d'installation, voir "Téléchargement d'agents de protection" (p. 47).

Les hôtes exécutant Proxmox VE 8.2 ou une version ultérieure sont pris en charge. Dans les environnements en cluster, vous devez installer un agent sur chaque nœud.

Un quota de **Machine virtuelle** est requis par machine virtuelle ou conteneur Proxmox VE. Aucun quota n'est requis pour l'ordinateur sur lequel l'agent pour Proxmox s'exécute.

Les stockages Proxmox suivants sont pris en charge pour la sauvegarde et la restauration :

- Pour les machines virtuelles : Tous les stockages sur lesquels une machine virtuelle peut être créée
- Pour les conteneurs : LWM Thin, Ceph/RBD, BtrFS

Les emplacements de sauvegarde suivants sont disponibles pour les machines virtuelles et les conteneurs Proxmox :

- Le stockage dans le cloud (y compris le stockage hébergé par un partenaire)
- Stockage dans le cloud public

© Acronis International GmbH, 2003-2026
   ```

- Dossiers réseau sur des partages SMB et NFS
- Dossiers locaux

Limitations pour les ressources Proxmox

Les limitations suivantes s'appliquent à la sauvegarde et à la restauration de machines virtuelles et de conteneurs Proxmox.

Général

- Les fonctionnalités suivantes ne sont pas prises en charge :
  - Exécuter en tant que MV
  - Convertir en MV
  - Sauvegarde reconnaissant les applications
  - Réplication de MV
- Vous ne pouvez pas restaurer des disques ou des conteneurs virtuels dans le stockage `CephFS`.
- Les disques pour lesquels l'option de sauvegarde est désactivée dans Proxmox VE ne sont pas sauvegardés.
- Lors d'une restauration, la sélection du type de provisionnement de disque (thin/thick) ne fonctionnera que si le stockage cible prend en charge le type sélectionné. Par exemple, le stockage LVM prend uniquement en charge les disques thick. Si vous sélectionnez l'allocation de disque thin, cette option sera ignorée.

Machines virtuelles

- Les éléments suivants ne sont pas sauvegardés :
  - Modèles de machine virtuelle
  - Disques détachés
  - Images instantanées
  - Contenu de l'état du terminal TPM.

    Lorsque vous restaurez une machine virtuelle en tant que nouvel ordinateur, elle disposera d'un terminal d'état TPM vide. Par exemple, si BitLocker est activé sur un tel ordinateur, vous devez utiliser la clé de restauration BitLocker.
- Au moins un stockage de `Directory` est requis pour les fichiers temporaires.
- La fonction CBT (Changed Block Tracking) n'est pas disponible pour les machines virtuelles éteintes ni pour celles ayant subi un cycle d'alimentation (mise hors tension, puis remise sous tension). L'absence d'informations de la fonction CBT peut entraîner des sauvegardes plus lentes.
- Lors d'une sauvegarde, les machines virtuelles éteintes sont allumées, puis maintenues dans un état gelé qui n'utilise pas de ressources RAM ou processeur sur l'hôte.
- La sauvegarde d'une machine virtuelle verrouillée n'est pas possible. Par exemple, les machines virtuelles en veille prolongée sont verrouillées.

Conteneurs

© Acronis International GmbH, 2003-2026

- Seuls les types de stockage suivants sont pris en charge pour la sauvegarde et la restauration : LWM Thin, Ceph/RBD, BtrFS.
- Les conteneurs pour lesquels les instantanés sont désactivés ne sont pas pris en charge.
- La fonction CBT (Changed Block Tracking) n'est pas disponible.
- La propriété `OS type` n'est pas restaurée.

Installation de l'agent pour Proxmox

L'agent pour Proxmox est inclus dans l'offre groupée avec l'agent pour Linux (64 bits) et nécessite que l'agent pour Linux soit également installé sur l'hôte protégé.

Vous devez installer l'agent pour Proxmox localement, sur l'hôte protégé, en utilisant l'une des options suivantes :

- Interface graphique
  Pour plus d'informations, voir "Installation des agents de protection sous Linux" (p. 69).
- Interface de ligne de commande
  Pour plus d'informations, voir "Installation et désinstallation d'agents de protection sous Linux" (p. 92).

Après avoir installé l'agent sur l'hôte, vous pouvez voir toutes les machines virtuelles et tous les conteneurs disponibles sur cet hôte dans la console Cyber Protect, dans l'onglet **Terminaux** > **Proxmox**.

Sauvegarde des ressources Proxmox

Vous pouvez sauvegarder des machines virtuelles et des conteneurs Proxmox.

Pour sauvegarder une ressource, créez un plan de protection. Pour plus d'informations, voir "Création d'un plan de protection" (p. 244).

Dans les plans de protection pour les ressources Proxmox, seul le module **Sauvegarde** est disponible.

Vous pouvez également sauvegarder l'hôte Proxmox séparément, en tant que serveur Linux. Pour éviter les sauvegardes doubles, vous pouvez configurer des filtres de fichiers dans le plan de protection de l'hôte et exclure les répertoires qui contiennent les données de la machine virtuelle.

Restaurer des ressources Proxmox

Vous pouvez restaurer une machine virtuelle Proxmox sauvegardée en tant que :

- Une machine physique.
- La machine virtuelle d'origine ou une nouvelle machine virtuelle sur le même hyperviseur.
- Un nouvel ordinateur sur un autre hyperviseur. Voir "Restauration interplate-forme" (p. 667).

© Acronis International GmbH, 2003-2026

Pour plus d'informations sur la restauration d'une machine virtuelle, voir "Restauration d'une machine virtuelle en tant que machine physique" (p. 690) et "Restauration d'une machine virtuelle en tant que machine virtuelle" (p. 691).

Vous pouvez restaurer un conteneur Proxmox sauvegardé en tant que :

- Le conteneur d'origine.
- Un nouveau conteneur Proxmox. La restauration multiplate-forme n'est pas prise en charge.

Pour plus d'informations sur la restauration d'un conteneur, consultez "Restauration de conteneurs" (p. 702).

Vous pouvez restaurer des fichiers à partir de machines virtuelles et de conteneurs Proxmox sauvegardés vers l'hôte Proxmox ou le stockage en réseau qui lui est associé. Vous ne pouvez pas effectuer de restauration au niveau des fichiers vers une machine virtuelle ou un conteneur.

Protéger les serveurs d'hébergement Web

Vous pouvez protéger les serveurs d'hébergement Web Linux qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager. Les serveurs qui exécutent des panneaux de configuration d'hébergement Web d'autres fournisseurs sont protégés comme des ressources classiques.

Quotas

Les serveurs qui exécutent des panneaux de configuration cPanel, Plesk, DirectAdmin, VirtualMin ou ISPManager sont considérés comme des serveurs d'hébergement Web. Chaque serveur d'hébergement Web sauvegardé consomme le quota des **serveurs d'hébergement Web**. Si ce quota est désactivé ou si la surconsommation pour ce quota est dépassée, un quota sera attribué comme suit ou la sauvegarde échouera :

- Si le serveur est physique, le quota des **serveurs** sera utilisé. Si ce quota est désactivé ou dépassé, la sauvegarde échouera.
- Si le serveur est virtuel, le quota des **machines virtuelles** sera utilisé. Si ce quota est désactivé ou dépassé, la sauvegarde échouera.

Intégration de DirectAdmin, de cPanel et de Plesk

Les administrateurs d'hébergement Web qui utilisent DirectAdmin, Plesk ou cPanel peuvent intégrer ces panneaux de configuration au service Cyber Protection afin d'accéder à différentes fonctionnalités très utiles :

- Sauvegarde de l'intégralité d'un serveur d'hébergement Web dans le stockage dans le cloud, avec sauvegarde de disque
- Restauration de l'intégralité d'un serveur, y compris tous les comptes et sites Web

© Acronis International GmbH, 2003-2026

- Exécution d'une restauration granulaire et téléchargement de comptes, de sites Web, de fichiers, de boîtes aux lettres ou de bases de données
- Activation de revendeurs et de clients pour qu'ils exécutent la restauration en libre-service de leurs propres données

Pour exécuter l'intégration, vous devez utiliser une extension de service Cyber Protection. Pour plus d'informations, reportez-vous aux guides d'intégration correspondants :

- Guide d'intégration de DirectAdmin
- Guide d'intégration de WHM et cPanel
- Guide d'intégration de Plesk

Opérations spéciales avec les machines virtuelles

Exécution d'une machine virtuelle à partir d'une sauvegarde (restauration instantanée)

Vous pouvez exécuter une machine virtuelle depuis une sauvegarde de niveau disque contenant un système d'exploitation. Cette opération, aussi appelée restauration instantanée, vous permet de lancer un serveur virtuel en quelques secondes. Les disques virtuels sont émulés directement depuis la sauvegarde et n'utilisent pas d'espace dans le magasin de données (stockage). Seule la conservation des modifications des disques virtuels nécessite de l'espace de stockage.

Nous vous recommandons de laisser cette machine virtuelle temporaire fonctionner pendant un maximum de trois jours. Vous pourrez alors la supprimer entièrement ou la convertir en machine virtuelle standard (finalisation) sans temps d'arrêt du système.

Tant que la machine virtuelle temporaire existe, les règles de rétention ne peuvent être appliquées à la sauvegarde utilisée par celle-ci. L'exécution des sauvegardes de la machine d'origine se poursuit.

Exemples d'utilisation

- **Reprise d'activité après sinistre**
  Mettez instantanément en ligne une copie d'une machine qui a planté.
- **Test d'une sauvegarde**
  Exécutez la machine depuis la sauvegarde et assurez-vous que le SE invité et les applications fonctionnent correctement.
- **Accès aux données d'application**
  Tant que la machine est en cours d'exécution, utilisez les outils de gestion natifs de l'application pour accéder aux données nécessaires et les extraire.

© Acronis International GmbH, 2003-2026

Prérequis

- Au moins un agent pour VMware ou Hyper-V doit être enregistré dans le service Cyber Protection.
- La sauvegarde peut être stockée dans un dossier réseau ou local de la machine sur laquelle l'agent pour VMware ou Hyper-V est installé. Si vous sélectionnez un dossier réseau, il doit être accessible depuis cette machine. Il est possible d'exécuter une machine virtuelle à partir d'une sauvegarde stockée sur le Cloud, mais celle-ci sera plus lente, car l'opération nécessite d'importantes lectures en accès aléatoire à partir de la sauvegarde.
- La sauvegarde doit contenir une machine entière ou l'ensemble des volumes requis pour le démarrage du système d'exploitation.
- Des sauvegardes de machines à la fois physiques et virtuelles peuvent être utilisées. Les sauvegardes de *conteneurs* Virtuozzo ne peuvent pas être utilisées.
- Les sauvegardes qui contiennent des volumes logiques Linux (LVM) doivent être créées par l'agent pour VMware ou l'agent pour Hyper-V. La machine virtuelle doit être du même type que la machine d'origine (ESXi ou Hyper-V).

Exécution de la machine

1. Effectuez l'une des actions suivantes :
   - Sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez un point de restauration.
   - Sélectionnez un point de restauration dans l'onglet Stockage de sauvegarde.
2. Cliquez sur **Exécuter en tant que MV**.
   Le logiciel sélectionne automatiquement l'hôte et les autres paramètres requis.
3. [Facultatif] Cliquez sur **Machine cible**, puis modifiez le type de machine virtuelle (ESXi ou Hyper-V), l'hôte ou le nom de machine virtuelle.
4. [Facultatif] Cliquez sur **Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V, puis sélectionnez le magasin de données pour la machine virtuelle.
   Les modifications des disques virtuels s'accumulent tant que la machine est en cours d'exécution. Assurez-vous que le magasin de données sélectionné dispose d'un espace libre suffisant. Si vous prévoyez de conserver ces modifications en rendant la machine virtuelle permanente, sélectionnez un magasin de données adapté à la machine en production.
5. [Facultatif] Cliquez sur **Paramètres de MV** pour modifier la taille de la mémoire et les connexions réseau de la machine virtuelle.
6. [Facultatif] Sélectionnez l'état d'alimentation de la MV (**Marche**/**Arrêt**).
7. Cliquez sur **Exécuter maintenant**.

La machine apparaît alors dans l'interface Web avec une des icônes suivantes :  ou 

.
Ces machines virtuelles ne peuvent pas être sélectionnées pour la sauvegarde.

© Acronis International GmbH, 2003-2026

Remarque
Vous pouvez exécuter l'opération Exécuter en tant que machine virtuelle (restauration instantanée) avec des sauvegardes dans Microsoft Azure. Toutefois, cette opération engendre un trafic considérable pour le transfert de données vers des emplacements externes qui sera ajouté à votre facture d'abonnement Microsoft Azure. En général, le trafic pour le transfert de données vers des emplacements externes d'un ordinateur Windows s'exécutant à partir d'une sauvegarde Microsoft Azure est d'environ 5 Go, depuis le démarrage de la machine virtuelle jusqu'à la connexion.

Suppression de la machine

Nous vous recommandons de ne pas supprimer une machine virtuelle temporaire directement dans vSphere/Hyper-V, car cela peut créer des artefacts dans l'interface Web. De plus, la sauvegarde depuis laquelle s'exécutait la machine peut rester verrouillée pendant un certain temps (elle ne peut pas être supprimée par les règles de rétention).

Suppression d'une machine virtuelle s'exécutant depuis une sauvegarde

1. Dans l'onglet **Tous les terminaux**, sélectionnez une machine virtuelle s'exécutant depuis une sauvegarde.
2. Cliquez sur **Supprimer**.

La machine est supprimée de l'interface Web. Elle est également supprimée du magasin de données (stockage) et de l'inventaire vSphere ou Hyper-V. Toutes les modifications des données pendant l'exécution de la machine sont perdues.

Finalisation de la machine

Tant qu'une machine virtuelle s'exécute depuis une sauvegarde, le contenu des disques virtuels est obtenu directement de cette sauvegarde. De ce fait, la machine devient inaccessible, voire endommagée, si la connexion avec l'emplacement de sauvegarde ou l'agent de protection est perdue.

Vous pouvez rendre cette machine permanente, c'est-à-dire restaurer l'ensemble de tous les disques virtuels, y compris les modifications effectuées lors de l'exécution de la machine, dans le magasin de données stockant ces modifications. Ce processus s'appelle la finalisation.

La finalisation s'effectue sans indisponibilité du système. La machine virtuelle n'est *pas* mise hors tension lors de la finalisation.

L'emplacement des disques virtuels finaux est défini dans les paramètres de l'opération **Exécuter en tant que MV** (**Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V). Avant de commencer la finalisation, assurez-vous que l'espace disponible, les capacités de partage et les performances de ce magasin de données sont adaptés à l'exécution de la machine en production.

© Acronis International GmbH, 2003-2026

Remarque
La finalisation n'est pas prise en charge pour l'Hyper-V qui s'exécute sous Windows Server 2008/2008 R2 et Microsoft Hyper-V Server 2008/2008 R2, car l'API nécessaire manque dans ces versions d'Hyper-V.

Finalisation d'une machine virtuelle s'exécutant depuis une sauvegarde

1. Dans l'onglet **Tous les terminaux**, sélectionnez une machine virtuelle s'exécutant depuis une sauvegarde.
2. Cliquez sur **Finaliser**.
3. [Facultatif] Indiquez un nouveau nom pour la machine.
4. [Facultatif] Modifiez le mode d'allocation du disque. Le paramètre par défaut est **Dynamique**.
5. Cliquez sur **Finaliser**.

Le nom de la machine est immédiatement modifié. La progression de la restauration sont affichées dans l'onglet **Activités**. Une fois la restauration terminée, l'icône de la machine devient celle d'une machine virtuelle standard.

Ce que vous devez savoir à propos de la finalisation

Finalisation vs. restauration normale

Le processus de finalisation est plus lent qu'une restauration normale pour les raisons suivantes :

- Lors d'une finalisation, l'agent accède aléatoirement aux différentes parties de la sauvegarde. Lorsqu'une machine entière est restaurée, l'agent lit de manière séquentielle les données de la sauvegarde.
- Si la machine virtuelle est exécutée pendant la finalisation, l'agent lit les données de la sauvegarde plus souvent, afin de maintenir les deux processus simultanément. Lors d'une restauration normale, la machine virtuelle est arrêtée.

Finalisation des machines exécutées depuis des sauvegardes Cloud

En raison de l'accès intensif aux données sauvegardées, la vitesse de finalisation dépend fortement de la bande passante de connexion entre l'emplacement de la sauvegarde et l'agent. La finalisation sera plus lente pour les sauvegardes situées dans le Cloud que pour les sauvegardes locales. Si la connexion Internet est très lente ou instable, la finalisation d'une machine exécutée depuis une sauvegarde Cloud peut échouer. Nous vous recommandons d'exécuter des machines virtuelles à partir de sauvegardes locales si vous prévoyez d'effectuer la finalisation et que vous avez le choix.

© Acronis International GmbH, 2003-2026

Remarque
La vitesse de finalisation varie selon que l'agent est connecté à un hôte VMware ESXi ou à vCenter, comme le décrit l'étape 3 de "Configuration de l'appliance virtuelle" (p. 139). La connexion à un VMware vCenter peut ralentir la finalisation en raison des spécificités des API VMware. Pour accélérer la finalisation, utilisez un agent pour VMware distinct pour l'opération **Exécuter en tant que MV** qui est suivie de la finalisation et dans laquelle cet agent est connecté à un hôte ESXi au lieu d'un vCenter.

Fonctionnement dans VMware vSphere

Cette section décrit les opérations spécifiques aux environnements VMware vSphere.

Réplication de machines virtuelles

La réplication est uniquement disponible pour les machines virtuelles VMware ESXi.

La réplication est un processus visant à créer une copie exacte (réplica) d'une machine virtuelle, puis à conserver la synchronisation du réplica avec la machine d'origine. En répliquant une machine virtuelle critique, vous disposerez toujours d'une copie de cette machine et qui sera toujours prête à démarrer.

La réplication peut être démarrée manuellement ou selon la planification que vous définissez. La première réplication est complète (elle copie la machine en entier). Toutes les réplications subséquentes sont incrémentielles et effectuées avec Suivi des blocs modifiés, sauf si cette option est désactivée.

Réplication vs. sauvegarde

Contrairement aux sauvegardes planifiées, un réplica conserve l'état le plus récent de la machine virtuelle. Un réplica consomme de l'espace au sein du magasin de données, tandis que les sauvegardes peuvent être conservées dans un espace de stockage plus abordable.

Toutefois, recourir à un réplica est beaucoup plus rapide qu'une restauration et que l'exécution d'une machine virtuelle depuis une sauvegarde. Lorsqu'il est utilisé, un réplica travaille plus rapidement qu'une machine virtuelle exécutée depuis une sauvegarde et ne charge pas l'agent pour VMware.

Exemples d'utilisation

- **Répliquer des machines virtuelles sur un site distant.**
  La réplication vous permet de faire face aux défaillances des centres de données partielles ou complètes, en clonant les machines virtuelles depuis un site secondaire. Le site secondaire se trouve habituellement dans emplacement à distance qui est susceptible d'être affecté par l'environnement, l'infrastructure ou d'autres facteurs qui pourraient provoquer la défaillance du premier site.

© Acronis International GmbH, 2003-2026

- **Répliquer des machines virtuelles au sein d'un site unique (depuis un hôte/magasin de données vers un autre).**
  La réplication sur site peut être utilisée pour des scénarios de reprise d'activité après sinistre et de haute disponibilité.

Ce qu'un réplica vous permet de faire

- **Tester un réplica**
  Le réplica sera mis sur tension pour le test. Utilisez vSphere Client ou d'autres outils pour vérifier si le réplica fonctionne correctement. La réplication est suspendue pendant que le test est en cours.
- **Basculement sur un réplica**
  Le basculement est une transition de la ressource depuis la machine virtuelle d'origine vers le réplica. La réplication est suspendue pendant que le basculement est en cours.
- **Sauvegarder le réplica**
  La sauvegarde et la réplication requièrent l'accès aux disques virtuels, ce qui a une incidence sur les performances de l'hôte sur lequel la machine virtuelle s'exécute. Si vous souhaitez à la fois un réplica et des sauvegardes pour une machine virtuelle, mais que vous ne souhaitez pas ajouter de charge sur l'hôte de production, répliquez la machine sur un hôte différent et configurez des sauvegardes du réplica.

Limites

- Les types de machines virtuelles suivants ne peuvent pas être répliqués :
  - Machines insensibles aux défaillances s'exécutant sur ESXi 5.5 et versions ultérieures
  - Machines s'exécutant à partir de sauvegardes
  - Réplicas de machines virtuelles
- Certaines modifications matérielles, telles que l'ajout d'une carte d'interface réseau (NIC) à l'hôte ESXi ou la suppression d'une NIC, entraînent une modification des identifiants internes de l'hôte. Ce changement affecte les plans de réplication des VM. Après une telle modification, vous devez recréer les plans de réplication de VM dans lesquels l'hôte ESXi est sélectionné comme source ou cible. Sinon, les plans de réplication de VM échoueront.

Création d'un plan de réplication

Un plan de réplication doit être créé individuellement pour chaque machine. Il est impossible d'appliquer un plan existant à d'autres machines.

Pour créer un plan de réplication

1. Sélectionnez une machine virtuelle à répliquer.
2. Cliquez sur **Réplication**.
   Le logiciel affiche un nouveau modèle de plan de réplication.
3. [Facultatif] Pour modifier le nom du plan de réplication, cliquez sur le nom par défaut.

© Acronis International GmbH, 2003-2026

4. Cliquez sur **Machine cible**, puis suivez les instructions suivantes :
   a. Choisissez de créer un nouveau réplica ou d'utiliser un réplica existant sur la machine d'origine.
   b. Sélectionnez l'hôte ESXi et spécifiez le nouveau nom du réplica ou sélectionnez un réplica existant.
      Le nom par défaut d'un nouveau réplica est **[Nom d'origine de la machine]_réplica**.
   c. Cliquez sur **OK**.
5. [Uniquement en cas de réplication sur une nouvelle machine] Cliquez sur **Magasin de données**, puis sélectionnez le magasin de données pour la machine virtuelle.
6. [Facultatif] Cliquez sur **Planification** pour modifier la planification de réplication.
   Par défaut, la réplication s'effectue de manière quotidienne, du lundi au vendredi. Vous pouvez sélectionner l'heure de démarrage de la réplication.
   Si vous souhaitez modifier la fréquence des réplications, faites glisser le curseur, puis indiquez la planification.
   Vous pouvez également procéder comme suit :
   - Définir une période au cours de laquelle la planification sera effective. Cochez la case **Exécuter le plan dans une plage de dates**, puis indiquez la plage de dates.
   - Désactiver la planification. Dans ce cas, la réplication peut commencer manuellement.
7. [Facultatif] Cliquez sur l'icône en forme d'engrenage pour modifier les options de réplication.
8. Cliquez sur **Appliquer**.
9. [Facultatif] Pour exécuter le plan manuellement, cliquez sur **Exécuter maintenant** dans le volet du plan.

À la suite de l'exécution d'un plan de réplication, le réplica de la machine virtuelle apparaît dans la liste **Tous les terminaux** avec l'icône suivante : 

Test d'un réplica

Pour préparer un réplica à des fins de test

1. Sélectionnez un réplica à tester.
2. Cliquez sur **Tester un réplica**.
3. Cliquez sur **Démarrer le test**.
4. Sélectionnez si le réplica sous tension doit être connecté à un réseau. Par défaut, le réplica ne sera pas connecté à un réseau.
5. [Facultatif] Si vous choisissez de connecter le réplica au réseau, cochez la case **Arrêter la machine virtuelle d'origine** pour arrêter la machine d'origine avant de mettre le réplica sous tension.
6. Cliquez sur **Démarrer**.

Pour arrêter le test d'un réplica

© Acronis International GmbH, 2003-2026

1. Sélectionnez un réplica en cours de test.
2. Cliquez sur **Tester un réplica**.
3. Cliquez sur **Arrêter le test**.
4. Confirmez votre choix.

Basculement sur un réplica

Pour basculer une machine sur un réplica

1. Sélectionnez un réplica sur lequel basculer.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Basculement**.
4. Sélectionnez si le réplica sous tension doit être connecté à un réseau. Par défaut, le réplica sera connecté au même réseau que la machine d'origine.
5. [Facultatif] Si vous choisissez de connecter le réplica au réseau, décochez la case **Arrêter la machine virtuelle** pour conserver la machine d'origine en ligne.
6. Cliquez sur **Démarrer**.

Lorsque le réplica est en état de basculement, vous pouvez choisir une des options suivantes :

- **Arrêter le basculement**
  Arrêtez le basculement si la machine d'origine a été réparée. Le réplica sera mis hors tension. La réplication sera reprise.
- **Effectuer un basculement permanent sur le réplica**
  Cette opération instantanée supprime la marque « réplica » de la machine virtuelle, et la réplication n'est alors plus possible. Si vous souhaitez reprendre la réplication, modifiez le plan de réplication pour sélectionner cette machine en tant que source.
- **Restauration automatique**
  Effectuez une restauration automatique si vous avez basculé sur le site qui n'est pas destiné aux opérations continues. Le réplica sera restauré sur la machine d'origine ou sur une nouvelle machine virtuelle. Une fois la restauration effectuée sur la machine d'origine, celle-ci est mise sous tension et la réplication reprend. Si vous choisissez de restaurer sur une nouvelle machine, modifiez le plan de réplication pour sélectionner cette machine en tant que source.

Arrêt du basculement

Pour arrêter le basculement

1. Sélectionnez un réplica en état de basculement.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Arrêter le basculement**.
4. Confirmez votre choix.

© Acronis International GmbH, 2003-2026

Effectuer un basculement permanent

Pour effectuer un basculement permanent

1. Sélectionnez un réplica en état de basculement.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Basculement permanent**.
4. [Facultatif] Modifiez le nom de la machine virtuelle.
5. [Facultatif] Cochez la case **Arrêter la machine virtuelle d'origine**.
6. Cliquez sur **Démarrer**.

Restauration automatique

Pour restaurer automatiquement depuis un réplica

1. Sélectionnez un réplica en état de basculement.
2. Cliquez sur **Actions de réplica**.
3. Cliquez sur **Restauration automatique depuis un réplica**.
   Le logiciel sélectionne automatiquement la machine d'origine comme machine cible.
4. [Facultatif] Cliquez sur **Machine cible**, puis suivez les instructions suivantes :
   a. Sélectionnez si vous souhaitez restaurer automatiquement sur une machine nouvelle ou existante.
   b. Sélectionnez l'hôte ESXi et spécifiez le nouveau nom de machine ou sélectionnez une machine existante.
   c. Cliquez sur **OK**.
5. [Facultatif] Lors de la restauration automatique sur une nouvelle machine, vous pouvez également procéder comme suit :
   - Cliquez sur **Magasin de données** pour sélectionner le magasin de données pour la machine virtuelle.
   - Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.
6. [Facultatif] Cliquez sur **Options de restauration** pour modifier les options de restauration automatique.
7. Cliquez sur **Démarrer la restauration**.
8. Confirmez votre choix.

Options de réplication

Pour modifier les options de réplication, cliquez sur l'icône en forme d'engrenage située à côté du nom du plan de réplication, puis cliquez sur **Options de réplication**.

© Acronis International GmbH, 2003-2026

Suivi des blocs modifiés (CBT)

Cette option est identique à l'option de sauvegarde « Suivi des blocs modifiés (CBT) ».

Provisionnement du disque

Cette option définit les paramètres de provisionnement du disque pour le réplica.

Le préréglage est le suivant : **Allocation dynamique**.

Les valeurs suivantes sont disponibles : **Thin provisioning**, **Thick provisioning**, **Conserver les paramètres d'origine**.

Gestion erreurs

Cette option est identique à l'option de sauvegarde « Gestion des erreurs ».

Commandes Pré/Post

Cette option est identique à l'option de sauvegarde « Commandes Pré/Post ».

Service de cliché instantané des volumes (VSS) pour les machines virtuelles

Cette option est identique à l'option de sauvegarde « Service de cliché instantané des volumes (VSS) pour les machines virtuelles ».

Options de restauration automatique

Pour modifier les options de restauration automatique, cliquez sur **Options de restauration** lors de la configuration de la restauration automatique.

Gestion erreurs

Cette option est identique à l'option de restauration « Gestion des erreurs ».

Performance

Cette option est identique à l'option de restauration « Performance ».

Commandes Pré/Post

Cette option est identique à l'option de restauration « Commandes Pré/Post ».

Gestion de l'alimentation des MV

Cette option est identique à l'option de restauration « Gestion de l'alimentation des MV ».

Amorçage d'un réplica initial

Pour accélérer la réplication vers un emplacement distant et économiser de la bande passante réseau, vous pouvez effectuer un amorçage du réplica.

© Acronis International GmbH, 2003-2026

Important
Pour réaliser l'amorçage d'un réplica, l'agent pour VMware (appliance virtuelle) doit être exécuté sur l'ESXi cible.

Pour réaliser l'amorçage initial d'un réplica

1. Effectuez l'une des actions suivantes :
   - si la machine virtuelle d'origine peut être mise hors tension, éteignez-la, puis passez à l'étape 4.
   - Si la machine virtuelle d'origine ne peut pas être mise hors tension, passez à l'étape suivante.
2. Créez un plan de réplication.
   Lorsque vous créez le plan, sous **Machine cible**, sélectionnez **Nouveau réplica** et l'ESXi qui héberge la machine d'origine.
3. Exécutez une fois le plan.
   Un réplica est créé sur l'ESXi d'origine.
4. Exportez les fichiers de la machine virtuelle (ou du réplica) sur un disque dur externe.
   a. Connectez le disque dur externe à la machine exécutant vSphere Client.
   b. Connectez vSphere Client au vCenter/ESXi d'origine.
   c. Sélectionnez le réplica nouvellement créé dans l'inventaire.
   d. Cliquez sur **Fichier** > **Exporter** > **Exporter le modèle OVF**.
   e. Dans **Répertoire**, spécifiez le dossier sur le disque dur externe.
   f. Cliquez sur **OK**.
5. Transférez le disque dur à l'emplacement distant.
6. Importez le réplica sur l'ESXi cible.
   a. Connectez le disque dur externe à la machine exécutant vSphere Client.
   b. Connectez vSphere Client au vCenter/ESXi cible.
   c. Cliquez sur **Fichier** > **Déployer le modèle OVF**.
   d. Dans **Déployer à partir d'un fichier ou d'une URL**, spécifiez le modèle que vous avez exporté lors de l'étape 4.
   e. Terminez la procédure d'importation.
7. Modifiez le plan de réplication que vous avez créé dans l'étape 2. Sous **Machine cible**, sélectionnez **Réplica existant**, puis sélectionnez le réplica importé.

En conséquence, le logiciel continuera à mettre à jour le réplica. Toutes les réplications seront incrémentielles.

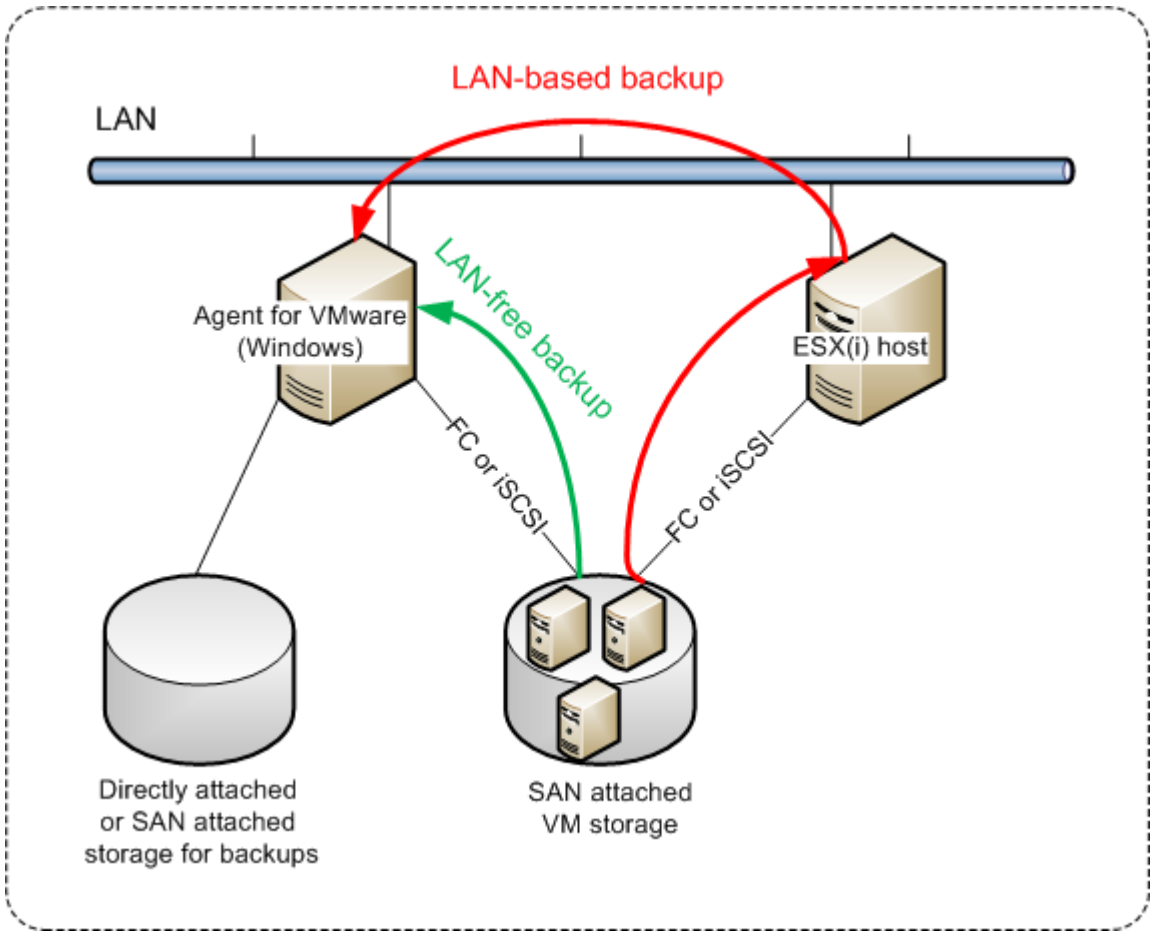
Agent pour VMware - Sauvegarde sans réseau local

Si votre ESXi utilise un stockage SAN, installez l'agent sur une machine connectée au même SAN. L'agent sauvegardera les machines virtuelles directement à partir du stockage plutôt que via l'hôte

© Acronis International GmbH, 2003-2026

ESXi et le réseau local. Cette fonctionnalité s'appelle une sauvegarde sans réseau local.

Le diagramme ci-dessous montre une sauvegarde basée sur un réseau local et une sauvegarde sans réseau local. L'accès aux machines virtuelles sans utiliser le réseau local est possible si vous utilisez fibre channel (FC) ou un réseau de zone de stockage iSCSI. Pour éliminer complètement le transfert des données sauvegardées via le LAN, stockez les sauvegardes sur un disque local de la machine de l'agent ou sur un stockage connecté au SAN.



Pour activer l'agent de sorte qu'il puisse accéder directement à un magasin de données

1. Installez l'agent pour VMware sur une machine Windows possédant un accès réseau au vCenter Server.
2. Connectez à la machine le numéro d'unité logique (LUN) qui héberge le magasin de données. Considérez ce qui suit :
   - Utilisez le même protocole (par ex. iSCSI ou FC) que celui utilisé pour connecter le magasin de données au système ESXi.
   - Le LUN *ne doit pas* être initialisé et doit apparaître comme disque « hors ligne » sous **Gestion de disque**. Si Windows initialise le LUN, celui-ci risque d'être corrompu et illisible par VMware vSphere.

© Acronis International GmbH, 2003-2026

Par conséquent, l'agent utilisera le mode de transport SAN pour accéder aux disques virtuels, c'est-à-dire qu'il lira les secteurs LUN bruts via iSCSI/FC sans reconnaître le système de fichiers VMFS (dont Windows n'a pas connaissance).

Limites

- Dans vSphere 6.0 et versions ultérieures, l'agent ne peut pas utiliser le mode de transport SAN si certains des disques VM se trouvent sur un volume VVol (VMware Virtual Volume) et d'autres non. La sauvegarde de telles machines virtuelles échouera.
- Les machines virtuelles chiffrées, introduites dans VMware vSphere 6.5, sont sauvegardées via LAN, même si vous configurez le mode de transport SAN pour l'agent. L'agent revient au transport NBD, car VMware ne prend pas en charge le transport SAN pour la sauvegarde de disques virtuels chiffrés.

Exemple

Si vous utilisez un réseau de zone de stockage (SAN) iSCSI, configurez l'initiateur iSCSI sur la machine Windows où l'agent pour VMware est installé.

Pour configurer la stratégie SAN

1. Connectez-vous en tant qu'administrateur, ouvrez l'invite de commande, saisissez `diskpart`, puis appuyez sur **Entrée**.
2. Saisissez `san`, puis appuyez sur **Entrée**. Assurez-vous que **Stratégie SAN : Tout hors ligne** s'affiche.
3. Si une autre valeur est définie pour la stratégie SAN :
   a. Saisissez `san policy=offlineall`.
   b. Appuyez sur **Entrée**.
   c. Pour vérifier si le paramètre a bien été appliqué, exécutez l'étape 2.
   d. Redémarrez la machine.

Pour configurer un initiateur iSCSI

1. Accédez à **Panneau de configuration** > **Outils administratifs** > **Initiateur iSCSI**.

   Remarque
   Pour trouvez l'applet **Outils administratifs**, vous devrez peut-être définir l'affichage du **panneau de configuration** sur autre chose que **Accueil** ou **Catégorie**, ou utiliser la fonction de recherche.

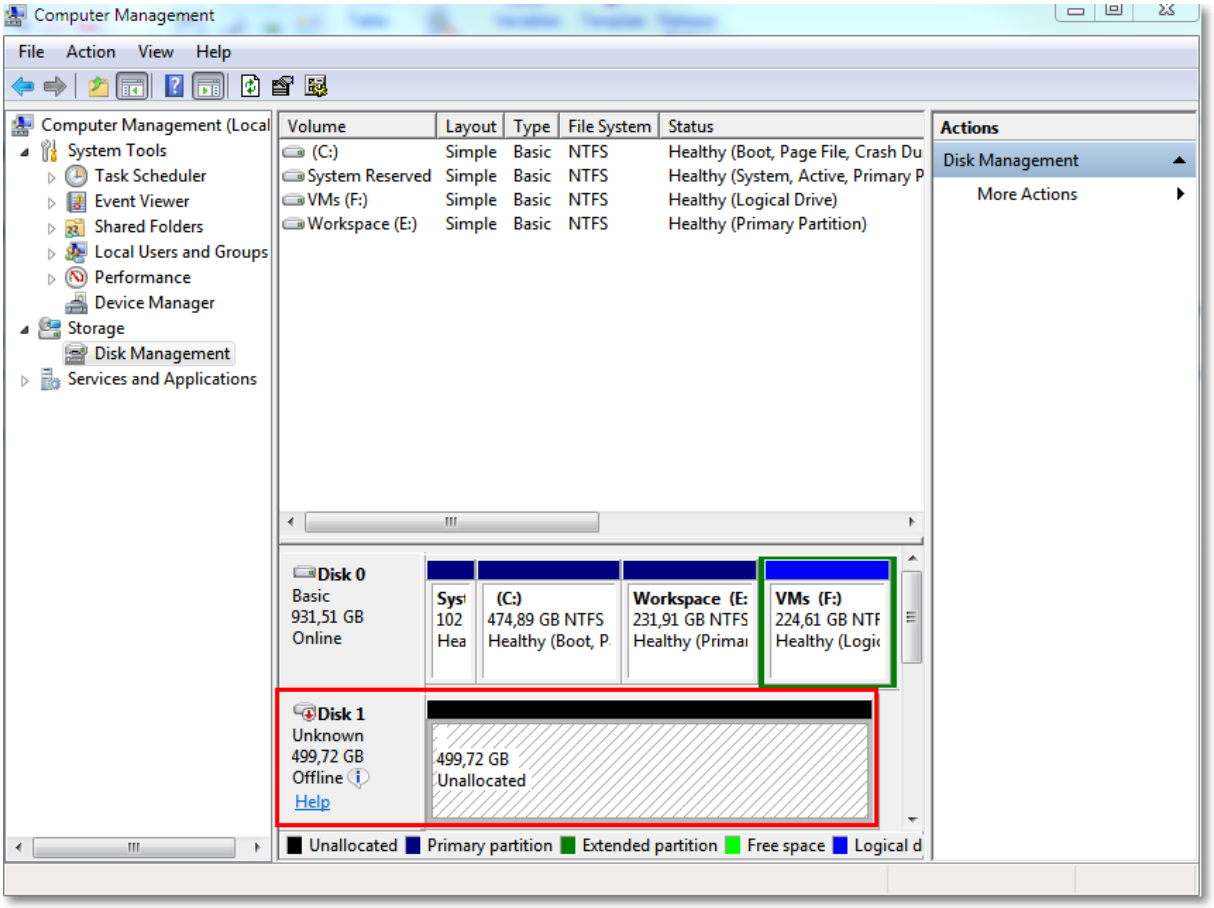
2. Si c'est la première fois que vous lancez l'initiateur Microsoft iSCSI, confirmez votre choix.
3. Sous l'onglet **Cibles**, entrez le nom de domaine complet (FQDN) ou l'adresse IP du périphérique SAN cible, puis cliquez sur **Connexion rapide**.
4. Sélectionnez le LUN qui héberge le magasin de données, puis cliquez sur **Connexion**.

© Acronis International GmbH, 2003-2026

Si le LUN ne s'affiche pas, assurez-vous que la zone de la cible iSCSI permet bien à la machine exécutant l'agent d'accéder au LUN. La machine doit être ajoutée à la liste d'initiateurs iSCSI autorisés sur cette cible.

5. Cliquez sur **OK**.

Le LUN du SAN prêt doit apparaître sous **Gestion de disque**, comme illustré dans la capture d'écran ci-dessous.



Utilisation d'un stockage localement connecté

Avec l'agent pour VMware (appliance virtuelle) ou l'agent pour Scale Computing HC3, vous pouvez utiliser le stockage localement connecté pour éliminer le trafic réseau entre l'agent de protection et l'emplacement de sauvegarde.

© Acronis International GmbH, 2003-2026

Important
Le stockage localement attaché (LAS) est conçu pour les petits environnements avec un seul agent de protection (appliance virtuelle). L'utilisation de plusieurs agents de protection avec un stockage localement attaché dans le même environnement peut entraîner des sauvegardes en double, car les machines virtuelles sont réparties aléatoirement entre les agents, et chaque agent utilise son propre stockage localement attaché.

Dans les environnements VMware, vous pouvez utiliser plusieurs appliances virtuelles si vous liez manuellement chaque appliance virtuelle à toutes les machines virtuelles que cette appliance sauvegardera. Pour plus d'informations, voir "Liaison de machine virtuelle" (p. 972).

Remarque
La taille de disque recommandée pour le stockage localement attaché est jusqu'à 5 To. Des disques plus grands peuvent également fonctionner, mais ces configurations ne sont pas testées. Vous pouvez attacher des disques plus grands à vos propres risques.

Si vous devez sauvegarder plus de 5 To de données, nous vous recommandons d'utiliser un autre type de stockage. Par exemple, vous pouvez attacher un disque virtuel à une machine virtuelle dans l'environnement, puis créer un partage réseau sur ce disque. Vous pouvez ensuite utiliser le partage réseau comme destination de sauvegarde, au lieu d'utiliser un stockage attaché localement.

Vous pouvez configurer le stockage localement connecté lorsque vous déployez une appliance virtuelle, ou vous pouvez configurer le stockage ultérieurement.

Pour plus d'informations sur la configuration du stockage local lors du déploiement d'une appliance virtuelle, voir "Configuration de l'appliance virtuelle" (p. 139) (pour VMware) et "Configuration de l'appliance virtuelle" (p. 143) (pour Scale Computing).

Pour configurer le stockage local après le déploiement d'une appliance virtuelle

1. Dans votre environnement de machine virtuelle, sélectionnez l'appliance virtuelle, puis ouvrez ses paramètres pour les modifier.
2. Ajoutez un nouveau disque dur à l'appliance virtuelle.
   La taille du disque doit être d'au moins 10 Go.

   Avertissement !
   Si vous utilisez un disque qui contient des données, les données seront supprimées.

3. Dans votre environnement de machine virtuelle, ouvrez la console de l'appliance virtuelle.
4. Sous **Stockages locaux**, cliquez sur **Actualiser**.
   Le bouton **Créer un stockage** devient actif.
5. Cliquez sur **Créer un stockage**, puis sélectionnez le disque que vous avez ajouté à l'appliance virtuelle.
   - Sélectionnez une lettre de lecteur.
   - [Facultatif] Spécifiez une étiquette de disque.

© Acronis International GmbH, 2003-2026

La longueur du nom est limitée à 16 caractères à cause des limites du système de fichiers.

6. Cliquez sur **OK**.
7. Cliquez sur **Oui**.

Pour sélectionner le stockage localement connecté comme destination de sauvegarde

- Lorsque vous créez un plan de protection, dans **Où sauvegarder**, sélectionnez **Dossiers locaux**, puis spécifiez la lettre de lecteur du stockage localement connecté. Par exemple, **D:**.

Liaison de machine virtuelle

Ce sujet décrit comment le service Cyber Protection organise le fonctionnement de plusieurs agents au sein de VMware vCenter.

L'algorithme de distribution ci-dessous fonctionne à la fois pour les appliances virtuelles et les agents installés dans Windows.

Algorithme de distribution

Les machines virtuelles sont automatiquement distribuées de façon égale entre les Agents pour VMware. Par uniformément, nous voulons dire que chaque agent gère un nombre égal de machines. La quantité d'espace de stockage occupée par une machine virtuelle n'est pas comptée.

Toutefois, lors du choix d'un agent pour une machine, le logiciel essaie d'optimiser les performances générales du système. En particulier, le logiciel considère l'emplacement de l'agent et de la machine virtuelle. Un agent hébergé sur le même hôte est préféré. S'il n'y a aucun agent sur le même hôte, un agent du même cluster est préféré.

Quand une machine virtuelle est assignée à un agent, toutes les sauvegardes de cette machine sont déléguées à cet agent.

Redistribution

La redistribution prend place chaque fois que l'équilibre établi se brise ou, plus précisément, lorsqu'un déséquilibre de charge entre les agents atteint 20 pour cent. Cela peut se produire lorsqu'une machine ou un agent est ajouté ou supprimé, ou qu'une machine migre vers un autre hôte ou cluster, ou si vous liez manuellement une machine à un agent. Si cela se produit, le service Cyber Protection redistribue les machines en utilisant le même algorithme.

Par exemple, vous réalisez que vous avez besoin de plus d'agents pour aider avec le débit et déployez une appliance virtuelle supplémentaire au cluster. Le service Cyber Protection assignera les machines les plus adaptées au nouvel agent. La charge des anciens agents sera réduite.

Lorsque vous supprimez un agent du service Cyber Protection, les machines assignées à l'agent sont distribuées parmi les agents restants. Cependant, cela ne se produira pas si un agent est endommagé ou est supprimé manuellement de vSphere. La redistribution démarrera seulement après que vous ayez supprimé cet agent de l'interface Web.

© Acronis International GmbH, 2003-2026

Affichage du résultat de la distribution

Vous pouvez voir le résultat de la distribution automatique :

- dans la colonne **Agent** pour chaque machine virtuelle dans la section **Tous les terminaux**
- dans la section **machines virtuelles attribuées** du volet **Détails** lorsqu'un agent est sélectionné dans la section **Paramètres** > **Agents**

Liaison manuelle

La liaison de l'Agent pour VMware vous permet d'exclure une machine virtuelle de ce processus de distribution en spécifiant l'agent qui doit toujours sauvegarder cette machine. L'équilibre général sera maintenu, mais cette machine en particulier peut être passée à un agent différent uniquement si l'agent d'origine est supprimé.

Pour lier une machine avec un agent

1. Sélectionnez la machine.
2. Cliquez sur **Détails**.
   Dans la section **Agent attribué**, le logiciel affiche l'agent qui gère actuellement la machine sélectionnée.
3. Cliquez sur **Modifier**.
4. Sélectionnez **Manuel**.
5. Sélectionnez l'agent auquel vous souhaitez lier la machine.
6. Cliquez sur **Enregistrer**.

Pour annuler la liaison d'une machine avec un agent

1. Sélectionnez la machine.
2. Cliquez sur **Détails**.
   Dans la section **Agent attribué**, le logiciel affiche l'agent qui gère actuellement la machine sélectionnée.
3. Cliquez sur **Modifier**.
4. Sélectionnez **Automatique**.
5. Cliquez sur **Enregistrer**.

Désactivation de l'attribution automatique pour un agent

Vous pouvez désactiver l'attribution automatique pour un Agent pour VMware dans le but de l'exclure du processus de distribution en spécifiant la liste des machines que cet agent doit sauvegarder. L'équilibre général sera maintenu entre les autres agents.

L'attribution automatique ne peut pas être désactivée pour un agent s'il n'y a aucun autre agent enregistré, ou si l'attribution automatique est désactivée pour tous les autres agents.

Pour désactiver l'attribution automatique pour un agent

© Acronis International GmbH, 2003-2026

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez l'Agent pour VMware pour lequel vous souhaitez désactiver l'attribution automatique.
3. Cliquez sur **Détails**.
4. Désactivez le commutateur **Attribution automatique**.

Exemples d'utilisation

- La liaison manuelle est pratique si vous voulez qu'une machine en particulier (de très grande capacité) soit sauvegardée par l'Agent pour VMware (Windows) via fibre channel, tandis que les autres machines sont sauvegardées par des appliances virtuelles.
- Il est nécessaire de lier les machines virtuelles à un agent si l'agent utilise un stockage localement attaché.
- Désactiver l'attribution automatique vous permet de vous assurer qu'une machine en particulier est sauvegardée de façon prévisible selon le calendrier que vous avez spécifié. L'agent qui ne sauvegarde qu'une seule MV ne peut pas se charger de sauvegarder d'autres MV à l'heure planifiée.
- Désactiver l'attribution automatique est utile si vous avez plusieurs hôtes ESXi séparés géographiquement. Si vous désactivez l'attribution automatique puis liez les MV de chaque hôte à l'agent s'exécutant sur le même hôte, vous pouvez vous assurer que l'agent ne sauvegardera jamais aucune machine s'exécutant sur des hôtes ESXi distants, réduisant ainsi le trafic réseau.

Exécution automatique de scripts pre-freeze et post-thaw

Avec VMware Tools, vous pouvez exécuter automatiquement des scripts pre-freeze et post-thaw personnalisés sur des machines virtuelles que vous sauvegardez en mode sans agent. Ainsi, vous pouvez exécuter des scripts de suspension personnalisés et créer des sauvegardes cohérentes avec les applications pour les machines virtuelles qui exécutent des applications compatibles VSS.

Prérequis

Les scripts pre-freeze et post-thaw doivent se trouver dans un dossier spécifique sur la machine virtuelle.

- Pour les machines virtuelles Windows, l'emplacement de ce dossier dépend de la version ESXi de l'hôte.

  Par exemple, pour les machines virtuelles exécutées sur un hôte ESXi 6.5, ce dossier est `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. Vous devez créer le dossier `backupScritps.d` manuellement. N'archivez pas d'autres types de fichiers dans ce dossier, parce que cela pourrait rendre l'outil VMware Tools instable.

  Pour plus d'informations sur l'emplacement des scripts pre-freeze et post-thaw pour d'autres extensions ESXi, reportez-vous à la documentation VMware.
- Pour les machines virtuelles Linux, copiez respectivement vos scripts dans les répertoires `/usr/sbin/pre-freeze-script` et `/usr/sbin/post-thaw-script`. Les scripts sous `/usr/sbin/pre-`

© Acronis International GmbH, 2003-2026

`freeze-script` sont exécutés lorsque vous créez un instantané et ceux sous `/usr/sbin/post-thaw-script` sont exécutés une fois l'instantané terminé. Les scripts doivent pouvoir être exécutés par l'utilisateur de VMware Tools.

Pour exécuter automatiquement des scripts pre-freeze et post-thaw

1. Assurez-vous que VMware Tools est installé sur la machine virtuelle.
2. Sur la machine virtuelle, ajoutez vos scripts personnalisés aux dossiers appropriés.
3. Dans le plan de protection de cette machine, activez l'option **Service de cliché instantané des volumes (VSS) pour les machines virtuelles**.
   Cela crée un instantané VMware avec l'option **Suspendre le système de fichiers invité**, ce qui déclenche à son tour les scripts de pre-freeze et de post-thaw sur la machine virtuelle.

Vous n'avez pas besoin d'exécuter de scripts de suspension sur les machines virtuelles qui exécutent des applications compatibles VSS, telles que Microsoft SQL Server ou Microsoft Exchange. Pour créer une sauvegarde cohérente avec les applications pour de telles machines, activez l'option **Service de cliché instantané des volumes (VSS) pour les machines virtuelles** dans le plan de protection.

Support pour la migration d'une machine virtuelle

Cette section vous renseigne sur ce qui vous attend lors de la migration de machines virtuelles au sein d'un environnement vSphere, y compris lors de la migration entre des hôtes ESXi appartenant à un cluster vSphere.

vMotion déplace l'état et la configuration d'une machine virtuelle vers un autre hôte alors que les disques de l'ordinateur demeurent dans le même emplacement dans le stockage partagé. Storage vMotion déplace les disques d'une machine virtuelle d'un magasin de données vers un autre.

- La migration avec vMotion, y compris Storage vMotion, n'est pas prise en charge pour une machine virtuelle qui exécute l'agent pour VMware (appliance virtuelle) et doit être désactivée après le déploiement de l'appliance. Vous devez ajouter cette machine virtuelle à la liste des substitutions de la machine virtuelle dans la configuration du cluster vSphere afin d'éviter la migration de la machine virtuelle de l'appliance dans les nœuds du cluster vSphere.
- Lorsque la sauvegarde d'une machine virtuelle démarre, la migration avec vMotion, y compris Storage vMotion, est automatiquement désactivée. Cette machine virtuelle est temporairement ajoutée à la liste **Remplacements de VM** dans la configuration des clusters vSphere. Une fois la sauvegarde terminée, les paramètres **Remplacements de VM** sont automatiquement rétablis à l'état précédent.
- Il n'est pas possible de lancer la sauvegarde d'une machine virtuelle pendant si sa migration avec vMotion, y compris Storage vMotion, est en cours. La sauvegarde démarrera une fois la migration terminée.

© Acronis International GmbH, 2003-2026

Protection des environnements de virtualisation

Dans la console Cyber Protect, vous pouvez voir les environnements vSphere, Hyper-V et Virtuozzo dans leur présentation native. Après avoir installé et enregistré l'agent correspondant, l'onglet **VMware**, **Hyper-V** ou **Virtuozzo** apparaît sous **Terminaux**.

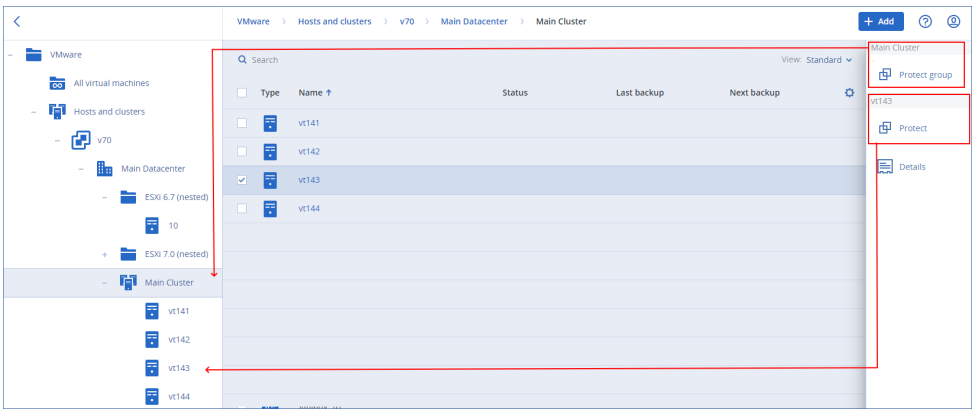
Par exemple, dans l'onglet **VMware**, vous pouvez sauvegarder les objets d'infrastructure vSphere suivants :

- vCenter
- Centre de données
- Dossier
- Cluster
- Hôte ESXi
- Liste des ressources
- Machine virtuelle

Pour appliquer un plan à un objet d'infrastructure sélectionné, cliquez sur **Protéger**. Tous les objets enfants seront sauvegardés.

Pour appliquer un plan à l'objet parent de l'objet d'infrastructure sélectionné, cliquez sur **Protéger le groupe**. Tous les objets enfants de l'objet parent seront sauvegardés.

Par exemple, si vous appliquez un plan à un hôte ESXi, toutes les machines virtuelles de cet hôte seront sauvegardées. Si vous appliquez un plan au cluster parent, toutes les machines virtuelles de tous les hôtes de ce cluster seront sauvegardées.



Affichage de l'état de la sauvegarde dans vSphere Client

Vous pouvez afficher l'état de la sauvegarde et la dernière heure de sauvegarde d'une machine virtuelle dans vSphere Client.

Cette information apparaît dans le résumé de la machine virtuelle (**Résumé** > **Attributs personnalisés**/**Annotations**/**Remarques**, en fonction du type de client et de la version de

© Acronis International GmbH, 2003-2026

vSphere). Vous pouvez également activer les colonnes **Dernière sauvegarde** et **État de la sauvegarde** sur l'onglet **Machines virtuelles** pour tous les hôtes, centres de données, dossiers, pools de ressources ou le serveur vCenter entier.

Pour fournir ces attributs, l'agent pour VMware doit disposer des privilèges suivants en plus de ceux décrits dans la section « Agent pour VMware - privilèges nécessaires » :

- **Global** > **Gérer les rapports personnalisés**
- **Global** > **Définir un attribut personnalisé**

Privilèges requis pour l'agent pour VMware

Remarque
Pour permettre les sauvegardes des machines virtuelles, installez les API vStorage sur l'hôte ESXi. Pour plus d'informations, voir cet article de la base de connaissances.

L'agent pour VMware s'authentifie auprès de vCenter ou de l'hôte ESXi à l'aide d'un compte d'utilisateur spécifié lors du déploiement de l'agent. Le compte d'utilisateur doit avoir un rôle qui inclut les privilèges énumérés dans le tableau ci-dessous. Nous vous recommandons d'utiliser un compte et un rôle dédiés, plutôt que d'utiliser un compte existant ayant le rôle d'administrateur.

Le compte d'utilisateur doit être autorisé à accéder à tous les niveaux de l'infrastructure vSphere, tels que vCenter, les centres de données, les clusters, les hôtes ESXi, les pools de ressources et les machines virtuelles. Pour savoir comment ajouter une autorisation au niveau vCenter et la propager aux autres niveaux, voir "Octroi d'une autorisation d'accès au compte utilisateur" (p. 983).

Vous pouvez modifier le compte utilisateur utilisé par l'agent pour VMware sans redéployer l'agent. Pour savoir comment modifier le compte, voir "Modification du compte utilisateur de l'agent pour VMware" (p. 984).

Objet	Droit	Opération			
		Sauvegarder une MV	**Restaurer sur une nouvelle MV**	**Restaurer sur une MV existante**	**Exécuter une MV à partir d'une sauvegarde**
Opérations de chiffrement (à partir de vSphere 6.5)					
	Ajouter un disque	+*			

© Acronis International GmbH, 2003-2026

Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
	Accès direct	+*			
Magasin de données					
	Allouer de l'espace		+	+	+
	Parcourir le magasin de données				+
	Configurer un magasin de données	+	+	+	+
	Opérations de bas niveau sur les fichiers				+
Global					
	Désactiver les méthodes	+	+	+	
	Activer les méthodes	+	+	+	
	Licences	+	+	+	+
	Gérer les rapports personnalisés	+	+	+	
	Définir un attribut personnalisé	+	+	+	
Hôte > **Configuration**					
	Configuration de la partition de stockage				+

© Acronis International GmbH, 2003-2026

Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
	Modifier le cluster				
Hôte > **Opérations locales**					
	Créer une machine virtuelle				+
	Supprimer une machine virtuelle				+
	Reconfigurer la machine virtuelle				+
Réseau					
	Attribuer un réseau		+	+	+
Ressource					
	Attribuer une machine virtuelle à un pool de ressources		+	+	+
Machine virtuelle > **Modifier la configuration**					
	Acquérir une location de disque	+		+	
	Ajouter un disque existant	+	+		+

© Acronis International GmbH, 2003-2026

Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
	Ajouter un nouveau disque		+	+	+
	Ajouter ou supprimer un terminal		+		+
	Configuration avancée	+	+	+	
	Modifier le nombre de processeurs		+		
	Modifier la mémoire		+		
	Modifier les paramètres		+	+	+
	Modifier une ressource	+	+		
	Modifier les paramètres du terminal	+	+		
	Supprimer un disque	+	+	+	+
	Renommer		+		
	Définir une annotation				+
	Afficher/Masquer le suivi des changements de disque	+		+	
Machine virtuelle > Opérations invité					

© Acronis International GmbH, 2003-2026

Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
	Modifications des opérations invité	+**			
	Exécution de programme d'opération invité	+**			
	Requêtes d'opération invité	+**			
Machine virtuelle > **Interaction**					
	Obtenir le ticket de contrôle invité (dans vSphere 4.1 et 5.0)				+
	Configurer le support CD		+	+	
	Gestion du système d'exploitation invité par VIX API (dans vSphere 5.1 et versions ultérieures)				+
	Mise hors tension			+	+
	Mettre sous tension		+	+	+
Machine virtuelle >					

© Acronis International GmbH, 2003-2026

Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
Inventaire					
	Créer à partir d'une machine existante		+	+	+
	Créer une nouvelle		+	+	+
	Enregistrer				+
	Supprimer		+	+	+
	Désinscrire				+
Machine virtuelle > **Allocation**					
	Autoriser l'accès au disque		+	+	+
	Autoriser l'accès au disque en lecture seule	+		+	
	Autoriser le téléchargement de machine virtuelle	+	+	+	+
Machine virtuelle > **État** **Machine virtuelle** > **Gestion des instantanés** (vSphere 6.5 et versions ultérieures)					
	Créer un	+		+	+

© Acronis International GmbH, 2003-2026

Objet	Droit	Opération			
		Sauvegarder une MV	Restaurer sur une nouvelle MV	Restaurer sur une MV existante	Exécuter une MV à partir d'une sauvegarde
	instantané				
	Supprimer l'instantané	+		+	+
vApp					
	Ajouter une machine virtuelle				+

* Ce privilège n'est requis que pour la sauvegarde d'ordinateurs chiffrés.

** Ce privilège n'est requis que pour les sauvegardes reconnaissant les applications.

Octroi d'une autorisation d'accès au compte utilisateur

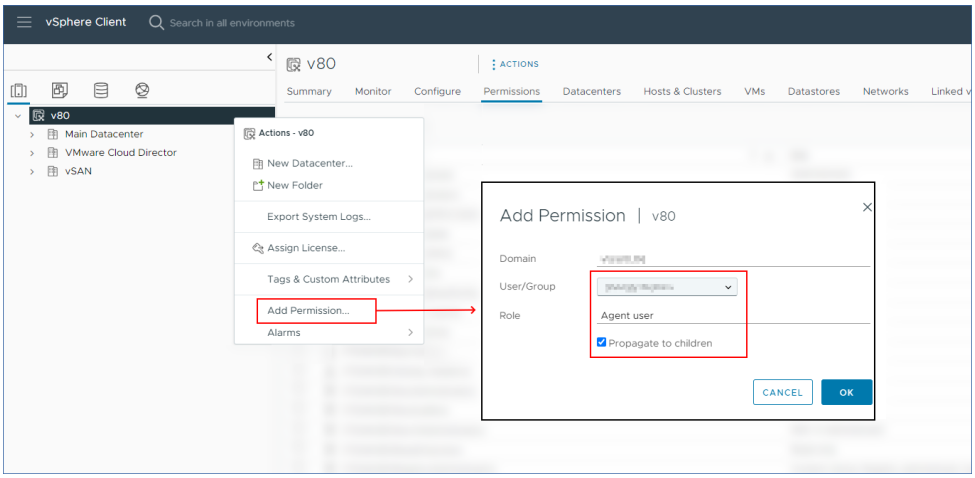
Le compte d'utilisateur utilisé par l'agent pour VMware doit avoir accès à tous les niveaux de l'infrastructure vSphere tels que vCenter, les centres de données, les clusters, les hôtes ESXi, les pools de ressources et les machines virtuelles.

Pour accorder une autorisation d'accès au compte utilisateur

1. Dans vSphere Client, accédez à **Inventaire**.
2. Cliquez avec le bouton droit de la souris sur l'objet **vCenter** pour lequel vous souhaitez accorder une autorisation, puis cliquez sur **Ajouter une autorisation**.
3. Dans la boîte de dialogue **Ajouter une autorisation**, sélectionnez un compte utilisateur et un rôle.

   Le rôle doit inclure les privilèges répertoriés dans "Privilèges requis pour l'agent pour VMware" (p. 977).
4. Cochez la case **Propager aux enfants**.
5. Cliquez sur **OK**.

© Acronis International GmbH, 2003-2026



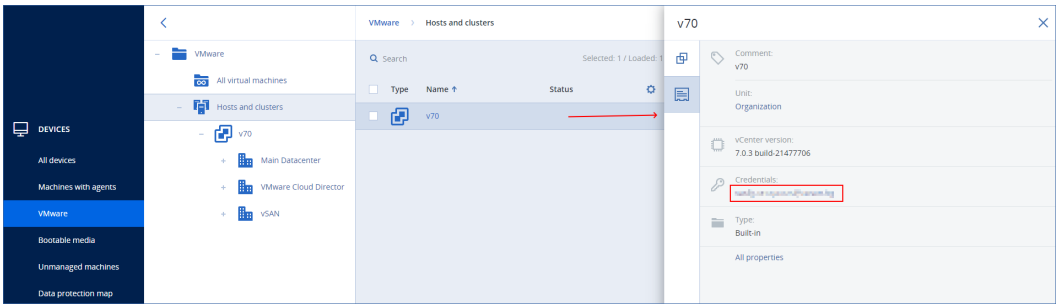
Modification du compte utilisateur de l'agent pour VMware

Dans la console Cyber Protect, vous pouvez modifier le compte utilisateur d'un seul agent ou de tous les agents sur vCenter ou un hôte ESXi.

Pour modifier le compte d'utilisateur de l'agent pour VMware

Pour tous les agents

1. Dans la console Cyber Protect, accédez à **Terminaux** > **VMware**.
2. Cliquez sur **Hôtes et clusters**.
3. Dans le panneau principal, cliquez sur l'espace vide à côté du nom de vCenter ou de l'hôte ESXi autonome.
4. Dans le panneau de droite, cliquez sur **Détails**.
5. Sous **Informations d'identification**, cliquez sur le compte d'utilisateur.



6. Spécifiez le nouveau compte d'utilisateur et le mot de passe de ce compte.
7. Cliquez sur **OK**.

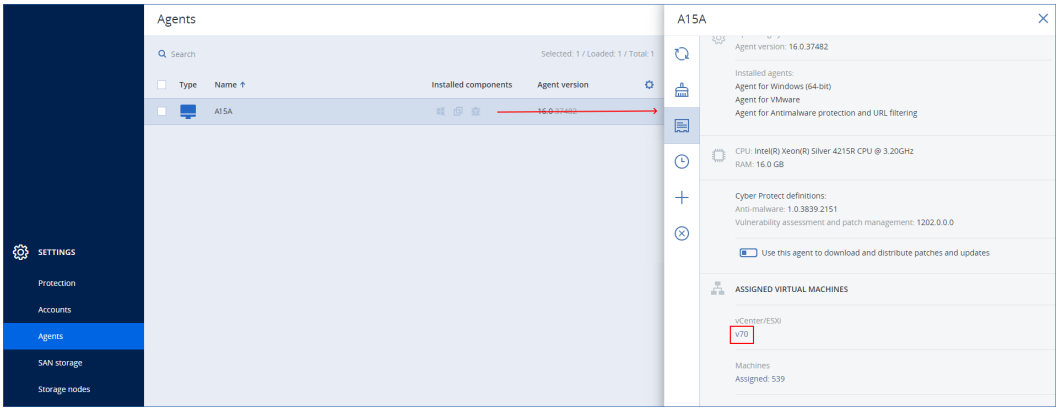
Par conséquent, tous les agents de ce vCenter ou de cet hôte ESXi utiliseront le nouveau compte d'utilisateur.

Pour un seul agent

1. Dans la console Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez l'agent.

© Acronis International GmbH, 2003-2026

3. Dans le panneau de droite, cliquez sur **Détails**.
4. Sous **Machines virtuelles assignées**, cliquez sur le nom du vCenter/de l'hôte ESXi.



5. Dans l'écran **Ajouter un hôte VMware vCenter ou ESXi**, indiquez le nouveau compte d'utilisateur et le mot de passe de ce compte.
6. Cliquez sur **Configurer**.

Sauvegarde de machines Hyper-V en cluster.

Dans un cluster Hyper-V, les machines virtuelles peuvent migrer entre les nœuds cluster. Suivez ces recommandations pour configurer une sauvegarde correcte de machines Hyper-V en cluster :

1. Une machine doit être disponible pour la sauvegarde quel que soit le nœud sur lequel elle migre. Pour garantir que l'agent pour Hyper-V puisse accéder à une machine sur n'importe quel nœud, le service de l'agent doit être exécuté sous un compte utilisateur de domaine qui dispose de privilèges administratifs sur chacun des nœuds cluster.

   Nous vous conseillons de spécifier un tel compte pour le service de l'agent pendant l'installation de l'agent pour Hyper-V.
2. Installez l'agent pour Hyper-V sur chaque nœud du cluster.
3. Enregistrez tous les agents dans le service Cyber Protection.

Haute disponibilité d'une machine restaurée

Lorsque vous restaurez des disques sauvegardés vers une machine virtuelle Hyper-V *existante*, la propriété de haute disponibilité de la machine reste inchangée.

Lorsque vous récupérez des disques sauvegardés sur une *nouvelle* machine virtuelle Hyper-V, la machine résultante n'est pas hautement disponible. Elle est considéré comme une machine de rechange et est normalement désactivée. Si vous devez utiliser la machine dans l'environnement de production, vous pouvez la configurer pour la haute disponibilité à partir du composant logiciel enfichable **Gestion du cluster de basculement**.

© Acronis International GmbH, 2003-2026

Limite le nombre total de machines virtuelles sauvegardées simultanément.

Dans l'option de sauvegarde **Planification**, vous pouvez limiter le nombre de machines virtuelles sauvegardées simultanément par plan de protection.

Lorsqu'un agent exécute plusieurs plans simultanément, le nombre de machines sauvegardées simultanément s'incrémente. Cela peut avoir une incidence sur les performances de sauvegarde et surcharger aussi bien l'hébergeur que le stockage de la machine virtuelle. Vous pouvez éviter ces problèmes en configurant une limite au niveau de l'agent.

Pour limiter le nombre de sauvegardes simultanées au niveau de l'agent

Agent pour VMware (Windows)

1. Sur l'ordinateur avec l'agent, créez un nouveau document texte et ouvrez-le dans un éditeur de texte.
2. Copiez et collez les lignes suivantes dans le fichier.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Remplacez `00000001` par la valeur hexadécimale de la limite que vous souhaitez définir.
   Par exemple, `00000001` est 1 et `0000000A` est 10.
4. Enregistrez le document sous **limit.reg**.
5. Exécutez le fichier en tant qu'administrateur.
6. Confirmez que vous souhaitez modifier le registre Windows.
7. Redémarrez l'agent.
   a. Dans le menu **Démarrer**, cliquez sur **Exécuter**.
   b. Saisissez **cmd**, puis cliquez sur **OK**.
   c. Dans la ligne de commande, exécutez les commandes suivantes :

```
net stop mms
net start mms
```

Agent pour Hyper-V

1. Sur l'ordinateur avec l'agent, créez un nouveau document texte et ouvrez-le dans un éditeur de texte.
2. Copiez et collez les lignes suivantes dans le fichier.

© Acronis International GmbH, 2003-2026

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Remplacez `00000001` par la valeur hexadécimale de la limite que vous souhaitez définir.
   Par exemple, `00000001` est 1 et `0000000A` est 10.
4. Enregistrez le document sous **limit.reg**.
5. Exécutez le fichier en tant qu'administrateur.
6. Confirmez que vous souhaitez modifier le registre Windows.
7. Redémarrez l'agent.
   a. Dans le menu **Démarrer**, cliquez sur **Exécuter**.
   b. Saisissez **cmd**, puis cliquez sur **OK**.
   c. Dans la ligne de commande, exécutez les commandes suivantes :

```
net stop mms
net start mms
```

Appliances virtuelles

Cette procédure s'applique aux appliances virtuelles, telles que l'agent pour VMware (appliance virtuelle), l'agent pour Scale Computing, l'agent pour Virtuozzo Hybrid Infrastructure, l'agent pour oVirt et l'agent pour Nutanix.

1. Dans la console de l'appliance virtuelle, appuyez sur CTRL+MAJ+F2 pour ouvrir l'interface de ligne de commande.
2. Ouvrez le fichier `/etc/Acronis/MMS.config` dans un éditeur de texte.
3. Localisez la section suivante :

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Remplacez `10` par le nombre maximal de sauvegardes simultanées que vous souhaitez définir.
5. Enregistrez le fichier.
6. Redémarrez l'agent en exécutant la commande `reboot`.

Agents inclus dans l'offre groupée Agent pour Linux

Cette procédure s'applique aux agents qui sont offerts groupés avec l'agent pour Linux, tels que l'agent pour Proxmox et l'agent pour Virtuozzo.

1. Connectez-vous en tant qu'utilisateur root sur la machine sur laquelle se trouve l'agent.
   Utilisez le même mot de passe que celui utilisé pour vous connecter à la console Cyber Protect.

© Acronis International GmbH, 2003-2026

2. Ouvrez le fichier `/etc/Acronis/MMS.config` dans un éditeur de texte.
3. Localisez la section suivante :

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Remplacez `10` par le nombre maximum de sauvegardes parallèles que vous souhaitez définir.
5. Enregistrez le fichier.
6. Exécutez la commande suivante pour redémarrer l'agent :

```
sudo service acronis_mms restart
```

Sauvegarde avec agent de machines virtuelles Microsoft Azure et Amazon EC2

Important
Suivez les procédures de cette section pour sauvegarder et restaurer des machines virtuelles Azure si vous n'utilisez pas l'agent pour Azure.

Si vous utilisez l'agent pour Azure, vous pouvez restaurer une sauvegarde de type **Machine complète** en tant que machine virtuelle directement. Pour plus d'informations, voir "Restauration de machines physiques" (p. 674) et "Restauration de machines virtuelles" (p. 689).

Sauvegarde des machines virtuelles Microsoft Azure et Amazon EC2

Important
Suivez cette procédure pour les machines virtuelles Microsoft Azure si vous n'utilisez pas l'agent pour Azure.

Si vous utilisez l'agent pour Azure, vous pouvez restaurer une sauvegarde de type **Machine complète** en tant que machine virtuelle directement. Pour plus d'informations, voir "Restauration de machines physiques" (p. 674) et "Restauration de machines virtuelles" (p. 689).

Pour sauvegarder des machines virtuelles Microsoft Azure ou Amazon EC2

1. Installez un agent de protection sur la machine que vous souhaitez sauvegarder.
2. Configurez et exécutez un plan de protection en suivant les indications de "Sauvegarde" (p. 547).

Les opérations de sauvegarde et de restauration sont les mêmes que celles d'un ordinateur physique. Toutefois, la machine sauvegardée sera comptée comme étant virtuelle lorsque vous définirez des quotas pour le nombre de machines.

Contrairement aux machines physiques, vous ne pouvez pas démarrer les machines virtuelles Microsoft Azure et Amazon EC2 à partir de supports de démarrage.

© Acronis International GmbH, 2003-2026

Restauration de machines virtuelles Microsoft Azure et Amazon EC2

Important
Suivez cette procédure pour les machines virtuelles Microsoft Azure si vous n'utilisez pas l'agent pour Azure.

Si vous utilisez l'agent pour Azure, vous pouvez restaurer une sauvegarde de type **Machine complète** en tant que machine virtuelle directement. Pour plus d'informations, voir "Restauration de machines physiques" (p. 674) et "Restauration de machines virtuelles" (p. 689).

Pour restaurer une machine en tant que nouvelle machine virtuelle Microsoft Azure ou Amazon EC2

1. Créez une nouvelle machine virtuelle à partir d'une image/d'un modèle dans Microsoft Azure ou Amazon EC2.
   La nouvelle machine doit avoir la même configuration de disque que la machine que vous souhaitez restaurer.
2. Sur la nouvelle machine, installez l'agent pour Windows ou l'agent pour Linux.
3. Restaurez la machine sauvegardée en suivant les indications de "Restauration de machines physiques" (p. 674).
   Lorsque vous configurez la restauration, sélectionnez la nouvelle machine en tant que machine cible.

Remarque
Pour les machines virtuelles Microsoft Azure, cette procédure de restauration s'applique uniquement aux sauvegardes d'ordinateurs qui contiennent tous les pilotes nécessaires pour fonctionner dans Azure de manière native (sauvegardes de machines virtuelles Azure, d'ordinateurs Hyper-V locaux ou d'ordinateurs exécutant Windows Server 2016 ou une version ultérieure). Pour une restauration interplate-forme, consultez cet article de la base de connaissances.

Création d'un support de démarrage afin de restaurer des systèmes d'exploitation

Un support de démarrage est un support physique (CD, DVD, lecteur flash USB ou autre support amovible) qui vous permet d'exécuter l'agent de protection dans un environnement Linux, WinPE (Windows Preinstallation Environment) ou WinRE (Windows Recovery Environment), sans l'aide d'un système d'exploitation. La fonction première d'un support de démarrage est de restaurer les systèmes d'exploitation qui ne démarrent pas.

Remarque
Le support de démarrage n'est pas compatible avec les lecteurs hybrides.

L'exécution du support de démarrage nécessite 1,5 Go de RAM.

© Acronis International GmbH, 2003-2026

Support de démarrage personnalisé ou tout prêt ?

Avec Bootable Media Builder, vous pouvez créer un support de démarrage personnalisé (basé sur Linux ou WinPE) pour ordinateurs Windows, Linux ou macOS. Dans votre support de démarrage personnalisé basé sur Linux ou WinPE/WinRE, vous pouvez configurer des paramètres supplémentaires, comme l'enregistrement automatique, les paramètres réseau ou les paramètres de serveur proxy. Dans les supports de démarrage personnalisés basés sur WinPE/WinRE, vous pouvez aussi ajouter des pilotes supplémentaires.

Si vous préférez, vous pouvez aussi télécharger un support de démarrage tout prêt (basé sur Linux uniquement). Le support de démarrage tout prêt ne peut être utilisé que pour les opérations de restauration et l'accès à la fonctionnalité Universal Restore.

Support de démarrage basé sur Linux ou sur WinPE/WinRE ?

Basé sur Linux

Un support de démarrage basé sur Linux contient un agent de protection basé sur un noyau Linux. L'agent peut démarrer et réaliser des opérations sur n'importe quel matériel compatible PC, y compris un système vierge et des machines avec des systèmes de fichiers corrompus ou incompatibles.

Basé sur WinPE/WinRE

Un support de démarrage basé sur WinPE contient un système Windows minimal appelé Windows Preinstallation Environment (WinPE) ainsi qu'un plug-in Cyber Protection pour WinPE. Ce plug-in est une modification de l'agent de protection et peut s'exécuter dans l'environnement de préinstallation. Un support de démarrage basé sur WinRE utilise Windows Recovery Environment et ne nécessite pas l'installation de packages Windows supplémentaires.

WinPE se révèle être la solution de démarrage la plus pratique dans les grands environnements avec un matériel hétérogène.

Avantages :

- L'utilisation de Cyber Protection dans Windows Preinstallation Environment offre davantage de fonctionnalités que l'utilisation d'un support de démarrage basé sur Linux. Après avoir démarré un matériel compatible PC sous WinPE, vous pouvez utiliser l'agent de protection, les commandes et scripts WinPE, ainsi que tous les plug-ins que vous avez ajoutés à l'environnement de préinstallation (PE).
- Un support de démarrage PE aide à résoudre certains problèmes de support de démarrage liés à un environnement Linux tels que la prise en charge de certains contrôleurs RAID ou certains niveaux de piles RAID seulement. Un support basé sur WinPE 2.x ou ultérieur permet le chargement dynamique des pilotes des périphériques nécessaires.

Limites :

© Acronis International GmbH, 2003-2026

- Un support de démarrage basé sur une version de WinPE antérieure à 4.0 ne peut pas démarrer sur des machines qui utilisent le Unified Extensible Firmware Interface (UEFI).

Création d'un support de démarrage physique

Nous vous recommandons vivement de créer un support de démarrage et de le tester dès que vous commencez à utiliser une sauvegarde de niveau disque. En outre, il est également recommandé de recréer le support à chaque nouvelle mise à jour importante de l'agent de protection.

Vous pouvez restaurer Windows et Linux à partir du même support. Pour restaurer macOS, créez un support à part à partir d'une machine sous macOS.

Pour créer un support de démarrage physique sous Windows ou Linux

1. Créez un fichier ISO de support de démarrage personnalisé ou téléchargez le fichier ISO tout prêt.

   Pour créer un fichier ISO personnalisé, utilisez "Bootable Media Builder" (p. 992).

   Pour télécharger le fichier ISO tout prêt, accédez à la console Cyber Protect, sélectionnez un ordinateur, puis cliquez sur **Restaurer** > **Autres méthodes de restauration...** > **Télécharger l'image ISO**.
2. [Facultatif] Dans la console Cyber Protect, générez un jeton d'enregistrement. Le jeton d'enregistrement s'affiche automatiquement lorsque vous téléchargez un fichier ISO tout prêt.

   Ce jeton permet au support de démarrage d'accéder au stockage Cloud, sans vous demander de saisir d'identifiant ni de mot de passe.
3. Créez un support de démarrage physique de l'une des manières suivantes :
   - Gravez le fichier ISO sur un CD/DVD.
   - Créez un lecteur flash USB de démarrage avec le fichier ISO et l'un des outils gratuits disponibles en ligne.

     Utilisez `ISO vers USB` ou `RUFUS` pour démarrer une machine UEFI et `Win32DiskImager` pour une machine BIOS. Sous Linux, l'utilisation de la commande `dd` est toute indiquée.

   Pour les machines virtuelles, vous pouvez connecter le fichier ISO en tant que lecteur CD/DVD à la machine virtuelle que vous souhaitez restaurer.

Pour créer un support de démarrage physique sous macOS

1. Sur les machines où l'agent pour Mac est installé, cliquez sur **Applications** > **Rescue Media Builder**.
2. Le logiciel affiche les supports amovibles connectés. Sélectionnez celui que vous désirez utiliser.

   Avertissement !
   Toutes les données sur le disque seront effacées.
3. Cliquez sur **Créer**.
4. Patientez pendant que le logiciel crée le support de démarrage.

© Acronis International GmbH, 2003-2026

Bootable Media Builder

Bootable Media Builder permet de créer des supports de démarrage. Il est installé sous la forme d'un composant optionnel sur l'ordinateur sur lequel l'agent de protection est installé.

Pourquoi utiliser Bootable Media Builder ?

Le support de démarrage tout prêt et disponible au téléchargement dans la console Cyber Protect se base sur un noyau Linux. Contrairement à Windows PE, il ne permet pas d'implanter des pilotes personnalisés à la volée.

Bootable Media Builder vous permet de créer des images de support de démarrage personnalisées Linux ou WinPE.

32 bits ou 64 bits ?

Bootable Media Builder crée un support de démarrage avec des composants 32 bits et 64 bits. Dans la plupart des cas, vous avez besoin d'un support 64 bits pour démarrer une machine qui utilise l'interface UEFI (Unified Extensible Firmware Interface).

Support de démarrage basé sur un environnement Linux

Pour créer un support de démarrage basé sur Linux

1. Démarrez **Bootable Media Builder**.
2. Dans **Type de support de démarrage**, sélectionnez **Défaut (support basé sur Linux)**.
3. Sélectionnez la manière dont les volumes et les ressources réseau seront représentés :
   - Un support de démarrage avec une représentation de volume de type Linux affiche les volumes comme suit : hda1 et sdb2, par exemple. Il essaye de reconstruire les périphériques MD et les volumes logiques (LVM) avant de démarrer une restauration.
   - Un support de démarrage avec une représentation de volume de type Windows affiche les volumes comme suit : C: et D:, par exemple. Il permet d'accéder aux volumes dynamiques (LDM).
4. [Facultatif] Spécifiez les paramètres du noyau Linux. Séparez des paramètres multiples par des espaces.

   Par exemple, pour pouvoir sélectionner un mode d'affichage pour l'agent de démarrage chaque fois que le support démarre, saisissez : **vga=ask**. Pour plus d'informations sur les paramètres disponibles, reportez-vous à "Paramètres du noyau" (p. 993).
5. [Facultatif] Sélectionnez la langue du support de démarrage.
6. [Facultatif] Sélectionnez le mode de démarrage (BIOS ou UEFI) que Windows utilisera après la restauration.
7. Sélectionnez le composant à placer sur le support : l'agent de démarrage Cyber Protection.
8. [Facultatif] Spécifiez l'intervalle d'arrêt pour le menu de démarrage. Si ce paramètre n'est pas configuré, le chargeur attendra que vous choisissiez quoi démarrer entre le système

© Acronis International GmbH, 2003-2026

d'exploitation (s'il est présent) ou le composant.

9. [Facultatif] Si vous souhaitez automatiser les opérations de l'agent de démarrage, cochez la case **Utiliser le script suivant**. Sélectionnez ensuite l'un des scripts et définissez les paramètres du script. Pour plus d'informations sur les scripts, reportez-vous à "Scripts sur un support de démarrage" (p. 996).
10. [Facultatif] Sélectionnez le mode d'enregistrement du support de démarrage dans le service Cyber Protection lors du démarrage. Pour plus d'informations sur les paramètres d'enregistrement, reportez-vous à "Enregistrement du support de démarrage" (p. 1005).
11. Spécifiez les paramètres réseau des adaptateurs réseau de l'ordinateur démarré ou gardez la configuration DHCP automatique.
12. [Facultatif] Si un serveur proxy est activé sur votre réseau, spécifiez son nom d'hôte/adresse IP et le port.
13. [Facultatif] Pour spécifier la méthode d'authentification de mise en réseau, cliquez sur **Paramètres Wi-Fi**, puis sélectionnez l'une des options suivantes :
    - Authentification ouverte
    - WEP
    - WEP partagé
    - IEEE 802.1X
    - WPA Personal
    - WPA Enterprise
    - WPA2 Personal
    - WPA2 Enterprise
14. Sélectionnez le type de fichier du support de démarrage :
    - Image ISO
    - Fichier ZIP
15. Spécifiez un nom de fichier pour le fichier de support de démarrage.
16. Vérifiez vos paramètres sur l'écran Résumé et cliquez sur **Poursuivre**.

Paramètres du noyau

Vous pouvez spécifier un ou plusieurs paramètres du noyau Linux qui seront automatiquement appliqués au lancement du support de démarrage. Ces paramètres sont généralement utilisés en cas de problème d'utilisation du support de démarrage. Normalement, vous pouvez laisser ce champ vide.

Vous pouvez également spécifier n'importe lequel de ces paramètres en appuyant sur F11 dans le menu de démarrage.

Paramètres

Lorsque vous spécifiez plusieurs paramètres, séparez-les avec des espaces.

© Acronis International GmbH, 2003-2026

- **acpi=off**

  Désactive ACPI (Advanced Configuration and Power Interface). Vous pouvez utiliser ce paramètre lorsque vous rencontrez un problème avec une configuration matérielle spécifique.
- **noapic**

  Désactive APIC (Advanced Programmable Interrupt Controller). Vous pouvez utiliser ce paramètre lorsque vous rencontrez un problème avec une configuration matérielle spécifique.
- **vga=ask**

  Invite à spécifier le mode vidéo que doit utiliser l'interface graphique utilisateur du support de démarrage. Sans le paramètre **vga**, le mode vidéo est détecté automatiquement.
- **vga=** *mode_number*

  Spécifie le mode vidéo à utiliser dans l'interface utilisateur graphique du support de démarrage. Le numéro de mode est donné par *mode_number* sous forme hexadécimale, par exemple : **vga=0x318**

  La résolution de l'écran et le nombre de couleurs correspondant à un numéro de mode peuvent être différents sur des ordinateurs différents. Nous vous recommandons de commencer par utiliser le paramètre **vga=ask** afin de choisir une valeur pour *numéro_mode*.
- **quiet**

  Désactive l'affichage des messages de démarrage quand le noyau Linux est en cours de chargement, et démarre la console d'administration dès que le noyau est chargé.

  Ce paramètre est implicitement spécifié lors de la création du support de démarrage, mais vous pouvez le supprimer dans le menu de démarrage.

  Si ce paramètre est supprimé, tous les messages de démarrage s'affichent, suivis d'une invite de commandes. Pour démarrer la console de gestion à partir de l'invite de commandes, exécutez la commande suivante : **/bin/product**
- **nousb**

  Désactive le chargement du sous-système USB (Universal Serial Bus).
- **nousb2**

  Désactive la prise en charge USB 2.0. Ce paramètre n'affecte pas le fonctionnement des périphériques USB 1.1. Ce paramètre vous permet d'utiliser certains lecteurs USB en mode USB 1.1 s'ils ne fonctionnent pas en mode USB 2.0.
- **nodma**

  Désactive l'accès direct à la mémoire (DMA) pour tous les disques durs IDE. Empêche le noyau de se figer pour certains matériels.
- **nofw**

  Désactive la prise en charge de l'interface FireWire (IEEE1394).
- **nopcmcia**

  Désactive la détection du matériel PCMCIA.
- **nomouse**

  Désactive la prise en charge de la souris.
- *module_name* **=off**

© Acronis International GmbH, 2003-2026

Désactive le module dont le nom est donné par *module_name*. Par exemple, pour désactiver l'utilisation du module SATA, saisissez : **sata_sis=off**

- **pci=bios**

  Force l'utilisation du BIOS PCI au lieu d'accéder directement au terminal matériel. Vous pouvez utiliser ce paramètre si la machine possède un pont d'hôte PCI non standard.
- **pci=nobios**

  Désactive l'utilisation du BIOS PCI. Seules les méthodes d'accès direct au matériel seront autorisées. Vous pouvez utiliser ce paramètre quand le support de démarrage ne démarre pas, ce qui peut être causé par le BIOS.
- **pci=biosirq**

  Utilise des appels BIOS PCI pour obtenir la table de routage d'interruptions Vous pouvez utiliser ce paramètre si le noyau ne parvient pas à allouer les requêtes d'interruption (IRQ) ou à découvrir les bus PCI secondaires sur la carte-mère.

  Il se peut que ces appels ne fonctionnent pas correctement sur certaines machines. Mais ceci pourrait être la seule façon d'obtenir la table de routage d'interruptions.
- **STRUCTURES=en-US, de-DE, fr-FR, ...**

  Spécifie la structure du clavier qui peut être utilisée dans l'interface utilisateur graphique du support de démarrage.

  Sans ce paramètre, seules deux structures peuvent être utilisées : Anglais (USA) et la structure correspondant à la langue sélectionnée dans le menu de démarrage de votre support.

  Vous pouvez indiquer l'une des structures suivantes :

  Belge : **be-BE**

  Tchèque : **cz-CZ**

  Anglais : **en-GB**

  Anglais (USA) : **en-US**

  Français : **fr-FR**

  Français (Suisse) : **fr-CH**

  Allemand : **de-DE**

  Allemand (Suisse) : **de-CH**

  Italien : **it-IT**

  Polonais : **pl-PL**

  Portugais : **pt-PT**

  Portugais (Brésil) : **pt-BR**

  Russe : **ru-RU**

  Serbe (cyrillique) : **sr-CR**

  Serbe (latin) : **sr-LT**

  Espagnol : **es-ES**

  En cas d'utilisation avec le support de démarrage, utilisez CTRL + SHIFT pour parcourir les structures disponibles.

© Acronis International GmbH, 2003-2026

Scripts sur un support de démarrage

Si vous voulez que le support de démarrage exécute un ensemble prédéfini d'opérations, vous pouvez spécifier un script lors de la création du support avec Bootable Media Builder. Ainsi, chaque fois qu'un ordinateur démarrera à partir du support, le script spécifié sera exécuté et l'interface utilisateur ne s'affichera pas.

Vous pouvez sélectionner l'un des scripts prédéfinis ou créer un script personnalisé en suivant les conventions de script.

Scripts prédéfinis

Le support de démarrage fournit les scripts prédéfinis suivants :

- Restauration du stockage dans le Cloud (**entire_pc_cloud**)
- Restauration depuis un partage réseau (**entire_pc_share**)

Les scripts se trouvent dans les répertoires suivants sur l'ordinateur où Bootable Media Builder est installé :

- Sous Windows : %**ProgramData%\Acronis\MediaBuilder\scripts**
- Sous Linux : **/var/lib/Acronis/MediaBuilder/scripts/**

Restauration du stockage Cloud

Dans le support de démarrage, spécifiez les paramètres de script suivants :

1. Le nom du fichier de sauvegarde.
2. [Facultatif] Un mot de passe que le script utilisera pour accéder aux sauvegardes chiffrées.

Restauration depuis un partage réseau

Dans le support de démarrage, spécifiez les paramètres de script suivants :

- Le chemin d'accès au partage réseau.
- Les nom d'utilisateur et mot de passe du partage réseau.
- Le nom du fichier de sauvegarde. Pour trouver le nom du fichier de sauvegarde :
  a. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Emplacements**.
  b. Sélectionnez le partage réseau (cliquez sur **Ajouter un emplacement** si le partage n'est pas répertorié).
  c. Sélectionnez la sauvegarde.
  d. Cliquez sur **Détails**. Le nom du fichier s'affiche sous **Nom de fichier de la sauvegarde**.
- [Facultatif] Un mot de passe que le script utilisera pour accéder aux sauvegardes chiffrées.

© Acronis International GmbH, 2003-2026

Important
La création de scripts personnalisés requiert la connaissance du langage de commande Bash et de JavaScript Object Notation (JSON). Si vous ne connaissez pas Bash, il existe un bon site pour le découvrir : http://www.tldp.org/LDP/abs/html. La spécification JSON est disponible à l'adresse http://www.json.org

Fichiers d'un script

Votre Un script doit se trouver dans les répertoires suivants sur la machine où Bootable Media Builder est installé :

- Sous Windows : %**ProgramData%\Acronis\MediaBuilder\scripts**
- Sous Linux : **/var/lib/Acronis/MediaBuilder/scripts/**

Le script doit être composé d'au moins trois fichiers :

- **<script_file>.sh** : fichier avec votre script Bash. Lors de la création du script, utilisez uniquement un ensemble limité de commandes, que vous trouverez à l'adresse : https://busybox.net/downloads/BusyBox.html. Les commandes suivantes peuvent également être utilisées :
  - `acrocmd` : utilitaire de ligne de commande pour la sauvegarde et la restauration
  - `product` : commande qui lance l'interface utilisateur du support de démarrage

  Ce fichier et tous les fichiers supplémentaires inclus dans le script (par exemple, en utilisant la commande dot) doivent être situés dans le sous-dossier **bin**. Dans ce script, indiquez les chemins de fichier supplémentaires sous la forme **/ConfigurationFiles/bin/<some_file>**.
- **autostart** : fichier pour démarrer **<script_file>.sh**. Le contenu du fichier doit être comme suit :

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** : fichier JSON contenant les éléments suivants :
  - Nom et description du script à afficher dans Bootable Media Builder.
  - Noms des variables de script à configurer via Bootable Media Builder.
  - Paramètres des contrôles qui seront affichés dans le support de démarrage pour chaque variable.

© Acronis International GmbH, 2003-2026

Structure d'autostart.json

Objet Toplevel

Paire		Requis	Description
Nom	**Type de valeur**		
`displayName`	string	Oui	Nom du script affiché dans le support de démarrage.
`description`	string	Non	Description du script affiché dans le support de démarrage.
`timeout`	number	Non	Délai d'expiration (en secondes) pour le menu de démarrage avant de lancer le script. Si la paire n'est pas indiquée, le délai d'expiration sera de dix secondes.
`variables`	objet	Non	Toute variable pour **<script_file>.sh** que vous voulez configurer via le support de démarrage. La valeur doit être un ensemble des paires suivantes : l'identificateur de chaîne d'une variable et l'objet de la variable (voir tableau ci-dessous).

Objet de variable

Paire		Requis	Description
Nom	**Type de valeur**		
`displayName`	string	Oui	Nom de variable utilisé dans **<script_file>.sh**.
`type`	string	Oui	Type de contrôle affiché dans le support de démarrage. Ce contrôle est utilisé pour configurer la valeur de la variable. Pour connaître tous les types pris en charge, consultez le tableau ci-dessous.
`description`	string	Oui	Étiquette de contrôle affichée au-dessus du contrôle dans le support de démarrage.
`default`	chaîne si `type` est `string`, `multiString`, `password` ou	Non	Valeur par défaut du contrôle. Si la paire n'est pas indiquée, la valeur par défaut sera une chaîne vide ou un zéro en fonction du type de contrôle. La valeur par défaut d'une case à cocher peut être `0`

© Acronis International GmbH, 2003-2026

	`enum` nombre si `type` est `number`, `spinner` ou `checkbox`		(l'état effacé) ou `1` (l'état sélectionné).
`order`	number (non négatif)	Oui	Ordre de contrôle dans le support de démarrage. Plus la valeur est élevée, plus le contrôle est placé bas par rapport aux autres contrôles définis dans **autostart.json**. La valeur initiale doit être `0`.
`min` (pour `spinner` uniquement)	number	Non	Valeur minimale de la toupie dans une zone de sélection numérique. Si la paire n'est pas indiquée, la valeur sera `0`.
`max` (pour `spinner` uniquement)	number	Non	Valeur minimale de la toupie dans une zone de sélection numérique. Si la paire n'est pas indiquée, la valeur sera `100`.
`step` (pour `spinner` uniquement)	number	Non	Valeur de pas de la toupie dans une zone de sélection numérique. Si la paire n'est pas indiquée, la valeur sera `1`.
`items` (pour `enum` uniquement)	grappe de chaînes	Oui	Valeurs d'une liste déroulante.
`required` (pour `string`, `multiString`, `password` et `enum`)	number	Non	Indique si la valeur de contrôle peut être vide (`0`) ou non (`1`). Si la paire n'est pas indiquée, la valeur de contrôle peut être vide.

Type de contrôle

Nom	Description
`string`	Zone de texte sans contrainte d'une seule ligne, utilisée pour saisir ou modifier des chaînes courtes.
`multiString`	Zone de texte sans contrainte de plusieurs lignes, utilisée pour saisir ou modifier des chaînes longues.
`password`	Zone de texte sans contrainte d'une seule ligne, utilisée pour saisir des mots de passe en toute sécurité.

© Acronis International GmbH, 2003-2026

number	Zone de texte numérique uniquement et d'une seule ligne, utilisée pour saisir ou modifier des nombres.
spinner	Zone de texte numérique uniquement et d'une seule ligne, utilisée pour saisir ou modifier des nombres, avec une toupie. Également appelée zone de sélection numérique.
enum	Liste déroulante standard, avec un ensemble fixe de valeurs prédéterminées.
checkbox	Case à cocher avec deux états : l'état effacé ou l'état sélectionné.

L'échantillon **autostart.json** ci-dessous contient tous les types possibles de contrôle pouvant être utilisés pour configurer des variables pour **<script_file>.sh**.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type": "string", "order": 1,
                        "description": "This is a 'string' control:", "default": "Hello,
world!"
                },
                "var_multistring": {
                        "displayName": "VAR_MULTISTRING",
                        "type": "multiString", "order": 2,
                        "description": "This is a 'multiString' control:",
                        "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName": "VAR_NUMBER",
                        "type": "number", "order": 3,
                        "description": "This is a 'number' control:", "default": 10
                },
                "var_spinner": {
                        "displayName": "VAR_SPINNER",
```


© Acronis International GmbH, 2003-2026

```
                "type": "spinner", "order": 4,
                "description": "This is a 'spinner' control:",
                "min": 1, "max": 10, "step": 1, "default": 5
            },
            "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
            },
            "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
                "description": "This is a 'password' control:", "default": "qwe"
            },
            "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "This is a 'checkbox' control", "default": 1
            }
        }
}
```

Support de démarrage basé sur Windows

Vous pouvez créer des images WinRE sans préparation supplémentaire, ou créer des images WinPE après avoir installé le kit d'installation automatisée Windows (AIK) ou le kit de déploiement et d'évaluation Windows (ADK).

Images WinRE

La création d'images WinRE est prise en charge pour les systèmes d'exploitation suivants :

- Windows 7 (64 bits)
- Windows 8 (32 bits et 64 bits)

© Acronis International GmbH, 2003-2026

- Windows 8.1 (32 bits et 64 bits)
- Windows 10 (32 bits et 64 bits)
- Windows 11 (64 bits)
- Windows Server 2012 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)
- Windows Server 2022 (64 bits)
- Windows Server 2025 (64 bits)

Images WinPE

Après l'installation du kit d'installation automatisée Windows (AIK) ou du kit de déploiement et d'évaluation Windows (ADK), Bootable Media Builder prend en charge les distributions WinPE qui sont basées sur n'importe lequel des noyaux suivants :

- Windows Vista (PE 2.0)
- Windows Vista SP1 et Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) avec ou sans le supplément pour Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder prend en charge les distributions WinPE 32 bits et 64 bits. Les distributions WinPE 32 bits peuvent également fonctionner sur un matériel 64 bits. Cependant, vous avez besoin d'une distribution 64 bits pour démarrer une machine qui utilise le Unified Extensible Firmware Interface (UEFI).

Création d'un support de démarrage WinPE ou WinRE

Bootable Media Builder offre deux méthodes pour intégrer Cyber Protection avec WinPE et WinRE :

- Création d'un fichier ISO avec le plug-in Cyber Protection à partir de zéro.
- Ajout du plug-in Cyber Protection à un fichier WIM pour n'importe quel usage ultérieur (création manuelle d'ISO, ajout d'autres outils à l'image et ainsi de suite).

Pour créer un support de démarrage WinPE ou WinRE

1. Sur l'ordinateur sur lequel l'agent de protection est installé, exécutez Bootable Media Builder.
2. Dans **Bootable media type**, sélectionnez **Windows PE** ou **Windows PE (64-bit)**. Un support 64 bits est nécessaire pour démarrer une machine qui utilise l'interface micrologicielle extensible unifiée (Unified Extensible Firmware Interface) (UEFI).

© Acronis International GmbH, 2003-2026

3. Sélectionnez le sous-type du support de démarrage : **WinRE** ou **WinPE**.

   La création d'un support de démarrage WinRE ne nécessite l'installation d'aucun paquet supplémentaire.

   Pour créer un support WinPE 64 bits, vous devez télécharger le kit d'installation automatisée Windows (AIK) ou le kit de déploiement et d'évaluation Windows (ADK). Pour créer un support WinPE 32 bits, en plus de télécharger le kit AIK ou ADK, vous devez procéder comme suit :

   a. Cliquez sur **Télécharger le plug-in pour WinPE (32 bits)**.

   b. Enregistrez le plug-in à l'emplacement **%PROGRAM_ FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Facultatif] Sélectionnez la langue du support de démarrage.
5. [Facultatif] Sélectionnez le mode de démarrage (BIOS ou UEFI) que Windows utilisera après la restauration.
6. Spécifiez les paramètres réseau des adaptateurs réseau de l'ordinateur démarré ou gardez la configuration DHCP automatique.
7. [Facultatif] Sélectionnez le mode d'enregistrement du support de démarrage dans le service Cyber Protection lors du démarrage. Pour plus d'informations sur les paramètres d'enregistrement, reportez-vous à "Enregistrement du support de démarrage" (p. 1005).
8. [Facultatif] Spécifiez les pilotes Windows à ajouter au support de démarrage.

   Après avoir démarré un ordinateur avec Windows PE ou Windows RE, les pilotes peuvent vous aider à accéder au terminal où se trouve la sauvegarde. Ajoutez les pilotes 32 bits si vous utilisez une distribution WinPE ou WinRE 32 bits ou les pilotes 64 bits si vous utilisez une distribution WinPE ou WinRE 64 bits.

   Pour ajouter des pilotes :

   - Cliquez sur **Ajouter** et spécifiez le chemin d'accès au fichier .inf correspondant à un contrôleur SCSI, RAID, SATA, à un adaptateur réseau, ou à tout autre périphérique.
   - Répétez cette procédure pour chaque pilote que vous souhaitez inclure dans le support WinPE ou WinRE obtenu.
9. Sélectionnez le type de fichier du support de démarrage :
   - Image ISO
   - Image WIM
10. Indiquez le chemin complet au fichier image obtenu, y compris le nom de fichier.
11. Vérifiez vos paramètres sur l'écran Résumé et cliquez sur **Poursuivre**.

Pour créer une image PE (fichier ISO) à partir du fichier WIM obtenu

- Remplacez le fichier boot.wim par défaut dans votre dossier Windows PE par le fichier WIM nouvellement créé. Pour l'exemple ci-dessus, saisissez :

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Utiliser l'outil **Oscdimg**. Pour l'exemple ci-dessus, saisissez :

© Acronis International GmbH, 2003-2026

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Avertissement !
Ne pas copier/coller cet exemple. Pour qu'elle fonctionne, saisissez manuellement la commande.

Préparation : WinPE 2.x et 3.x

Pour pouvoir créer ou modifier des images PE 2.x ou 3.x, installez Bootable Media Builder et Windows Automated Installation Kit (AIK) sur le même ordinateur.

Pour préparer un ordinateur

1. Téléchargez le fichier image AIK à partir du site Web de Microsoft, comme suit :
   - Pour Windows Vista (PE 2.0) : https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - Pour Windows Vista SP1 et Windows Server 2008 (PE 2.1) : https://www.microsoft.com/fr-fr/download/details.aspx?id=9085
   - Pour Windows 7 (PE 3.0) : https://www.microsoft.com/fr-fr/download/details.aspx?id=5753
     Pour Windows 7 SP1 (PE 3.1), vous avez également besoin du supplément AIK disponible à l'adresse https://www.microsoft.com/fr-fr/download/details.aspx?id=5188.
2. Gravez le fichier image sur un disque DVD ou une clé USB.
3. À partir du fichier image, installez les éléments suivants :
   - Microsoft .NET Framework (NETFXx86 ou NETFXx64, en fonction de votre matériel)
   - MSXML (analyseur XML de Microsoft)
   - Windows AIK
4. Installez Bootable Media Builder sur la même machine.

Préparation : WinPE 4.0 et versions ultérieures

Pour pouvoir créer ou modifier des images PE 4 ou ultérieures, installez Bootable Media Builder et Windows Assessment and Deployment Kit (ADK) sur le même ordinateur.

Pour préparer un ordinateur

1. Téléchargez le programme d'installation ADK à partir du site Web de Microsoft.
   Les versions suivantes de Windows sont prises en charge :
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Installez le kit d'évaluation et de déploiement.
3. Installez Bootable Media Builder.

© Acronis International GmbH, 2003-2026

Enregistrement du support de démarrage

L'enregistrement du support de démarrage auprès du service Cyber Protection vous permet d'accéder au stockage dans le Cloud pour vos sauvegardes. Vous pouvez préconfigurer l'enregistrement lors de la création du support de démarrage. Si l'enregistrement n'est pas préconfiguré, vous pouvez enregistrer le support après l'avoir utilisé pour démarrer un ordinateur.

Pour préconfigurer l'enregistrement auprès du service Cyber Protection

1. Dans Bootable Media Builder, accédez à **Enregistrement du support de démarrage**.
2. Dans **URL du service**, spécifiez l'adresse du service Cyber Protection.
3. [Facultatif] Dans **Nom d'affichage**, spécifiez un nom pour l'ordinateur démarré.
4. Pour définir l'enregistrement automatique dans le service Cyber Protection, cochez la case **Enregistrer automatiquement le support de démarrage**, puis sélectionnez le niveau d'enregistrement automatique :
   - **Demander le jeton d'enregistrement lors du démarrage**
     Le jeton doit être fourni chaque fois qu'un ordinateur démarre à partir de ce support de démarrage.
   - **Utiliser le jeton suivant**
     L'ordinateur est enregistré automatiquement lorsqu'il démarre à partir du support de démarrage.

Pour enregistrer le support de démarrage après l'avoir utilisé pour démarrer un ordinateur

1. Démarrez la machine à partir du support de démarrage.
2. Dans la fenêtre de démarrage, cliquez sur **Enregistrer le support**.
3. Dans **Serveur**, spécifiez l'adresse du service Cyber Protection.
4. Dans **Jeton d'enregistrement**, saisissez le jeton d'enregistrement.
5. Cliquez sur **Enregistrer**.

Paramètres réseau

Lors de la création d'un support de démarrage, vous pouvez préconfigurer les connexions réseau qui seront utilisées par l'agent de démarrage. Les paramètres suivants peuvent être préconfigurés :

- Adresse IP
- Masque de sous-réseau
- Passerelle
- Serveur DNS
- Serveur WINS

© Acronis International GmbH, 2003-2026

Une fois que l'agent de démarrage a démarré sur un ordinateur, sa configuration est appliquée sur la carte réseau (Network Interface Card - NIC) de l'ordinateur. Si les paramètres n'ont pas été préconfigurés, l'agent utilise la configuration automatique DHCP.

Vous pouvez aussi configurer les paramètres réseau manuellement lorsque l'agent de démarrage est en cours d'exécution sur l'ordinateur.

Préconfiguration de plusieurs connexions réseau

Vous pouvez préconfigurer les paramètres TCP/IP pour dix cartes réseau au maximum. Pour vous assurer que les paramètres appropriés seront affectés à chaque NIC, créez le support sur le serveur pour lequel le support est personnalisé. Lorsque vous sélectionnez une carte réseau existante dans la fenêtre de l'assistant, ses paramètres sont sélectionnés et enregistrés sur le support. L'adresse MAC de chaque NIC existante est également enregistrée sur le support.

Vous pouvez modifier les paramètres, sauf l'adresse MAC, ou configurer les paramètres pour une carte réseau inexistante.

Une fois que l'agent de démarrage a démarré sur le serveur, il récupère la liste des cartes réseau disponibles. La liste est classée en fonction du logement occupé par les cartes réseau : la plus proche du processeur est en haut.

L'agent de démarrage affecte les paramètres appropriés à chaque carte réseau connue, et identifie les cartes réseau par leur adresse MAC. Une fois que les cartes réseau ayant une adresse MAC connue sont configurées, les paramètres que vous avez créés pour les cartes réseau inexistantes sont affectés aux cartes réseau restantes en commençant par la carte réseau la plus haute.

Vous pouvez personnaliser le support de démarrage pour n'importe quel ordinateur, et pas seulement pour l'ordinateur sur lequel le support est créé. Pour cela, configurez les NIC en fonction de l'ordre de leur case sur cette machine : NIC1 occupe le logement le plus proche du processeur, NIC2 est dans le logement suivant et ainsi de suite. Lorsque l'agent de démarrage démarrera sur cet ordinateur, il ne trouvera pas de carte réseau ayant une adresse MAC connue et il configurera les cartes réseau dans le même ordre que vous l'avez fait précédemment.

Exemple

L'agent de démarrage pourrait utiliser l'un des adaptateurs réseau pour la communication avec la console de gestion au travers du réseau de production. Une configuration automatique peut être effectuée pour cette connexion. Une quantité assez importante de données à restaurer peut être transférée à travers la seconde carte réseau, incluse dans le réseau de sauvegarde dédié au moyen de paramètres TCP/IP statiques.

© Acronis International GmbH, 2003-2026

Connexion à un ordinateur démarré à partir d'un support de démarrage

Connexion locale

Pour travailler directement sur la machine démarrée à partir du support de démarrage, cliquez sur **Gérer cette machine localement** dans la fenêtre de démarrage.

Quand un ordinateur est démarré à partir d'un support de démarrage, le terminal de l'ordinateur affiche une fenêtre système avec les adresses IP obtenues à partir de DHCP ou configurées à partir de valeurs préétablies.

Configuration des paramètres réseau

Pour modifier les paramètres réseau pour une session en cours, cliquez sur **Configurer le réseau** dans la fenêtre de démarrage. La fenêtre **Paramètres réseau** vous permet de configurer les paramètres réseau pour chaque carte réseau (NIC) de l'ordinateur.

Les modifications apportées pendant une session seront perdues après le redémarrage de l'ordinateur.

Ajout de VLAN

Dans la fenêtre **Paramètres réseau**, vous pouvez ajouter des réseaux locaux virtuels (VLAN). Utilisez cette fonctionnalité si vous devez accéder à un emplacement de sauvegarde qui est inclus dans un VLAN spécifique.

Les VLAN sont principalement utilisés pour diviser un réseau local en plusieurs segments. Une carte d'interface réseau qui est connectée à un port *d'accès* du commutateur a toujours accès au VLAN spécifié dans la configuration du port. Une carte réseau connectée à un port en mode *trunk* du commutateur peut accéder aux VLAN autorisés dans la configuration du port uniquement si vous spécifiez les VLAN dans les paramètres réseau.

Pour activer l'accès à un VLAN via un port en mode trunk

1. Cliquez sur **Ajouter un VLAN**.
2. Sélectionnez la carte réseau qui donne accès au réseau local qui inclut le VLAN requis.
3. Spécifiez l'identificateur du VLAN.

Après avoir cliqué sur **OK**, une nouvelle entrée apparaît dans la liste des cartes réseau.

Si vous devez supprimer un VLAN, cliquez sur l'entrée VLAN, puis cliquez sur **Supprimer le VLAN**.

Opérations locales avec support de démarrage

Les opérations avec le support de démarrage sont semblables aux opérations de restauration exécutées sur un système d'exploitation en cours d'exécution. Les différences sont les suivantes :

© Acronis International GmbH, 2003-2026

1. Sous un support de démarrage avec représentation des volumes de type Windows, un volume a la même lettre de lecteur que sous Windows. Pour les volumes qui n'ont pas de lettre de lecteur sous Windows (comme le volume System Reserved), des lettres sont affectées librement dans leur ordre séquentiel sur le disque.

   Si le support de démarrage ne peut pas détecter Windows sur l'ordinateur ou s'il en détecte plusieurs, tous les volumes, y compris ceux sans lettre de lecteur, reçoivent une lettre dans leur ordre de séquence sur le disque. Par conséquent, les lettres des volumes peuvent différer de celles affichées dans Windows. Par exemple, le lecteur D: sous le support de démarrage peut correspondre au lecteur E: dans Windows.

   Remarque
   Il est conseillé d'assigner des noms uniques aux volumes.

2. Le support de démarrage avec une représentation des volumes de type Linux affiche les disques et volumes locaux comme n'étant pas montés (sda1, sda2...).
3. Les tâches ne peuvent pas être planifiées. Si vous devez répéter une opération, configurez-la de toutes pièces.
4. La durée de vie du journal est limitée à la durée de la session actuelle. Vous pouvez enregistrer le journal entier ou les entrées de journal filtrées dans un fichier.

Définition d'un mode d'affichage

Lorsque vous démarrez un ordinateur à partir d'un support de démarrage Linux, un mode d'affichage vidéo est détecté automatiquement en fonction de la configuration matérielle (spécifications du moniteur et de la carte graphique). Si le mode d'affichage vidéo est incorrectement détecté, procédez comme suit :

1. Lors de l'affichage du menu de démarrage, appuyez sur F11.
2. Dans l'interface de ligne de commande, saisissez **vga=ask**, puis continuez le démarrage.
3. Choisissez le mode vidéo approprié pris en charge à partir de la liste en entrant son numéro (**318**, par exemple), puis appuyez sur **Entrée**.

Si vous ne souhaitez pas suivre cette procédure à chaque démarrage d'une configuration matérielle donnée, recréez le support de démarrage avec le numéro de mode approprié (dans notre exemple, **vga=0x318**) spécifié dans le champ **Paramètres du noyau**.

Restauration des données à l'aide d'un support de démarrage local

L'exécution du support de démarrage nécessite 1,5 Go de RAM.

Pour restaurer des données à l'aide d'un support de démarrage local

1. Démarrez votre ordinateur à partir du support de démarrage.
2. Cliquez sur **Gérer cette machine localement**.
3. Cliquez sur **Restaurer**.

© Acronis International GmbH, 2003-2026

4. Dans **Quoi restaurer**, cliquez sur **Sélectionner les données**.
5. Sélectionnez l'archive de sauvegarde à restaurer.
6. Dans le volet inférieur gauche, sélectionnez les lecteurs/volumes (ou fichiers/dossiers) que vous souhaitez restaurer, puis cliquez sur **OK**.
7. Configurez les règles d'écrasement.
8. Configurez les exclusions de restauration.
9. Configurez les options de restauration.
10. Vérifiez que les paramètres sont corrects, puis cliquez sur **OK**.

Opérations à distance avec un support de démarrage

Pour voir le support de démarrage dans la console Cyber Protect, vous devez d'abord l'enregistrer en suivant les indications de "Enregistrement du support de démarrage" (p. 1005).

Une fois le support enregistré dans la console Cyber Protect, il apparaît dans l'onglet **Terminaux** > **Support de démarrage**. Un support de démarrage disparaît de cet onglet lorsqu'il est hors ligne depuis plus de 30 jours.

Vous pouvez gérer le support de démarrage à distance dans la console Cyber Protect. Par exemple, vous pouvez restaurer des données, redémarrer ou arrêter l'ordinateur démarré avec le support, ou encore afficher des informations, des activités et des alertes concernant le support.

L'exécution du support de démarrage nécessite 1,5 Go de RAM.

Important

- L'opération à distance avec un support de démarrage n'est pas prise en charge avec les volumes LVM/LDM.
- Vous ne pouvez pas mettre à jour le support de démarrage à distance, depuis l'onglet **Paramètres** > **Agents** de la console Cyber Protect.

  Pour mettre à jour le support de démarrage, créez-en un nouveau en suivant les indications de la section "Bootable Media Builder" (p. 992). Vous pouvez également télécharger le support tout prêt en cliquant sur l'icône de votre compte, puis sur **Téléchargements** > **Support de démarrage** dans la console Cyber Protect.

Pour restaurer à distance des fichiers ou des dossiers à l'aide d'un support de démarrage

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Support de démarrage**.
2. Sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
3. Cliquez sur **Restauration**.
4. Sélectionnez l'emplacement, puis la sauvegarde dont vous avez besoin. Vous remarquerez que les sauvegardes sont filtrées en fonction de leur emplacement.
5. Sélectionnez le point de restauration, puis cliquez sur **Restaurer des fichiers/dossiers**.

© Acronis International GmbH, 2003-2026

6. Accédez au dossier requis ou servez-vous de la barre de recherche pour obtenir la liste des fichiers et dossiers requis.
   La recherche ne dépend pas de la langue.
   Vous pouvez utiliser un ou plusieurs caractères génériques (* et ?). Pour plus de détails sur l'utilisation de caractères génériques, voir "Filtres de fichiers (Inclusions/Exclusions)" (p. 620).
7. Cliquez sur les fichiers que vous souhaitez restaurer, puis sur **Restaurer**.
8. Dans **Chemin d'accès**, sélectionnez la destination de la restauration.
9. [Facultatif] Pour définir la configuration avancée de la restauration, cliquez sur **Options de restauration**. Pour obtenir plus d'informations, consultez l'article "Options de restauration" (p. 721).
10. Cliquez sur **Démarrer la restauration**.
11. Sélectionnez l'une des options d'écrasement de fichier :
    - **Écraser les fichiers existants**
    - **Écraser un fichier existant s'il est plus ancien**
    - **Ne pas écraser les fichiers existants**
12. Choisissez si vous souhaitez redémarrer automatiquement la machine.
13. Cliquez sur **Poursuivre** pour lancer la restauration.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Pour restaurer à distance des disques, volumes, ou ordinateurs complets à l'aide d'un support de démarrage

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Restauration**.
3. Sélectionnez l'emplacement, puis la sauvegarde dont vous avez besoin. Vous remarquerez que les sauvegardes sont filtrées en fonction de leur emplacement.
4. Sélectionnez le point de restauration, puis cliquez sur **Restaurer** > **Toute la machine**.
   Si nécessaire, configurez la machine cible et le mappage de volume en suivant les indications de "Restauration de machines physiques" (p. 674).
5. Pour définir la configuration avancée de la restauration, cliquez sur **Options de restauration**. Pour obtenir plus d'informations, consultez l'article "Options de restauration" (p. 721).
6. Cliquez sur **Démarrer la restauration**.
7. Confirmez que vous souhaitez écraser les données du disque avec leurs versions sauvegardées. Choisissez si vous souhaitez redémarrer automatiquement la machine.

Vous pouvez vérifier la progression de la restauration dans la console Cyber Protect, dans l'onglet **Activités**.

Pour redémarrer à distance l'ordinateur démarré

© Acronis International GmbH, 2003-2026

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Redémarrer**.
3. Confirmez que vous souhaitez redémarrer l'ordinateur démarré avec le support.

Pour arrêter à distance l'ordinateur démarré

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Arrêt du système**.
3. Confirmez que vous souhaitez arrêter l'ordinateur démarré avec le support.

Pour afficher les informations concernant le support de démarrage

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Détails**, **Activités** ou **Alertes** pour voir les informations correspondantes.

Pour supprimer à distance le support de démarrage

1. Dans l'onglet **Terminaux**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Supprimer** pour supprimer le support de démarrage de la console Cyber Protect.
3. Confirmez que vous souhaitez supprimer le support de démarrage.

Prise en charge de l'agrégation de cartes réseau

L'agrégation (bonding) des cartes d'interface réseau (NIC) est conservée à la fois pendant la restauration d'une ressource avec des NIC agrégées, et après la restauration.

Remarque
La configuration réseau, y compris l'agrégation de cartes réseau (NIC), n'est pas conservée lorsque vous restaurez sur un matériel différent.

Vous pouvez désactiver l'agrégation de cartes réseau (NIC) pendant la restauration si vous restaurez une ressource de l'une des manières suivantes :

- Avec le support de démarrage téléchargé
- Avec un support de démarrage Linux créé dans Bootable Media Builder
- Via Acronis Startup Recovery Manager
- Via la restauration en un clic
- Via la restauration avec redémarrage, en utilisant l'environnement de restauration Linux

Pour désactiver l'agrégation de cartes réseau (NIC) pendant la restauration

© Acronis International GmbH, 2003-2026

1.

   Sur l'ordinateur sauvegardé, ouvrez le fichier de configuration suivant pour le modifier :

   - Windows :

     ```
     C:\Program Files\Common Files\Acronis\BackupAndRecoveryAgent\bootagent_
     msp64.config
     ```

   - Linux :

     ```
     /usr/lib/Acronis/BackupAndRecoveryAgent/bootagent_msp64.config
     ```

2.

   Dans le fichier de configuration, repérez la ligne suivante :

   - Windows :

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent media_for_windows"
     target="abr64ker.dat"/>
     ```

   - Linux :

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent media_for_linux"
     target="abr64ker.dat"/>
     ```

3. Modifiez la ligne comme suit :

   - Windows

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent DONT_CREATE_BONDING=1
     media_for_windows" target="abr64ker.dat"/>
     ```

   - Linux

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent DONT_CREATE_BONDING=1
     media_for_linux" target="abr64ker.dat"/>
     ```

4. Enregistrez le fichier de configuration.
5. Restaurez la ressource en utilisant l'une des méthodes prises en charge.

Par conséquent, l'agrégation des cartes réseau (NIC) ne sera pas utilisée pendant la restauration.

Remarque
La ressource restaurée conserve l'agrégation des cartes réseau (NIC). Pour désactiver l'agrégation des cartes réseau après la restauration, reconfigurez les paramètres réseau de la ressource.

Startup Recovery Manager

Startup Recovery Manager est un composant amorçable qui réside sur le disque dur. Avec Startup Recovery Manager, vous pouvez lancer l'utilitaire de secours amorçable sans utiliser de support d'amorçage distinct.

© Acronis International GmbH, 2003-2026

En cas d'échec, redémarrez l'ordinateur, attendez que le message **Appuyez sur F11 pour Acronis Startup Recovery Manager** apparaisse, puis appuyez sur F11 ou sélectionnez Startup Recovery Manager dans le menu de démarrage (si vous utilisez le chargeur de démarrage GRUB). Startup Recovery Manager démarre et vous pouvez effectuer une restauration.

Startup Recovery Manager est pris en charge pour les ordinateurs Windows et Linux.

Important
L'activation de Startup Recovery Manager sur un ordinateur dont le volume système est chiffré nécessite au moins un volume non chiffré sur le même ordinateur.

Espace disque nécessaire

Startup Recovery Manager nécessite de l'espace disque pour les fichiers temporaires. Les exigences varient en fonction de l'ordinateur sur lequel Startup Recovery Manager est activé.

Le tableau ci-dessous résume les options disponibles.

Mode de démarrage	Ordinateur sans Secure Zone		Ordinateur avec Secure Zone
	Avec un volume système non chiffré	Avec un volume système chiffré	Avec un volume système chiffré ou non chiffré
BIOS	200 Mo sur le volume système	400 Mo sur un volume non chiffré	400 Mo sur Secure Zone
UEFI	200 Mo sur la partition système EFI (ESP)	L'un des éléments suivants : • 400 Mo sur la partition système EFI (ESP) • 200 Mo sur la partition système EFI (ESP) et 200 Mo sur une partition non chiffrée accessible pendant le processus de démarrage.	400 Mo sur Secure Zone

Remarque
La restauration avec redémarrage nécessite de l'espace disque supplémentaire. Pour vérifier l'espace supplémentaire requis, voir "Espace disque nécessaire" (p. 717).

© Acronis International GmbH, 2003-2026

Limites

- [Ne s'applique pas à GRUB installé dans le secteur de démarrage principal] L'activation de Startup Recovery Manager écrase le secteur de démarrage principal (MBR) avec son propre code de démarrage. Par conséquent, vous devrez peut-être réactiver les chargeurs de démarrage tiers après l'activation.
- [Ne s'applique par à GRUB] Avant d'activer Startup Recovery Manager sous Linux, nous vous recommandons d'installer le chargeur de démarrage dans l'enregistrement de démarrage de la partition racine ou des partitions /boot au lieu de l'installer dans l'enregistrement de démarrage principal. Sinon, reconfigurez manuellement le chargeur de démarrage après l'activation.

Activation de Startup Recovery Manager

Pour activer l'invite de démarrage **Appuyez sur F11 pour Acronis Startup Recovery Manager** (ou pour ajouter l'élément **Startup Recovery Manager** au menu GRUB), vous devez activer Startup Recovery Manager.

Remarque
Les opérations de sauvegarde qui créent des sauvegardes de restauration en un clic échouent si Startup Recovery Manager n'est pas activé.

Pour activer Startup Recovery Manager

Sur un ordinateur avec agent

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel vous souhaitez activer Startup Recovery Manager.
2. Cliquez sur **Détails**.
3. Activez le commutateur **Startup Recovery Manager**.

Sur un ordinateur sans agent

1. Démarrez l'ordinateur en utilisant un support de démarrage.
2. Dans l'interface graphique du support de démarrage, cliquez sur **Outils** > **Activer Startup Recovery Manager**.
3. Sélectionnez **Activer**.
4. Cliquez sur **OK**.
5. Dans l'onglet **Détails**, vérifiez la ligne **Résultat** pour vous assurer que l'activation a réussi.
6. Cliquez sur **Fermer**.

Désactivation de Startup Recovery Manager

La désactivation porte sur l'invite de démarrage **Appuyez sur F11 pour Acronis Startup Recovery Manager** (ou supprime l'élément **Startup Recovery Manager** du menu GRUB).

© Acronis International GmbH, 2003-2026

Si Startup Recovery Manager n'est pas activé, vous pouvez toujours récupérer un ordinateur qui ne démarre pas en utilisant un support de démarrage distinct.

Remarque
Les opérations de sauvegarde qui créent des sauvegardes de restauration en un clic échouent si Startup Recovery Manager n'est pas activé.

Pour désactiver Startup Recovery Manager

Sur un ordinateur avec agent

1. Dans la console Cyber Protect, sélectionnez l'ordinateur sur lequel vous voulez désactiver Startup Recovery Manager.
2. Cliquez sur **Détails**.
3. Désactivez le commutateur **Startup Recovery Manager**.

Sur un ordinateur sans agent

1. Démarrez l'ordinateur en utilisant un support de démarrage.
2. Dans l'interface graphique du support de démarrage, cliquez sur **Outils** > **Désactiver Startup Recovery Manager**.
3. Sélectionnez **Désactiver**.
4. Cliquez sur **OK**.
5. Dans l'onglet **Détails**, vérifiez la ligne **Résultat** pour vous assurer que la désactivation a réussi.
6. Cliquez sur **Fermer**.

© Acronis International GmbH, 2003-2026

Implémentation de la reprise d'activité après sinistre

À propos d'Acronis Disaster Recovery

Acronis Disaster Recovery fait partie de Cyber Protection qui fournit un service de reprise d'activité après sinistre (DRaaS). Disaster Recovery est une solution rapide et stable qui, en cas de catastrophe naturelle ou d'origine humaine, lance des serveurs de restauration (copies exactes de vos serveurs locaux) sur le site de reprise d'activité après sinistre (DR).

Le site DR est un emplacement secondaire qui garantit que les opérations informatiques sont restaurées et se poursuivent si le site principal échoue. Dans ce cas, DR bascule les ressources des ordinateurs d'origine corrompus vers les serveurs de restauration sur le site DR. Le site DR comprend les serveurs cloud et la connectivité cloud (réseaux cloud).

Le site DR peut être situé dans Acronis Cyber Protect Cloud ou Microsoft Azure. La disponibilité des emplacements de site DR dépend des éléments d'offre qui sont activés pour votre tenant.

Remarque
Un seul emplacement est pris en charge par tenant client. Si vous souhaitez modifier l'emplacement de votre site DR, vous devez d'abord supprimer la configuration existante, puis en créer une nouvelle avec le nouvel emplacement.

Pour plus d'informations sur Disaster Recovery dans Acronis Cyber Protect Cloud, voir "Disaster Recovery vers Cyber Protect Cloud" (p. 1016).

Pour plus d'informations sur Disaster Recovery vers Microsoft Azure, voir "Disaster Recovery vers Microsoft Azure" (p. 1111).

Disaster Recovery vers Cyber Protect Cloud

Disaster Recovery vers Cyber Protect Cloud a les caractéristiques suivantes :

- L'emplacement du site DR est Cyber Protect Cloud.
- Les sauvegardes (points de restauration) des serveurs protégés sont stockées dans Cyber Protect Cloud.

Les fonctionnalités clés

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

© Acronis International GmbH, 2003-2026

- Gérez le service Disaster Recovery depuis une console unique
- Étendez jusqu'à 23 réseaux locaux au Cloud à l'aide d'un tunnel VPN sécurisé
- Établissez une connexion vers le site dans le Cloud sans aucun déploiement de appliance VPN (le mode « sur Cloud uniquement »)
- Établissez une connexion de point à site vers vos sites locaux et dans le cloud
- Protégez vos ordinateurs en utilisant des serveurs de restauration[1] dans le cloud
- Protégez vos applications et matériels en utilisant des serveurs primaires[2] dans le cloud
- Exécutez des opérations automatisées de reprise d'activité après sinistre pour des sauvegardes chiffrées
- Réalisez un basculement test dans le réseau isolé
- Utilisez des runbooks[3] pour automatiser le déploiement dans l'environnement de production sur le cloud

Exigences logicielles pour Disaster Recovery vers Cyber Protect Cloud

Systèmes d'exploitation pris en charge

La protection à l'aide d'un serveur de restauration a été testée pour les systèmes d'exploitation suivants :

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 18.04, 20.x, 21.x, 22.04, 22.10
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server

---

[1] [Disaster Recovery] Un réplica en MV de la machine d'origine, basé sur les sauvegardes de serveur protégées stockées dans le Cloud. Les serveurs de restauration sont utilisés pour remplacer les ressources depuis les serveurs originaux en cas de sinistre.
[2] [Disaster Recovery] Une machine virtuelle qui ne possède pas de machine associée sur le site local (tel qu'un serveur de restauration). Les serveurs primaires servent à protéger une application ou à exécuter divers services auxiliaires (tels qu'un service Web).
[3] [Disaster Recovery] Scénario planifié composé d'étapes configurables qui automatisent les actions de reprise d'activité après sinistre.

© Acronis International GmbH, 2003-2026

- AlmaLinux 8.x, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5
- Rocky Linux 9.x, 8.x
- SUSE Linux Enterprise Server 15

Le logiciel peut fonctionner avec d'autres systèmes d'exploitation Windows ou d'autres distributions Linux, mais cela n'est pas garanti.

Remarque
La protection à l'aide d'un serveur de restauration a été testée pour les machines virtuelles Microsoft Azure avec les systèmes d'exploitation suivants.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 – toutes les options d'installation, excepté Nano Server
- Ubuntu Server 20.04 LTS - Gen2 (Canonical). Pour plus d'informations sur l'accès à la console du serveur de restauration, consultez cet article de la base de connaissances.

Plates-formes de virtualisation prises en charge

La protection de machines virtuelles à l'aide d'un serveur de restauration a été testée pour les plates-formes de virtualisation suivantes :

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 avec Hyper-V
- Windows Server 2012/2012 R2 avec Hyper-V
- Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Machines virtuelles basées sur un noyau (KVM) — Invités entièrement virtualisés (HVM) uniquement. Les invités paravirtualisés (PV) ne sont pas pris en charge.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Nutanix Acropolis Hypervisor (AHV) avec Nutanix Acropolis Operating System (AOS) : 6.5, 6.6, 6.7, 6.8, 6.10
- Proxmox VE 8.2, 8.3, 8.4, 9.0

© Acronis International GmbH, 2003-2026

L'application VPN a été testée pour les plates-formes de virtualisation suivantes :

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 avec Hyper-V
- Windows Server 2012/2012 R2 avec Hyper-V
- Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Les ressources Linux qui ont des sauvegardes sans agent à partir d'un SE invité et des volumes avec des configurations de LVM (Logical Volume Manager) sont prises en charge.

Les ressources Windows qui ont des sauvegardes sans agent à partir d'un SE invité et des configurations de LDM (disques dynamiques) sont prises en charge.

Le logiciel peut fonctionner avec d'autres plates-formes de virtualisation ou d'autres versions, mais cela n'est pas garanti.

Limites

Les plate-formes et configurations suivantes ne sont pas prises en charge dans Disaster Recovery :

1. Plateformes non prises en charge :
   - Agents pour Virtuozzo
   - macOS
   - Les systèmes d'exploitation Windows de bureau ne sont pas pris en charge en raison des conditions générales relatives aux produits Microsoft.
   - Windows Server Azure Edition

     Azure Edition est une version particulière de Windows Server conçue spécifiquement pour fonctionner en tant que machine virtuelle Azure IaaS (VM) dans Azure ou en tant que VM dans un cluster HCI Azure Stack. Contrairement aux éditions Standard et Datacenter, Azure Edition n'a pas la licence nécessaire pour fonctionner sur un système nu, Windows Client Hyper-V, Windows Server Hyper-V, des hyperviseurs tiers ou dans des clouds tiers.
2. Configurations non prises en charge :

   Microsoft Windows
   - Les systèmes d'exploitation Windows de bureau ne sont pas pris en charge en raison des conditions générales relatives aux produits Microsoft.
   - Le service Active Directory avec réplication FRS n'est pas pris en charge.
   - Les supports amovibles sans formatage GPT ou MBR (dits « super disquettes ») ne sont pas pris en charge.

   Linux

© Acronis International GmbH, 2003-2026

- Systèmes de fichiers sans table de partition.
- Les ressources Linux qui sont sauvegardées avec un agent d'un SE invité et dont les volumes ont les configurations Logical Volume Manager avancées suivantes : volumes agrégés par bandes, volumes en miroir, volumes RAID 0, RAID 4, RAID 5, RAID 6 ou RAID 10.
- Pour SUSE Linux Enterprise Server 15, les configurations avec Btrfs ne sont pas prises en charge.

Remarque
Les ressources ayant plusieurs systèmes d'exploitation installés ne sont pas prises en charge.

3. Modes de tenant non pris en charge :
   - La reprise d'activité après sinistre n'est pas disponible lorsque le mode de conformité est activé pour le tenant.
4. Types de sauvegarde non pris en charge :
   - Les points de restauration de la protection continue des données (CDP) sont incompatibles.

     Important
     Si vous créez un serveur de restauration à partir d'une sauvegarde disposant d'un point de restauration CDP, lors de la restauration automatique ou lors de la création d'une sauvegarde d'un serveur de restauration, vous perdrez les données contenues dans le point de restauration CDP.

   - Les sauvegardes de données d'investigation ne peuvent pas être utilisées pour créer des serveurs de restauration.

Un serveur de restauration possède une interface réseau. Si la machine d'origine possède plusieurs interfaces réseau, une seule est émulée.

Les serveurs Cloud ne sont pas chiffrés.

Version d'évaluation Disaster Recovery

Vous pouvez utiliser une version d'évaluation de Acronis Disaster Recovery pour une période de 30 jours. Dans ce cas, Disaster Recovery présente les limitations suivantes pour les tenants partenaires :

- Aucun accès à l'Internet public pour les serveurs primaires et de restauration. Vous ne pouvez pas attribuer d'adresses IP aux serveurs.
- Le VPN multisite Ipsec n'est pas disponible.

Opérations réalisées avec les machines virtuelles Microsoft Azure

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

© Acronis International GmbH, 2003-2026

Vous pouvez effectuer le basculement des machines virtuelles Microsoft Azure vers Acronis Cyber Protect Cloud. Pour plus d'informations, voir "Réalisation d'un basculement" (p. 1088).

Après cela, vous pouvez effectuer une restauration automatique depuis Acronis Cyber Protect Cloud vers des machines virtuelles Azure. Pour plus d'informations, voir Restauration automatique depuis Cyber Protect Cloud vers une machine virtuelle Azure.

Vous pouvez configurer une connectivité VPN IPsec multisite entre Acronis Cyber Protect Cloud et la passerelle VPN Azure. Pour plus d'informations, voir "Configuration d'un VPN IPsec multi-site" (p. 1042).

Limites d'utilisation du stockage géoredondant dans le cloud

Le stockage géoredondant dans le cloud fournit un emplacement secondaire pour vos données de sauvegarde. L'emplacement secondaire se trouve dans une région distincte géographiquement de l'emplacement de stockage principal. La séparation géographique des régions garantit que, en cas de sinistre ayant des conséquences sur l'une des régions et rendant les données de stockage non récupérables, l'autre région ne sera pas affectée et les opérations pourront se poursuivre.

Important
Le service Disaster Recovery n'est pas pris en charge si l'emplacement de stockage des sauvegardes passe de l'emplacement principal à l'emplacement secondaire géoredondant.

Suppression automatique des environnements clients non utilisés sur un site dans le Cloud

Le service Disaster Recovery suit l'utilisation des environnements client créés à des fins de reprise après sinistre, et les supprime automatiquement s'ils ne sont pas utilisés.

Les critères suivants permettent de définir si le tenant du client est actif :

- Au moins un serveur Cloud est actuellement présent, ou un ou plusieurs serveurs Cloud étaient présents au cours des sept derniers jours.
  OU
- L'option **Accès VPN au site local** est activée et soit le tunnel OpenVPN site à site est établi, soit des données en provenance de l'appliance VPN ont été signalées au cours des 7 derniers jours.

Les autres tenants restants sont considérés comme des tenants inactifs. Pour ces tenants, le système effectue les opérations suivantes :

- La passerelle VPN et toutes les ressources Cloud liées à ce tenant sont supprimées.
- L'enregistrement de l'appliance VPN est annulé.

Les tenants inactifs sont ramenés à leur état antérieur à la configuration de la connectivité.

© Acronis International GmbH, 2003-2026

Travail avec Disaster Recovery vers Cyber Protect Cloud

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Le workflow de base utilisant la reprise d'activité après sinistre est le suivant :

1. Créez un serveur de restauration de la ressource que vous souhaitez protéger de l'une des manières suivantes :
   - a. Créez un plan de protection qui inclut les modules **Reprise d'activité après sinistre** et **Sauvegarde**, avec le paramètre **Que sauvegarder** défini sur **Toute la machine** ou **Système et volume de démarrage**.
     b. Appliquez le plan à vos terminaux. Cela configurera automatiquement l'infrastructure de reprise d'activité après sinistre par défaut. Pour plus d'informations, voir Créer un plan de protection de reprise d'activité après sinistre.

     Remarque
     Les administrateurs d'unité ne peuvent pas créer, modifier ni appliquer de plans de protection de reprise d'activité après sinistre.
   - Configurez manuellement l'infrastructure Cloud de reprise d'activité après sinistre et contrôlez chaque étape. Consultez "Création d'un serveur de restauration" (p. 1067).
2. Configurez la connectivité au site dans le cloud.
   - Mode « sur Cloud uniquement »
   - Connexion OpenVPN de site à site
   - Connexion VPN IPsec multi-site
   - Connexion de point à site
3. Configurez le basculement test automatisé.
4. Réalisez un basculement test.
5. [Lorsqu'un sinistre survient] Effectuez un basculement de production.
6. [Après le sinistre] Effectuez une restauration automatique des données sur le site local.
7. [Facultatif] Configurez des runbooks.

Création d'un plan de protection de reprise d'activité après sinistre

Le plan de protection de reprise d'activité après sinistre est un plan de protection dans lequel le module **Reprise d'activité après sinistre** est activé.

© Acronis International GmbH, 2003-2026

Une fois que vous avez activé la fonctionnalité de reprise d'activité après sinistre et appliqué le plan à vos terminaux, l'infrastructure réseau cloud (site cloud) est créée automatiquement. Pour plus d'informations, voir "Infrastructure par défaut du réseau cloud" (p. 1025).

Remarque

- L'application d'un plan de protection de reprise d'activité après sinistre crée une infrastructure de réseau Cloud uniquement si elle n'existe pas. Les réseaux Cloud existants ne sont pas modifiés ni recréés.
- Une fois que vous aurez configuré la reprise d'activité après sinistre, vous serez en mesure d'effectuer un basculement test ou un basculement de la production à partir de n'importe quel point de restauration généré après la création du serveur de restauration pour le terminal. Les points de restauration (sauvegardes) générés avant que le terminal ne soit protégé par la reprise d'activité après sinistre (c'est-à-dire avant la création du serveur de restauration) ne peuvent pas être utilisés pour le basculement.
- Un plan de protection de reprise d'activité après sinistre ne peut pas être activé si l'adresse IP d'un terminal ne peut pas être détectée. Par exemple lorsque des machines virtuelles sont sauvegardées sans agent, et qu'aucune adresse IP ne leur a été affectée.
- Lorsque vous appliquez un plan de protection, les mêmes réseaux et adresses IP sont attribués au site dans le Cloud. La connectivité VPN IPsec nécessite que les segments réseau du site local et du site dans le Cloud ne se chevauchent pas. Si une connectivité VPN IPsec multi-site est configurée et que vous appliquez un plan de protection ultérieurement à un ou plusieurs terminaux, vous devez en plus mettre à jour les réseaux Cloud et réaffecter les adresses IP des serveurs Cloud. Pour plus d'informations, voir "Réaffectation d'adresses IP" (p. 1061).

Pour créer un plan de protection de reprise d'activité après sinistre

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les machines que vous souhaitez protéger.
3. Cliquez sur **Protection**, puis sur **Création d'un plan**.
   Les paramètres par défaut du plan de protection s'affichent.
4. Configurez les options de sauvegarde.
   Pour utiliser la fonctionnalité de reprise d'activité après sinistre, le plan doit sauvegarder l'intégralité de la machine ou uniquement les disques requis pour le démarrage et la fourniture des services nécessaires à un stockage dans le Cloud.
5. Activez le module **Reprise d'activité après sinistre** en activant l'interrupteur à côté du nom du module.
6. Dans le champ **Emplacement**, sélectionnez où créer l'infrastructure de reprise d'activité après sinistre.
7. Cliquez sur **Créer**.
   Le plan est créé et appliqué aux ordinateurs sélectionnés. L'infrastructure réseau par défaut et les serveurs de restauration avec les paramètres par défaut sont créés. Pour plus d'informations, voir "Modification des paramètres par défaut d'un serveur de restauration" (p. 1024) et "Infrastructure par défaut du réseau cloud" (p. 1025).

© Acronis International GmbH, 2003-2026

Que faire ensuite

- Vous pouvez modifier la configuration par défaut du serveur de restauration. Pour plus d'informations, voir "Modification des paramètres par défaut d'un serveur de restauration" (p. 1024).
- Vous pouvez modifier la configuration de mise en réseau par défaut. Pour plus d'informations, voir "Connectivité et réseaux" (p. 1026).

Modification des paramètres par défaut d'un serveur de restauration

Lorsque vous créez et appliquez un plan de protection de reprise d'activité après sinistre, un serveur de restauration est créé avec les paramètres par défaut. Vous pouvez modifier ces paramètres par défaut si nécessaire.

La procédure suivante s'applique aux serveurs de restauration qui sont situés dans Cyber Protect Cloud. Si vous souhaitez configurer les paramètres d'un serveur de restauration situé dans Microsoft Azure, suivez les étapes décrites dans "Création de serveurs de restauration dans Microsoft Azure" (p. 1127).

Remarque
Un serveur de restauration est créé seulement s'il n'existe pas. Les serveurs de restauration existants ne sont pas modifiés ni recréés.

Pour modifier les paramètres par défaut du serveur de restauration

1. Accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez un terminal, puis cliquez sur **Reprise d'activité après sinistre**.
3. Pour modifier les paramètres par défaut du serveur de restauration.
   Les paramètres du serveur de restauration sont décrits dans le tableau suivant.

Paramètre	Valeur par défaut	Description
CPU et RAM	auto	Nombre de processeurs virtuels et la quantité de mémoire RAM pour le serveur de restauration. Les paramètres par défaut seront automatiquement déterminés en fonction du processeur du terminal et de la configuration de la mémoire RAM.
Réseau cloud	auto	Le serveur Cloud auquel le serveur sera connecté. Pour plus de détails sur la configuration des réseaux dans le Cloud, voir Infrastructure de réseau Cloud.
Adresse IP en réseau de production	auto	Adresse IP que le serveur aura dans le réseau de production. Par défaut, l'adresse IP de la machine d'origine est sélectionnée.

© Acronis International GmbH, 2003-2026

Adresse IP de test	désactivé	Cela vous permettra de tester un basculement dans le réseau de test isolé et de vous connecter au serveur de restauration via RDP ou SSH lors d'un basculement test. En mode de basculement test, la passerelle VPN remplace l'adresse IP test par l'adresse IP de production au moyen du protocole NAT. Si vous n'activez pas la case à cocher, la console sera le seul moyen d'accéder au serveur lors d'un basculement test.
Accès Internet	activé	Cela permettra au serveur de restauration d'accéder à Internet lors d'un vrai basculement ou d'un basculement test. Par défaut, le port TCP 25 est refusé pour les connexions sortantes.
Utiliser une adresse publique	désactivé	Disposer d'une adresse IP publique permet au serveur de restauration d'être accessible depuis Internet lors d'un basculement ou d'un basculement test. Si vous n'utilisez pas d'adresse IP publique, le serveur sera disponible uniquement sur votre réseau de production. L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes.
Définir le seuil des objectifs de point de restauration	désactivé	Le seuil des objectifs de point de restauration (RPO) définit l'intervalle de temps maximum autorisé entre le dernier point de restauration pour un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.

Infrastructure par défaut du réseau cloud

L'infrastructure de réseau cloud créée automatiquement lorsque vous appliquez à vos ressources un plan de protection de reprise d'activité après sinistre se compose des éléments suivants :

- Un serveur de restauration pour chaque terminal protégé.

  Le serveur de restauration est une machine virtuelle dans le cloud qui est une copie du terminal sélectionné.

  Pour chacun des terminaux sélectionnés, un serveur de restauration avec les paramètres par défaut est créé dans l'état **Veille** (la machine virtuelle n'est pas en cours d'exécution). La taille du serveur de restauration est ajustée automatiquement en fonction du processeur et de la RAM du terminal protégé.
- Passerelle VPN sur le site dans le cloud.
- Réseaux cloud auxquels les serveurs de restauration sont connectés.

© Acronis International GmbH, 2003-2026

Le système vérifie les adresses IP des terminaux et, s'il n'existe pas de réseaux Cloud correspondant à l'adresse IP, crée automatiquement les réseaux Cloud qui conviennent. Si vous disposez déjà de réseaux Cloud existants où les adresses IP des serveurs de restauration correspondent, ceux-ci ne seront ni modifiés ni recréés.

- Si vous ne disposez pas de réseaux Cloud existants ou si vous définissez une configuration de reprise d'activité après sinistre pour la première fois, les réseaux Cloud seront créés avec les plages maximales recommandées par IANA pour un usage privé (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) en fonction de votre plage d'adresses IP de terminaux. Vous pouvez restreindre l'accès réseau en modifiant le masque de réseau.
- Si vous avez des terminaux sur plusieurs réseaux locaux, le réseau sur le site dans le Cloud peut devenir un super-ensemble de réseaux locaux. Vous pouvez reconfigurer les réseaux dans la section **Connectivité**. Consultez "Gestion des réseaux pour OpenVPN site à site" (p. 1035).
- Si vous devez configurer la connectivité OpenVPN de site à site, téléchargez l'appliance VPN et configurez-la. Consultez "Configuration requise" (p. 1032). Assurez-vous que les plages des réseaux cloud correspondent aux plages de vos réseaux locaux connectés à l'appliance VPN.
- Pour modifier la configuration réseau par défaut, accédez à **Disaster Recovery** > **Connectivité**, ou cliquez sur **Accéder à connectivité** dans le module **Reprise d'activité après sinistre** du plan de protection.

Si vous révoquez, supprimez ou désactivez le module **Reprise d'activité après sinistre** d'un plan de protection, les serveurs de restauration et les réseaux cloud ne sont pas supprimés automatiquement. Si nécessaire, vous pouvez retirer manuellement l'infrastructure de reprise d'activité après sinistre.

Connectivité et réseaux

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Disaster Recovery vous permet de définir les types suivants de connexion au site dans le cloud :

- **Mode « sur Cloud uniquement »**

  Ce type de connexion ne nécessite pas de déploiement de matériel VPN sur le site local.

  Les réseaux locaux et dans le Cloud sont des réseaux indépendants. Ce type de connexion implique soit le basculement de tous les serveurs protégés du site local ou le basculement partiel de serveurs indépendants qui ne nécessitent pas de communiquer avec le site local.

  Les serveurs Cloud sur le site dans le Cloud sont accessibles via le VPN de point à site et les adresses IP publiques (si attribuées).
- **Connexion OpenVPN de site à site**

  Ce type de connexion requiert le déploiement d'un matériel VPN vers le site local.

  La connexion OpenVPN de site à site vous permet d'étendre vos réseaux au Cloud et de conserver les adresses IP.

© Acronis International GmbH, 2003-2026

Votre site local est connecté au site dans le Cloud au moyen d'un tunnel VPN sécurisé. Ce type de connexion est adapté en cas de serveurs hautement dépendants sur le site local, tels qu'un serveur Web et un serveur de bases de données. En cas de basculement partiel, quand l'un de ces serveurs est recréé sur le site dans le Cloud alors que l'autre reste dans le site local, ils pourront toujours communiquer entre eux via un tunnel VPN.

Les serveurs Cloud sur le site dans le Cloud sont accessibles via le réseau local, le VPN de point à site, et les adresses IP publiques (si attribuées).

- **Connexion VPN IPsec multi-site**

  Ce type de connexion nécessite un terminal VPN local compatible avec le protocole IPsec IKE v2.

  Lorsque vous commencez à configurer la connexion VPN IPsec multi-site, Disaster Recovery crée automatiquement une passerelle VPN Cloud avec une adresse IP publique.

  Avec le VPN IPsec multisite, vos sites locaux sont connectés au site dans le cloud au moyen d'un tunnel VPN IPsec sécurisé.

  Ce type de connexion est adapté aux scénarios de Disaster Recovery lorsque vous disposez d'un ou plusieurs sites locaux hébergeant des ressources critiques ou de services qui dépendent étroitement les uns des autres.

  En cas de basculement partiel de l'un des serveurs, le serveur est recréé sur le site dans le Cloud alors que les autres sont conservés dans le site local. Ils pourront toutefois toujours communiquer entre eux via un tunnel VPN IPsec.

  En cas de basculement partiel de l'un des sites locaux, les autres sites locaux restent opérationnels et pourront toujours communiquer entre eux via un tunnel VPN IPsec.

- **Accès VPN à distance de point à site**

  Un accès VPN à distance de point à site sécurisé vers les ressources de votre site Cloud et local provenant de l'extérieur en utilisant votre terminal.

  Pour accéder à un site local, ce type de connexion requiert le déploiement d'un matériel VPN vers le site local.

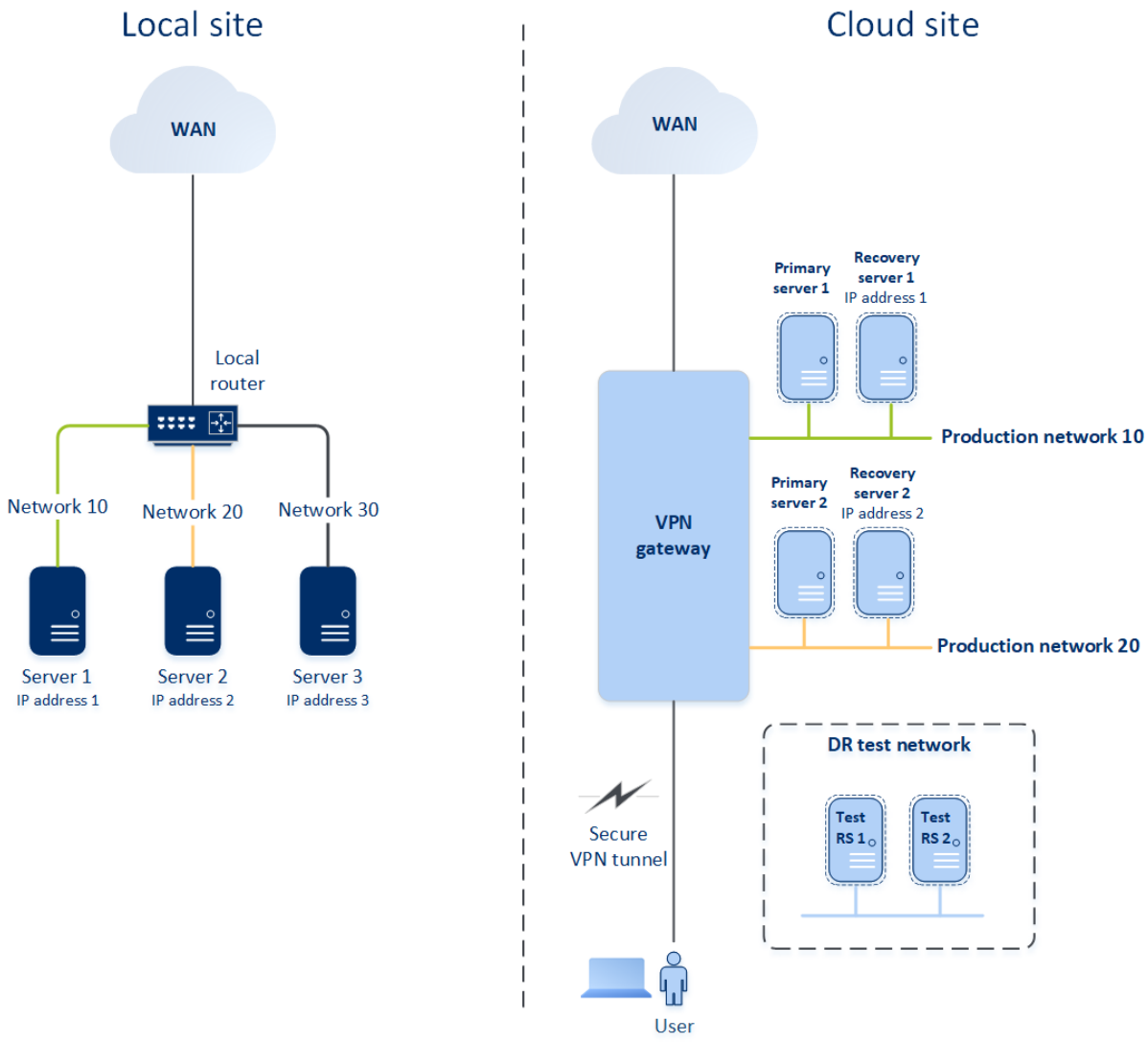
Mode « sur Cloud uniquement »

Le mode « sur Cloud uniquement » ne nécessite pas de déploiement d'une appliance VPN sur le site local. Cela implique que vous possédez deux réseaux indépendants : l'un sur le site local, l'autre sur le site dans le Cloud. Le routage est effectué avec le routeur sur le site dans le Cloud.

Fonctionnement du routage

Si le mode « sur Cloud uniquement » est activé, le routage est effectué avec le routeur sur le site Cloud, afin que les serveurs des différents réseaux Cloud puissent communiquer les uns avec les autres.

© Acronis International GmbH, 2003-2026



Configuration du mode « sur Cloud uniquement »

Le mode Cloud uniquement est le type de connectivité par défaut qui est créé automatiquement lorsque vous appliquez un plan de reprise d'activité après sinistre à une ressource.

Pour configurer une connexion dans le mode Cloud uniquement

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Sélectionnez **Sur Cloud uniquement** et cliquez sur **Configurer**.
   En conséquence, la passerelle VPN et le réseau cloud contenant l'adresse et le masque définis sont déployés dans le site dans le cloud.

Gestion des réseaux en mode Cloud uniquement

Vous pouvez ajouter et gérer jusqu'à 23 réseaux dans le cloud.

Ajouter un réseau

Pour ajouter un nouveau réseau Cloud

© Acronis International GmbH, 2003-2026

1. Accédez à **Disaster Recovery** > **Connectivité**.
2. Sous **Site dans le Cloud**, cliquez sur **Ajouter un réseau dans le Cloud**.
3. Définissez les paramètres de réseau cloud : adresse et masque du réseau. Cliquez ensuite sur **Terminé**.

En conséquence, le réseau cloud supplémentaire contenant l'adresse et le masque définis est créé dans le site cloud.

Supprimer un réseau

Prérequis

Tous les serveurs cloud sont supprimés du réseau que vous souhaitez supprimer.

Pour supprimer un réseau Cloud

1. Accédez à **Disaster Recovery** > **Connectivité**.
2. Dans **Site dans le Cloud**, cliquez sur l'adresse réseau que vous souhaitez supprimer.
3. Cliquez sur **Supprimer** pour confirmer l'opération.

Modifier les paramètres

Pour modifier les paramètres réseau

1. Accédez à **Disaster Recovery** > **Connectivité**.
2. Dans **Site dans le Cloud**, cliquez sur l'adresse réseau que vous souhaitez modifier.
3. Cliquez sur **Modifier.**
4. Définissez l'adresse et le masque du réseau, puis cliquez sur **Terminé**.

Connexion OpenVPN de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

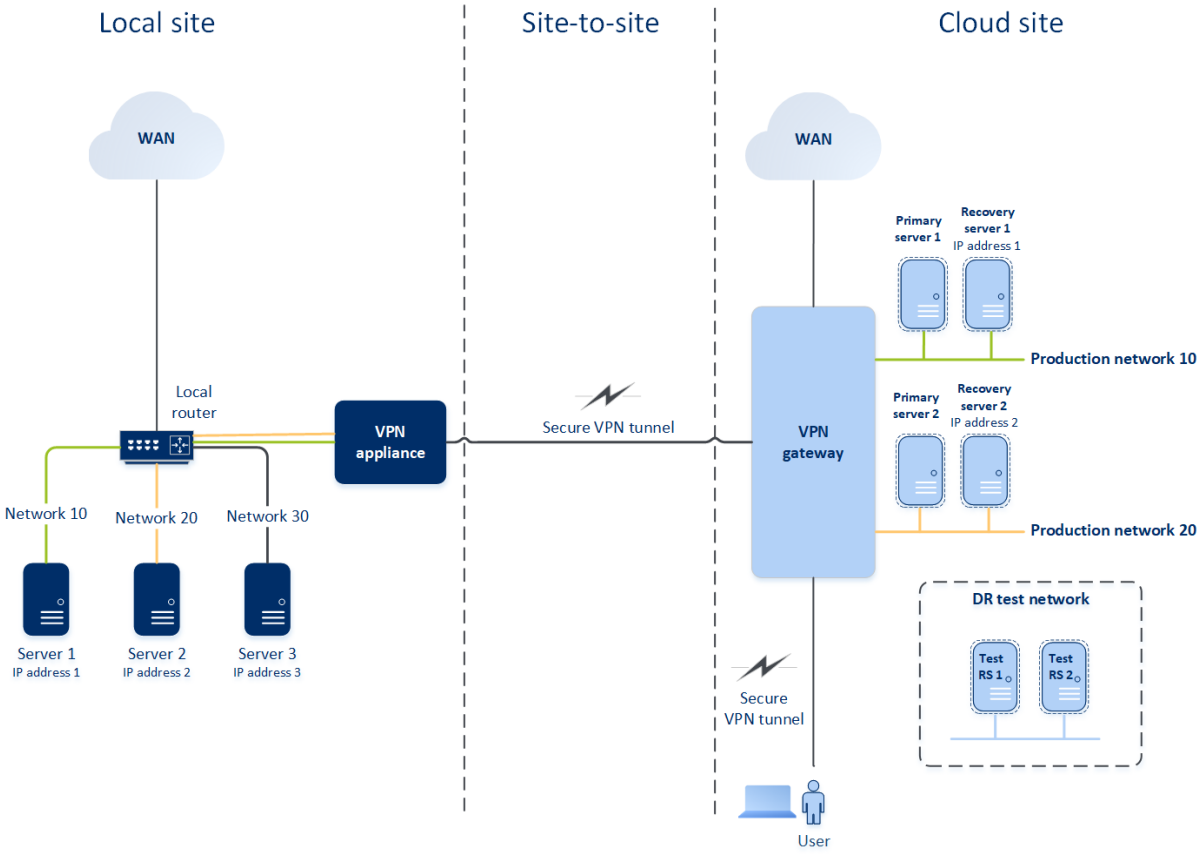
Pour comprendre comment le système de réseau fonctionne dans Disaster Recovery, nous examinerons un cas dans lequel vous possédez trois réseaux dotés chacun d'une machine sur le site local. Vous allez configurer la protection contre un sinistre pour les deux réseaux : le Réseau 10 et le Réseau 20.

Dans le diagramme ci-dessous, vous pouvez voir le site local dans lequel vos ordinateurs sont hébergés ainsi que le site dans le Cloud, où vos serveurs Cloud sont lancés en cas de sinistre.

La solution Disaster Recovery vous permet de basculer toute la ressource des ordinateurs corrompus du site local vers les serveurs cloud.

Vous pouvez ajouter et gérer jusqu'à 23 réseaux dans le cloud.

© Acronis International GmbH, 2003-2026



Pour établir une communication OpenVPN de site à site entre le site local et le site dans le cloud, une **appliance VPN** et une **passerelle VPN** sont utilisées.

Lorsque vous commencez à configurer la connexion OpenVPN site à site dans la console Cyber Protect, la passerelle VPN est automatiquement déployée sur le site dans le cloud.

Après le déploiement de la passerelle VPN, vous devez effectuer les opérations suivantes :

- Déployez le matériel VPN sur votre site local.
- Ajoutez les réseaux que vous souhaitez protéger.
- Enregistrez l'appliance VPN dans le cloud.

Disaster Recovery va créer une réplique de votre réseau local dans le cloud. Un tunnel VPN sécurisé sera établi entre l'appliance VPN et la passerelle VPN. Ce tunnel VPN fournira l'extension de votre réseau local vers le cloud. Les réseaux de production dans le cloud seront reliés à vos réseaux locaux. Les serveurs locaux et cloud communiqueront via ce tunnel VPN comme s'ils étaient tous dans le même segment Ethernet. Le routage sera effectué par votre routeur local.

Pour chaque machine source à protéger, vous devez créer un serveur de restauration dans le site dans le cloud. Ce serveur reste en **veille** jusqu'à ce qu'un événement de basculement se produise. Si un sinistre se produit et que vous lancez un processus de basculement (en **mode production**), le serveur de restauration représentant la copie exacte de votre machine protégée est lancé dans le cloud. Il se peut que la même adresse IP que celle de la machine source lui soit attribuée, et qu'il

© Acronis International GmbH, 2003-2026

soit lancé dans le même segment Ethernet. Vos clients peuvent continuer à travailler avec le serveur, sans remarquer de changement de fond.

Vous pouvez également démarrer un processus de basculement en **mode test**. Cela signifie que la machine source fonctionne toujours et que le serveur de restauration associé doté de la même adresse IP est lancé en même temps dans le cloud. Pour éviter les conflits d'adresse IP, un réseau virtuel spécial est créé dans le **réseau test** dans le cloud. Le réseau test est isolé pour éviter la duplication de l'adresse IP de la machine source dans un segment Ethernet. Pour accéder au serveur de restauration en mode de basculement test, vous devez affecter l'**adresse IP test** au serveur de restauration lorsque vous créez ce dernier. Vous pouvez également indiquer d'autres paramètres pour le serveur de restauration.

Fonctionnement du routage

Lorsqu'une connexion de site à site est établie, le routage entre réseaux cloud s'effectue par votre routeur local. Le serveur VPN n'effectue pas de routage entre des serveurs cloud situés dans différents réseaux cloud. Si un serveur cloud sur l'un des réseaux souhaite communiquer avec un serveur d'un autre réseau cloud, le trafic est acheminé au routeur local sur le site local via le tunnel VPN ; le routeur local l'achemine vers un autre réseau, puis le trafic revient au serveur de destination sur le site cloud via le tunnel.

Passerelle VPN

La passerelle VPN est le composant principal qui permet la communication entre les sites locaux et cloud. Il s'agit d'une machine virtuelle dans le cloud, sur laquelle un logiciel spécifique est installé et dont le réseau est configuré de manière spécifique. La passerelle VPN remplit les fonctions suivantes :

- Connecte les segments Ethernet de votre réseau local et de votre réseau de production dans le Cloud en mode couche 2.
- Fournit des règles iptables et ebtables.
- Agit comme routeur et NAT par défaut pour les ordinateurs des réseaux de test et de production.
- Agit comme serveur DHCP. Toutes les machines des réseaux de production et de test doivent obtenir la configuration réseau (adresses IP, paramètres DNS) via DHCP. À chaque fois, un serveur Cloud obtiendra la même adresse IP auprès du serveur DHCP. Si vous avez besoin de configurer un DNS personnalisé, nous vous invitons à contacter l'équipe d'assistance.
- Agit comme DNS de mise en cache.

Configuration réseau de la passerelle VPN

La passerelle VPN possède plusieurs interfaces réseau :

- Une interface externe, connectée à Internet
- Des interfaces de production, connectées aux réseaux de production
- Une interface de test, connectée au réseau test

© Acronis International GmbH, 2003-2026

Par ailleurs, deux interfaces virtuelles sont ajoutées pour les connexions de point à site et de site à site.

Lorsque la passerelle VPN est déployée et initialisée, les ponts sont créés : un pour l'interface externe et un pour les interfaces client et de production. Bien que le pont client-production et l'interface de test utilisent les mêmes adresses IP, la passerelle VPN peut router des packages correctement en utilisant une technique spécifique.

Application VPN

L'**appliance VPN** est une machine virtuelle dans le site local sur laquelle Linux et le logiciel spécial sont installés, et qui dispose d'une configuration réseau spéciale. Il permet la communication entre les sites locaux et dans le cloud.

Activation de la connexion de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez activer la connexion de site à site dans les cas suivants :

- Si vous avez besoin que les serveurs Cloud du site dans le Cloud communiquent avec les serveurs du site local.
- Après un basculement vers le Cloud, l'infrastructure est restaurée et vous souhaitez restaurer automatiquement vos serveurs vers le site local.

Pour activer la connexion de site à site

1. Accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**, puis activez l'option **Connexion de site à site**.

En conséquence, la connexion VPN de site à site est activée entre les sites locaux et dans le Cloud. Le service Disaster Recovery obtient les paramètres réseau à partir du matériel VPN et étend les réseaux locaux au site dans le Cloud.

Configuration OpenVPN de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Exigences relatives à l'appliance VPN

Configuration requise

- 1 processeur
- 1 Go de RAM

© Acronis International GmbH, 2003-2026

- 8 Go d'espace disque

Ports

- TCP 443 (sortant) : pour la connexion VPN
- TCP 80 (sortant) : pour la mise à jour automatique de l'application

Assurez-vous que vos pare-feux et les autres composants de votre système de sécurité réseau autorisent les connexions sur ces ports vers n'importe quelle adresse IP.

Configuration d'une connexion OpenVPN de site à site

L'appliance VPN étend votre réseau local au Cloud via un tunnel VPN sécurisé. Ce type de connexion est souvent appelé connexion de « site à site » (S2S). Vous pouvez suivre la procédure ci-dessous ou regarder le tutoriel vidéo.

Pour configurer une connexion via l'appliance VPN

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Sélectionnez **Connexion OpenVPN de site à site**, puis cliquez sur **Configurer**.
   Le système commence à déployer la passerelle VPN dans le Cloud. Cela peut prendre un certain temps. En attendant, vous pouvez passer à l'étape suivante.

   Remarque
   La passerelle VPN est fournie sans frais supplémentaires. Elle sera supprimée si la fonctionnalité de Disaster Recovery n'est pas utilisée, c'est-à-dire si aucun serveur primaire ni serveur de restauration n'est présent dans le Cloud pendant sept jours.

3. Dans le bloc **Application VPN**, cliquez sur **Télécharger et déployer**, puis, en fonction de la plate-forme de virtualisation que vous utilisez, téléchargez l'application VPN pour VMware vSphere, Proxmox ou Microsoft Hyper-V.
4. Déployez le matériel et connectez-le aux réseaux de production.
   Dans vSphere, vérifiez que le **mode Promiscuité** et l'option **Fausses transmissions** sont activés et configurés sur **Accepter** pour tous les commutateurs virtuels qui connectent l'appliance VPN aux réseaux de production. Pour accéder à ces paramètres, dans vSphere Client, sélectionnez l'hôte > **Résumé** > **Réseau**, puis sélectionnez le commutateur > **Modifier les paramètres...** > **Sécurité**.
   Dans Hyper-V, créez une machine virtuelle **Génération 1** avec 1 024 Mo de mémoire. Nous vous recommandons également d'activer la **mémoire dynamique** de l'ordinateur. Une fois la machine créée, accédez à **Paramètres** > **Matériel** > **Adaptateur réseau** > **Fonctionnalités avancées** et activez la case à cocher **Activer l'usurpation des adresses MAC**.
   Dans Proxmox, suivez la procédure concernant la création d'une appliance virtuelle dans Proxmox à partir d'un modèle OVA. Pour plus d'informations, voir "Créer une appliance virtuelle à partir d'un modèle OVA dans Proxmox" (p. 1040).
5. Démarrez l'application.

© Acronis International GmbH, 2003-2026

6. Ouvrez la console de l'application et connectez-vous à l'aide du nom d'utilisateur et du mot de passe « admin/admin ».
7. [Facultatif] Modifiez le mot de passe.
8. [Facultatif] Modifiez les paramètres réseau au besoin. Définissez l'interface qui sera utilisée comme WAN pour la connexion Internet.
9. Enregistrez le matériel dans le service Cyber Protection à l'aide des identifiants de l'administrateur de l'entreprise.

   Ces identifiants ne sont utilisés qu'une seule fois pour récupérer le certificat. L'URL du centre de données est prédéfinie.

   Remarque
   Si l'authentification à deux facteurs est configurée pour votre compte, vous serez également invité à saisir le code TOTP. Si l'authentification à deux facteurs est activée, mais pas configurée pour votre compte, vous ne pouvez pas enregistrer votre appliance VPN. Vous devez d'abord accéder à la page de connexion de la console Cyber Protect et terminer la configuration de l'authentification à deux facteurs pour votre compte. Pour en savoir plus sur l'authentification à deux facteurs, accédez au Guide de l'administrateur du portail de gestion.

Une fois la configuration terminée, l'application affiche le statut **En ligne**. Le matériel se connecte à la passerelle VPN et commence à communiquer des informations concernant les réseaux de toutes les interfaces actives au service Disaster Recovery. La console Cyber Protect affiche les interfaces en fonction des informations de l'appliance VPN.

Gestion des paramètres de l'appliance VPN

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Dans l'onglet **Disaster Recovery** > **Connectivité**, vous pouvez :

- Télécharger les fichiers journaux
- Désinscrire l'appliance (si vous devez réinitialiser les paramètres de l'appliance VPN ou basculer en mode Cloud uniquement).

Pour accéder à ces paramètres, cliquez sur l'icône **i** dans le bloc **Appliance VPN**.

Dans la console du matériel VPN, vous pouvez :

- Modifier le mot de passe de l'appliance
- Afficher/modifier les paramètres réseau et définir l'interface à utiliser comme WAN pour la connexion Internet
- Enregistrer/modifier le compte d'enregistrement (en répétant le processus d'enregistrement)
- Redémarrer le service VPN

© Acronis International GmbH, 2003-2026

- Redémarrer l'appliance VPN
- Exécuter la commande shell Linux (uniquement pour les cas de dépannage avancés)

Gestion des réseaux pour OpenVPN site à site

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Vous pouvez ajouter et gérer jusqu'à 23 réseaux dans le cloud.

Ajout de réseaux

Prérequis

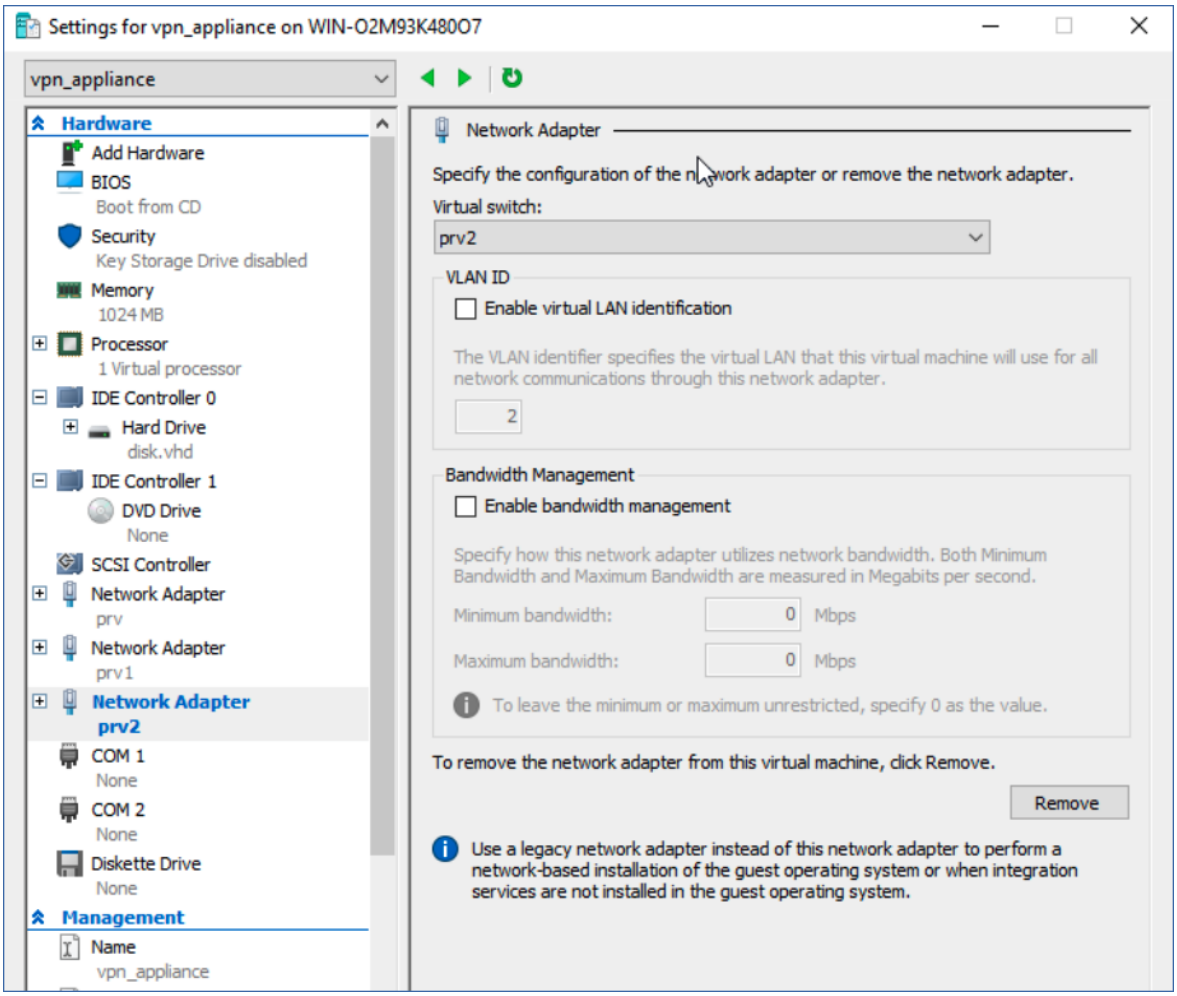
La connectivité Open VPN de site à site est configurée, conformément à la description figurant dans "Configuration requise" (p. 1032).

Pour ajouter des réseaux sur le site local et les étendre au cloud

1. Sur le matériel VPN, configurez la nouvelle interface réseau avec le réseau local que vous souhaitez étendre dans le Cloud.
2. [Facultatif] Si vous souhaitez ajouter un ou plusieurs réseaux, ajoutez pour chaque réseau supplémentaire une interface réseau virtuelle (carte réseau) à la machine virtuelle sur laquelle l'appliance virtuelle est en cours d'exécution.

   L'exemple suivant indique l'étape d'une machine virtuelle qui s'exécute sur un hyperviseur Hyper-V.

© Acronis International GmbH, 2003-2026

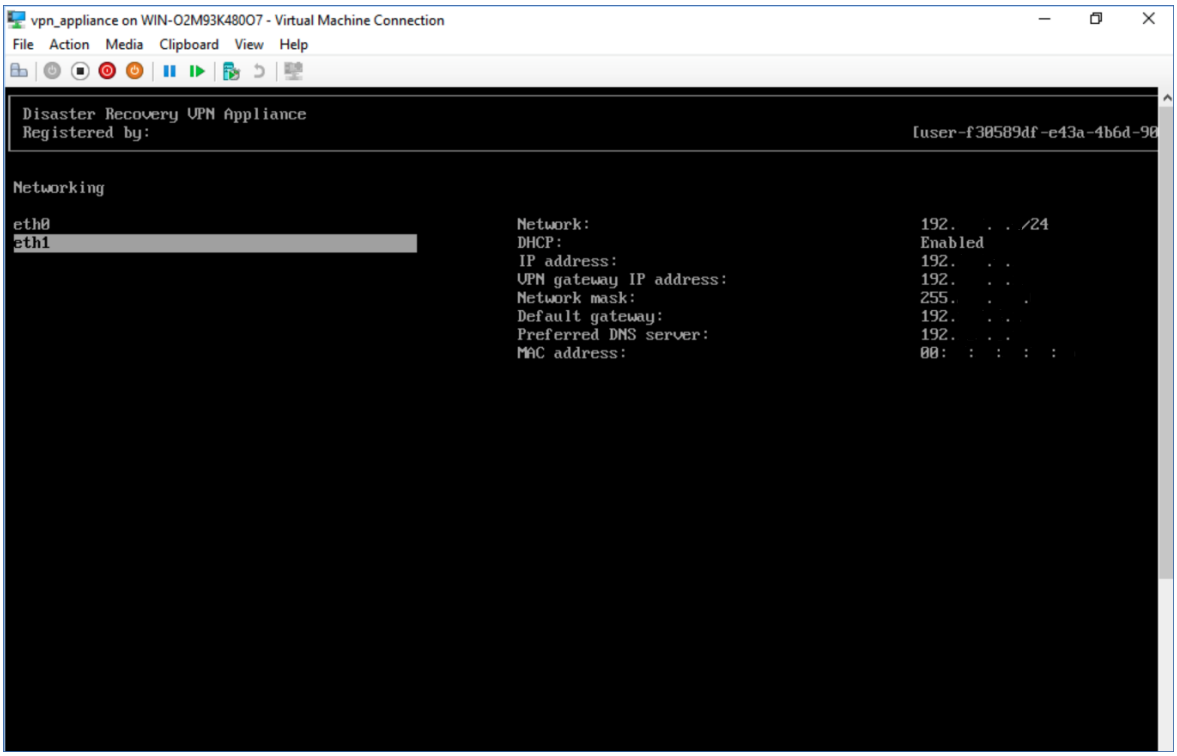


Remarque
Les nouvelles cartes de réseau virtuel doivent être configurées avec le réseau virtuel local que vous souhaitez étendre au cloud.

3. Connectez-vous à la console de l'appliance VPN, puis configurez dans la section **Réseau** les paramètres réseau pour l'une des interfaces (cartes).

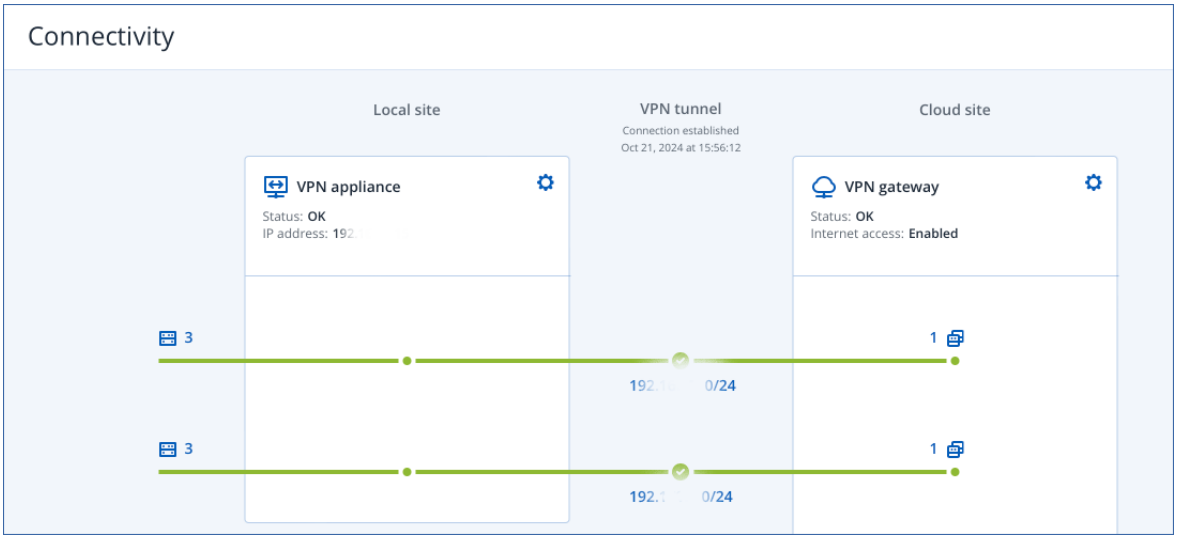
Remarque
- La configuration de l'adresse IP est obligatoire pour une seule des interfaces de réseau virtuel et permet l'accès à Internet. Vous pouvez ignorer la configuration de l'adresse IP des autres interfaces réseau.
- Le mode de promiscuité, les transmissions falsifiées ou l'usurpation d'adresses MAC doivent être activés pour chaque carte. Pour plus d'informations, consultez cet article de la base de connaissances.

© Acronis International GmbH, 2003-2026



L'appliance VPN commence automatiquement à communiquer à Disaster Recovery des informations concernant les réseaux de toutes les interfaces actives.

4. Connectez-vous à la console Cyber Protect, puis accédez à **Reprise d'activité après sinistre** > **Connectivité**.



Tous les réseaux locaux sont étendus automatiquement au site dans le cloud.

Supprimer un réseau

Pour supprimer un réseau étendu au Cloud

1. Connectez-vous à la console du matériel VPN.
2. Dans la section **Réseau**, sélectionnez l'interface que vous souhaitez supprimer, puis cliquez sur

© Acronis International GmbH, 2003-2026

Effacer les paramètres réseau.

3. Confirmez l'opération.

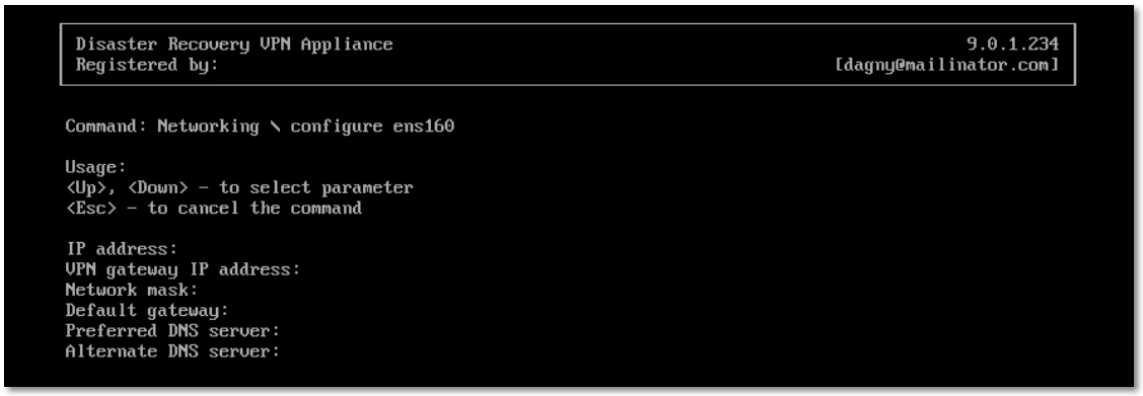
Par conséquent, l'extension du réseau local au cloud via un tunnel VPN sécurisé sera arrêtée. Ce réseau fonctionnera en tant que segment cloud indépendant. Si cette interface sert à faire passer le trafic en provenance et à destination du site dans le cloud, toutes vos connexions réseau depuis ou vers ce site dans le cloud seront déconnectées.

Modifier les paramètres

Pour changer les paramètres réseau

1. Connectez-vous à la console du matériel VPN.
2. Dans la section **Réseau**, sélectionnez l'interface que vous souhaitez modifier.
3. Cliquez sur **Modifier les paramètres réseau**.
4. Sélectionnez l'une des options :
   - Pour configurer le réseau automatiquement via DHCP, cliquez sur **Utiliser DHCP**, puis confirmez l'opération.
   - Pour configurer le réseau manuellement, cliquez sur **Définir une adresse IP statique**, configurez les paramètres, puis appuyez sur **Entrée**.

Paramètre	Description
Adresse IP	Adresse IP de l'interface dans le réseau local.
Adresse IP de la passerelle VPN	Adresse IP spéciale réservée au segment cloud du réseau pour le bon fonctionnement du service Disaster Recovery.
Masque réseau	Masque réseau du réseau local.
Passerelle par défaut	Passerelle par défaut sur le site local.
Serveur DNS préféré	Serveur DNS primaire sur le site local.
Autre serveur DNS	Serveur DNS secondaire sur le site local.



© Acronis International GmbH, 2003-2026

Autoriser le trafic DHCP via un VPN de couche 2

Si des terminaux sur votre site local obtiennent leur adresse IP depuis un serveur DHCP, vous pouvez protéger le serveur DHCP à l'aide de Disaster Recovery, le faire basculer vers le cloud, puis autoriser le trafic DHCP à passer par un VPN de couche 2. Ainsi, votre serveur DHCP fonctionnera dans le cloud, mais continuera à affecter des adresses IP à vos terminaux locaux.

Prérequis

Un type de connectivité site à site via un VPN de couche 2 doit être défini vers le site dans le cloud.

Pour autoriser le trafic DHCP à passer par la connexion VPN de couche 2

1. Accédez à **Disaster Recovery** > onglet **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Activez le commutateur **Autoriser le trafic DHCP via un VPN de couche 2**.

Passage d'OpenVPN site à site à un VPN IPsec multisite

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez facilement basculer d'une connexion OpenVPN de site à site à une connexion VPN IPsec multi-site, et vice-versa.

Lorsque vous basculez le type de connexion, les connexions VPN actives sont supprimées, mais les serveurs dans le Cloud et les configurations réseau sont préservés. Toutefois, vous devrez quand même réaffecter les adresses IP du réseau et des serveurs dans le Cloud.

Le tableau suivant compare les caractéristiques de base de la connexion OpenVPN de site à site et de la connexion VPN IPsec multi-site.

	Open VPN de site à site	VPN IPsec multi-site
Prise en charge de sites locaux	Site unique	Un ou plusieurs sites
Mode de passerelle VPN	L2 Open VPN	L3 IPsec VPN
Segments du réseau	Étend le réseau local au réseau dans le Cloud	Les segments réseau locaux et dans le Cloud ne doivent pas se chevaucher
Prise en charge de l'accès point à site au site local	Oui	Non
Prise en charge de l'accès point à site au site dans le	Oui	Oui

© Acronis International GmbH, 2003-2026

	Open VPN de site à site	VPN IPsec multi-site
Cloud		
Nécessite une offre d'IP publique	Non	Oui

Pour basculer d'une connexion OpenVPN de site à site à une connexion VPN IPsec multi-site

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Basculer sur un VPN IPsec multi-site**.
4. Cliquez sur **Reconfigurer**.
5. Réaffectez les adresses IP du réseau Cloud et des serveurs dans le Cloud.
6. Configurez les paramètres de connexion IPsec multi-site.

Désactivation de la connexion de site à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Si vous n'avez pas besoin que les serveurs du site dans le cloud communiquent avec les serveurs du site local, vous pouvez désactiver la connexion de site à site.

Pour désactiver la connexion de site à site

1. Accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**, puis désactivez l'option **Connexion de site à site**.

En conséquence, le site local est déconnecté du site dans le Cloud.

Créer une appliance virtuelle à partir d'un modèle OVA dans Proxmox

Après avoir téléchargé le modèle OVA, vous devez créer une appliance virtuelle à partir de celui-ci.

Pour créer une appliance virtuelle à partir d'un modèle OVA dans Proxmox

1. Dans Proxmox, développez l'arborescence **Vue du serveur** et accédez au nœud de cluster.
2. Cliquez sur **Importer**.
3. Dans la boîte de dialogue contextuelle, définissez les options requises de la machine virtuelle, puis cliquez sur **Importer**.
   L'appliance virtuelle est créée, mais elle n'est pas démarrée.

Dépannage de la connectivité VPN site à site OpenVPN

Lorsque vous rencontrez des problèmes de connectivité avec votre VPN site à site OpenVPN, vous pouvez effectuer un dépannage, puis corriger les erreurs signalées ou envoyer les informations à

© Acronis International GmbH, 2003-2026

l'équipe de support pour une analyse et une assistance supplémentaires.

Pour dépanner la connectivité du VPN site à site OpenVPN

1. Ouvrez l'interface graphique de l'appliance VPN.
2. Sous **Commandes**, sélectionnez **Dépannage**, puis appuyez sur **Entrée**.
3. Dans l'interface de ligne de commande, sur la ligne **Voulez-vous exécuter le diagnostic pour la connexion site à site [O/N]**, tapez **O**, puis appuyez sur **Entrée**.
   L'outil de diagnostic démarre. Si un problème est détecté, vous verrez une erreur correspondante et une description détaillée. Vous pouvez copier le texte de l'écran ou prendre une capture d'écran, puis l'envoyer à l'équipe de support pour obtenir de l'aide.

Connexion VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez utiliser la connectivité VPN IPsec multi-site pour connecter un site local ou plusieurs sites locaux à Disaster Recovery via une connexion VPN IPsec de couche 3 sécurisée.

Ce type de connectivité est utile pour les scénarios de reprise d'activité après sinistre dans les cas d'utilisation suivants :

- Vous disposez d'un site local hébergeant des ressources critiques.
- Vous disposez de plusieurs sites locaux hébergeant des ressources critiques, par exemple des bureaux à différents endroits.
- Vous utilisez des sites de logiciels tiers ou des sites de fournisseurs de services managés et vous êtes connectés à eux via un tunnel VPN IPsec.

Pour établir une communication VPN IPsec multi-site entre le site local et le site dans le Cloud, une **passerelle VPN** est utilisée. Lorsque vous commencez à configurer la connexion VPN IPsec multisite dans la console Cyber Protect, la passerelle VPN est déployée automatiquement sur le site dans le cloud. Vous devez configurer les segments réseau dans le Cloud et vous assurer qu'ils ne se chevauchent pas avec les segments réseau locaux. Un tunnel VPN sécurisé est établi entre les sites locaux et le site dans le Cloud. Les serveurs locaux et dans le Cloud peuvent communiquer via ce tunnel VPN comme s'ils se trouvaient tous dans le même segment Ethernet.

Remarque
Lorsque vous utilisez une connexion VPN IPsec multisite, une adresse IP publique est automatiquement affectée à la passerelle VPN.

Pour chaque machine source à protéger, vous devez créer un serveur de restauration dans le site dans le Cloud. Il reste en mode **Veille** jusqu'à ce qu'un événement de basculement se produise. Si un sinistre se produit et que vous lancez un processus de basculement (en **mode production**), le serveur de restauration représentant la copie exacte de votre machine protégée est lancé dans le

© Acronis International GmbH, 2003-2026

Cloud. Vos clients peuvent continuer à travailler avec le serveur, sans remarquer de changement de fond.

Vous pouvez également lancer un processus de basculement en **mode test**. Cela signifie que la machine source fonctionne toujours, et que le serveur de restauration associé doté de la même adresse IP est lancé en même temps dans le Cloud, dans un réseau privé spécial créé dans le Cloud - **réseau test**. Le réseau test est isolé pour éviter la duplication des adresses IP dans les autres segments de réseau Cloud.

Passerelle VPN

La **passerelle VPN** est le composant majeur qui permet la communication entre les sites locaux et le site dans le Cloud. Il s'agit d'une machine virtuelle dans le Cloud sur laquelle le logiciel spécial est installé et le réseau spécifiquement installé. La passerelle VPN a les fonctions suivantes :

- Connecte les segments Ethernet de votre réseau local et de votre réseau de production dans le Cloud en mode IPsec de couche 3.
- Agit comme routeur et NAT par défaut pour les ordinateurs des réseaux de test et de production.
- Agit comme serveur DHCP. Toutes les machines des réseaux de production et de test doivent obtenir la configuration réseau (adresses IP, paramètres DNS) via DHCP. À chaque fois, un serveur Cloud obtiendra la même adresse IP auprès du serveur DHCP.

  Si vous préférez, vous pouvez définir une configuration DNS personnalisée. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 1062).
- Agit comme DNS de mise en cache.

Fonctionnement du routage

Le routage entre les réseaux dans le Cloud est effectué avec le routeur sur le site Cloud, afin que les serveurs des différents réseaux Cloud puissent communiquer les uns avec les autres.

Configuration d'un VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez configurer une connexion VPN IPsec multi-site de deux manières différentes :

- depuis l'onglet **Disaster Recovery** > **Connectivité**.
- en appliquant un plan de protection sur ou un plusieurs terminaux, puis en basculant manuellement de la connexion OpenVPN site à site vers une connexion VPN IPsec multi-site, en configurant les paramètres du VPN IPsec multi-site et en réaffectant les adresses IP.

Onglet Connectivité

Pour configurer une connexion VPN IPsec multi-site depuis l'onglet Connectivité.

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Dans la section **Connexion VPN multi-site**, cliquez sur **Configurer**.
   Une passerelle VPN est déployée sur le site dans le Cloud.
3. Configurez les paramètres du VPN IPsec multi-site.

Plan de protection

Pour configurer une connexion VPN IPsec multi-site depuis un plan de protection

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Appliquez un plan de protection à un ou plusieurs terminaux dans la liste.
   Les paramètres du serveur de restauration et de l'infrastructure cloud sont automatiquement configurés pour la connectivité OpenVPN site à site.
3. Accédez à **Disaster Recovery** > **Connectivité**.
4. Cliquez sur **Afficher les propriétés**.
5. Cliquez sur **Basculer sur un VPN IPsec multi-site**.
6. Configurez les paramètres du VPN IPsec multi-site.
7. Réaffectez les adresses IP du réseau Cloud et des serveurs dans le Cloud.

Configuration des paramètres du VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Une fois que vous avez configuré un VPN IPsec multi-site, vous devez configurer les paramètres du site dans le Cloud et des sites locaux dans l'onglet **Disaster Recovery** > **Connectivité**.

Prérequis

- La connectivité VPN IPsec multi-site est configurée. Pour plus d'informations sur la configuration de la connectivité VPN IPsec multisite, reportez-vous à "Configuration d'un VPN IPsec multi-site" (p. 1042).
- Chaque passerelle VPN IPsec locale a une adresse IP publique.
- Votre réseau Cloud dispose d'un nombre suffisant d'adresses IP pour les serveurs Cloud qui sont des copies de vos machines protégées (dans le réseau de production) et pour les serveurs de restauration (avec une ou deux adresses IP selon vos besoins).
- [Si vous utilisez un pare-feu entre les sites locaux et le site dans le cloud] Les protocoles IP et les ports UDP suivants sont autorisés sur les sites locaux : ID de protocole IP 50 (ESP), Port UDP 500 (IKE) et Port UDP 4500.
- La configuration NAT-T sur les sites locaux est désactivée.

Pour configurer une connexion VPN IPsec multi-site

© Acronis International GmbH, 2003-2026

1. Ajoutez un ou plusieurs réseaux au site dans le Cloud.
   a. Cliquez sur **Ajouter un réseau**.

   Remarque
   Lorsque vous ajoutez un réseau dans le Cloud, un réseau de test correspondant sera ajouté automatiquement à la même adresse et au même masque de réseau pour effectuer des basculements tests. Les serveurs Cloud dans le réseau test auront les mêmes adresses IP que dans le réseau de production dans le Cloud. Si vous avez besoin d'accéder à un serveur Cloud depuis le réseau de production pendant un basculement test, attribuez-lui une seconde adresse IP test lorsque vous créez le serveur de restauration.

   b. Dans le champ **Adresse réseau**, tapez l'adresse IP du réseau.

   Remarque
   Vérifiez que les réseaux cloud ne chevauchent pas de réseau local dans votre environnement. Sinon, il est impossible d'établir un tunnel.

   c. Dans le champ **Masque réseau**, tapez le masque du réseau.
   d. Cliquez sur **Ajouter**.
2. Configurez les paramètres pour chaque site local que vous souhaitez connecter au site dans le Cloud, en suivant les recommandations pour les sites locaux. Pour plus d'informations sur ces recommandations, reportez-vous à "Recommandations générales pour les sites locaux" (p. 1045).
   a. Cliquez sur **Ajouter une connexion**.
   b. Saisissez un nom pour la passerelle VPN locale.
   c. Entrez l'adresse IP publique de la passerelle VPN locale.
   d. [Facultatif] Saisissez une description de la passerelle VPN locale.
   e. Cliquez sur **Suivant**.
   f. Dans le champ **Clé prépartagée**, tapez la clé prépartagée, ou cliquez sur **Générer une nouvelle clé prépartagée** pour utiliser une valeur générée automatiquement.

   Remarque
   Vous devez utiliser la même clé prépartagée pour les passerelles VPN locales et dans le Cloud.

   g. Cliquez sur **Paramètres de sécurité IPsec/IKE** pour les configurer. Pour plus d'informations sur les paramètres que vous pouvez configurer, reportez-vous à "Paramètres de sécurité IPsec/IKE" (p. 1046).

© Acronis International GmbH, 2003-2026

Remarque
Vous pouvez utiliser les paramètres par défaut, qui sont remplis automatiquement, ou utiliser des valeurs personnalisées. Seules les connexions de protocole IKEv2 sont prises en charge. L'**Action de démarrage** par défaut lors de l'établissement du VPN est **Ajouter** (votre passerelle VPN locale démarre la connexion), mais vous pouvez la modifier en **Démarrer** (la passerelle VPN dans le Cloud démarre la connexion) ou **Route** (adaptée pour les pare-feux qui prennent en charge les options de routage).

h. Configurez les **Politiques réseau**.
   Les politiques réseau spécifient les réseaux auxquels se connecte le VPN IPsec. Tapez l'adresse IP et le masque du réseau au format CIDR. Les segments réseau locaux et dans le Cloud ne doivent pas se chevaucher.
i. Cliquez sur **Enregistrer**.

Recommandations générales pour les sites locaux

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lors de la configuration des sites locaux pour votre connectivité VPN IPsec multi-site, prenez en compte les recommandations suivantes :

- Pour chaque phase d'IKE, définissez les paramètres suivants pour au moins une des valeurs configurées sur le site dans le Cloud : Algorithme de chiffrement, algorithme de hachage et numéros de groupes Diffie-Hellman.
- Activez la confidentialité persistante avec au moins une des valeurs pour les numéros de groupes Diffie-Hellman configurée sur le site dans le Cloud pour la phase 2 d'IKE.
- Configurez la même valeur **Durée de vie** que celle du site dans le cloud pour les phases 1 et 2 d'IKE.
- Les configurations avec NAT-T (NAT trasversal) ne sont pas prises en charge. Désactivez la configuration NAT-T sur le site local. Dans le cas contraire, aucune autre encapsulation UDP ne peut être négociée.
- La configuration **Action de démarrage** définit le côté où démarre la connexion. La valeur par défaut **Ajouter** signifie que le site local démarre la connexion et que le site dans le Cloud attend le démarrage de la connexion. Modifier la valeur sur **Démarrer** si vous souhaitez que le site dans le Cloud démarre la connexion ou sur **Route** si vous souhaitez que les deux côtés soient capables de démarrer la connexion (cette option est adaptée pour les pare-feux compatibles avec l'option de routage).

Pour en savoir plus et obtenir des exemples de configuration pour différentes solutions, consultez :

- Cette série d'articles de la base de connaissances
- Cet exemple de vidéo

© Acronis International GmbH, 2003-2026

Paramètres de sécurité IPsec/IKE

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le tableau suivant fournit plus de détails sur les paramètres de sécurité IPsec/IKE.

Paramètre	Description
Algorithme de chiffrement	L'algorithme de chiffrement qui sera utilisé pour s'assurer que les données ne peuvent pas être consultées pendant leur transit. Par défaut, tous les algorithmes sont sélectionnés. Vous devez configurer au moins un des algorithmes sélectionnés sur votre terminal de passerelle local pour chaque phase d'IKE.
Algorithme de hachage	L'algorithme de hachage qui sera utilisé pour vérifier l'intégrité et l'authenticité des données. Par défaut, tous les algorithmes sont sélectionnés. Vous devez configurer au moins un des algorithmes sélectionnés sur votre terminal de passerelle local pour chaque phase d'IKE.
Numéros de groupes Diffie-Hellman	Les numéros de groupes Diffie-Hellman définissent la fiabilité de la clé utilisée dans le processus Internet Key Exchange (IKE). Les numéros de groupes plus élevés sont plus sécurisés, mais nécessitent un temps de calcul plus long pour la clé. Par défaut, tous les groupes sont sélectionnés. Vous devez configurer au moins un des groupes sélectionnés sur votre terminal de passerelle local pour chaque phase d'IKE.
Durée de vie (secondes)	La valeur de Durée de vie détermine la durée d'une instance de connexion avec un ensemble de clés de chiffrement/d'authentification pour les paquets utilisateur, de la négociation réussie à l'expiration. Plage pour la phase 1 : 900-28 800 secondes avec par défaut 28 800. Plage pour la phase 2 : 900-3 600 secondes avec par défaut 3 600. La durée de vie de la phase 2 doit être inférieure à celle de la phase 1.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	La connexion est renégociée via le canal de clés avant son expiration, voir **Durée de marge du changement de clé**. Si une divergence de durée de vie a lieu entre le site local et le site distant, un encombrement de connexions substituées se produira du côté où la durée de vie est la plus longue. Voir aussi **Durée de marge du changement de clé** et **Fuzz du changement de clé**.
Durée de marge du changement de clé (secondes)	La durée de marge avant l'expiration de la connexion ou l'expiration du canal de changement de clé, au cours de laquelle le côté local de la connexion VPN essaie de négocier un remplacement. L'heure exacte du changement de clé est sélectionnée aléatoirement en fonction de la valeur de **Fuzz du changement de clé**. Pertinent uniquement au niveau local, le côté à distance n'a pas besoin de l'accepter. Plage : 900 à 3 600 secondes. La valeur par défaut est 3 600.
Taille de la fenêtre de réexécution (paquets)	La taille de la fenêtre de réexécution IPsec pour cette connexion. La valeur par défaut -1 utilise la valeur configurée avec charon.replay_window dans le fichier strongswan.conf. Les valeurs supérieures à 32 sont prises en charge uniquement lors de l'utilisation du back-end Netlink. Une valeur de 0 désactive la protection contre les attaques par rejeu d'IPsec.
Fuzz du changement de clé (%)	Le pourcentage maximum pour lequel les valeurs marginbytes, marginpackets et margintime sont augmentées aléatoirement pour randomiser les intervalles de changement de clé (primordial pour les hôtes avec de nombreuses connexions). La valeur fuzz du changement de clé peut dépasser 100 %. La valeur de marginTYPE, après l'augmentation aléatoire, ne doit pas dépasser celle de lifeTYPE, où TYPE correspond à Octets, Paquets ou Heure. La valeur 0 % annule la randomisation. Pertinent uniquement au niveau local, le côté à distance n'a

© Acronis International GmbH, 2003-2026

Paramètre	Description
	pas besoin de l'accepter.
Expiration du délai d'attente DPD (secondes)	Durée après laquelle une expiration du délai d'attente de la fonction Dead peer detection (DPD) se produit. Vous pouvez spécifier la valeur 30 ou une valeur supérieure. La valeur par défaut est 30.
Action d'expiration du délai d'attente de la fonction Dead peer detection (DPD)	L'action à effectuer après l'expiration du délai d'attente de la fonction dead peer detection (DPD). **Redémarrer** : redémarrage de la session lors de l'expiration du délai d'attente DPD. **Effacer** : fin de la session lors de l'expiration du délai d'attente DPD. **Aucun** : aucune action lors de l'expiration du délai d'attente DPD.
Action de démarrage	Détermine quel côté démarre la connexion et établit le tunnel pour la connexion VPN. **Ajouter** : votre passerelle VPN locale démarre la connexion. **Démarrer** : la passerelle VPN dans le Cloud démarre la connexion. **Route** : option adaptée aux passerelles VPN compatibles avec l'option de routage. Le tunnel est activé uniquement quand il y a un trafic provenant de la passerelle VPN locale ou la passerelle VPN dans le Cloud.

Passage d'un VPN IPsec multisite à un VPN OpenVPN site à site

Pour basculer d'une connexion VPN IPsec multisite à une connexion OpenVPN de site à site.

Lorsque vous basculez le type de connexion, les connexions VPN actives sont supprimées, mais les serveurs dans le Cloud et les configurations réseau sont préservés. Toutefois, vous devrez quand même réaffecter les adresses IP du réseau et des serveurs dans le Cloud.

Le tableau suivant compare les caractéristiques de base de la connexion OpenVPN de site à site et de la connexion VPN IPsec multi-site.

	Open VPN de site à site	VPN IPsec multi-site
Prise en charge de sites locaux	Site unique	Un ou plusieurs sites
Mode de passerelle VPN	L2 Open VPN	L3 IPsec VPN

© Acronis International GmbH, 2003-2026

	Open VPN de site à site	VPN IPsec multi-site
Segments du réseau	Étend le réseau local au réseau dans le Cloud	Les segments réseau locaux et dans le Cloud ne doivent pas se chevaucher
Prise en charge de l'accès point à site au site local	Oui	Non
Prise en charge de l'accès point à site au site dans le Cloud	Oui	Oui
Nécessite une offre d'IP publique	Non	Oui

Pour basculer d'une connexion VPN IPsec multisite à une connexion OpenVPN de site à site

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Basculer sur un OpenVPN de site à site**.
4. Cliquez sur **Reconfigurer**.
5. Réaffectez les adresses IP du réseau Cloud et des serveurs dans le Cloud.
6. Configurez les paramètres de connexion de site à site.

Dépannage de la configuration VPN IPsec

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsque vous configurez ou utilisez la connexion VPN IPsec, il est possible que vous rencontriez des problèmes.

Pour en savoir plus sur les problèmes rencontrés, reportez-vous aux fichiers journaux IPsec, et consultez les rubriques de problèmes de configuration VPN IPsec pour obtenir des solutions à certains des problèmes courants susceptibles de se produire.

Dépannage des problèmes de configuration VPN IPsec

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le tableau suivant décrit les problèmes de configuration VPN IPsec les plus courants, et explique comment les résoudre.

© Acronis International GmbH, 2003-2026

Problème	Solution possible
Le message d'erreur suivant s'affiche : **Erreur de négociation IKE phase 1. Vérifiez les paramètres IKE IPsec sur les sites Cloud et locaux.**	Cliquez sur **Réessayer** et vérifiez si un message d'erreur plus spécifique apparaît. Par exemple, il peut s'agir d'un message concernant une incompatibilité de l'algorithme ou une clé prépartagée incorrecte. **Remarque** Pour des raisons de sécurité, les restrictions suivantes s'appliquent à la connectivité VPN IPsec : • IKEv1 sera déprécié dans RFC8247 et n'est pas pris en charge pour des raisons de sécurité. Seules les connexions de protocole IKEv2 sont prises en charge. • Les algorithmes de chiffrement suivants ne sont pas considérés comme sécurisés et ne sont donc pas pris en charge : DES et 3DES. • Les algorithmes de hachage suivants ne sont pas considérés comme sécurisés et ne sont donc pas pris en charge : SHA1 et MD5. • Le groupe Diffie-Hellman 2 n'est pas considéré comme sécurisé et n'est donc pas pris en charge.
L'état **Connexion en cours** persiste lors de la connexion entre mon site local et le site dans le Cloud.	Vérifiez les points suivants : • Si le port UDP 500 est ouvert (lorsque vous utilisez un pare-feu). • La connectivité entre le site local et le site dans le Cloud. • Si l'adresse IP du site local est correcte.
L'état **En attente de connexion** persiste lors de la connexion entre mon site local et le site dans le Cloud.	Cet état apparaît lorsque l'**action de démarrage** pour le site dans le Cloud est définie sur **Ajouter**, ce qui signifie que le site dans le Cloud attend que le site local démarre la connexion. Démarrez la connexion depuis le site local.
L'état **En attente de trafic** persiste lors de la connexion entre mon site local et le site dans le Cloud.	Cet état apparaît lorsque l'**action de démarrage** pour le site dans le Cloud est définie sur **Route**. Si vous attendez une connexion depuis le site local, procédez comme suit : • Depuis le site local, essayez d'envoyer un ping à la machine virtuelle sur le site dans le Cloud. Ce comportement standard est nécessaire pour

© Acronis International GmbH, 2003-2026

Problème	Solution possible
	établir un tunnel pour certains terminaux, par exemple les terminaux Cisco ASA. (Mode de routage) • Assurez-vous que le site local a établi un tunnel en définissant l'**action de démarrage** du site local sur **Démarrer**.
La connexion entre mon site local et le site dans le Cloud est établie, mais je vois qu'une ou plusieurs politiques réseau sont désactivées.	Ce problème peut avoir plusieurs causes : • Le mappage réseau sur le site IPsec dans le Cloud est différent du mappage réseau sur le site local. Vérifiez que les mappages réseau et que la séquence des politiques réseau sur le site local et sur le site dans le Cloud correspondent. • Cet état est correct lorsque l'**action de démarrage** du site local et/ou du site dans le Cloud est définie sur **Route** (par exemple, sur les terminaux Cisco ASA), et qu'il n'y a pas de trafic actuellement. Vous pouvez essayer d'envoyer un ping pour vous assurer que le tunnel est établi. Si le ping ne fonctionne pas, vérifiez le mappage réseau sur le site local et sur le site dans le Cloud.
Je veux redémarrer une connexion IPsec spécifique.	Pour redémarrer une connexion IPsec spécifique : 1. Depuis l'écran **Reprise d'activité après sinistre** > **Connectivité**, cliquez sur la connexion IPsec. 2. Cliquez sur **Désactiver la connexion**. 3. Cliquez à nouveau sur la connexion IPsec. 4. Cliquez sur **Activer la connexion**.

Téléchargement des fichiers journaux VPN IPsec

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous trouverez des informations supplémentaires sur la connectivité IPsec dans les fichiers journaux sur le serveur VPN. Les fichiers journaux sont compressés sous la forme d'une archive .zip que vous pouvez télécharger et extraire.

Prérequis

La connectivité VPN IPsec multi-site est configurée.

© Acronis International GmbH, 2003-2026

Pour télécharger et extraire l'archive .zip avec les fichiers journaux

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur l'icône en forme d'engrenage située à côté de la passerelle VPN du site dans le Cloud.
3. Cliquez sur **Télécharger le journal**.
4. Cliquez sur **Terminé**.
5. Lorsque l'archive .zip est prête à être téléchargée, cliquez sur **Télécharger le journal**, puis enregistrez-la au niveau local.

Fichiers journaux VPN IPsec multi-site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La liste suivante décrit les fichiers journaux VPN IPsec qui font partie de l'archive zip, et les informations qu'ils contiennent.

- `ip.txt` : le fichier contient les journaux issus de la configuration des interfaces réseau. Vous devez voir deux adresses IP : une adresse IP publique et une adresse IP locale. Si vous ne voyez pas ces deux adresses IP dans le fichier journal, il y a un problème. Dans ce cas, contactez l'équipe d'assistance.

  Remarque
  Le masque pour l'adresse IP publique doit être 32.

- `swanctl-list-loaded-config.txt` : le fichier contient des informations concernant tous les sites IPsec.

  Si vous ne voyez pas un site dans le fichier, la configuration IPsec n'a pas été appliquée. Essayez de mettre à jour la configuration et de l'enregistrer, ou contacter l'équipe d'assistance.
- `swanctl-list-active-sas.txt` : le fichier contient des connexions et des politiques dont l'état est actif ou en cours de connexion.

Accès VPN à distance de point à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Une connexion point à site est une connexion sécurisée depuis l'extérieur utilisant vos terminaux (comme un ordinateur de bureau ou un ordinateur portable) vers le site dans le cloud et les sites locaux via un VPN. Elle est disponible après avoir établi une connexion OpenVPN site à site vers le site de reprise d'activité après sinistre. Ce type de connexion est utile dans les cas suivants :

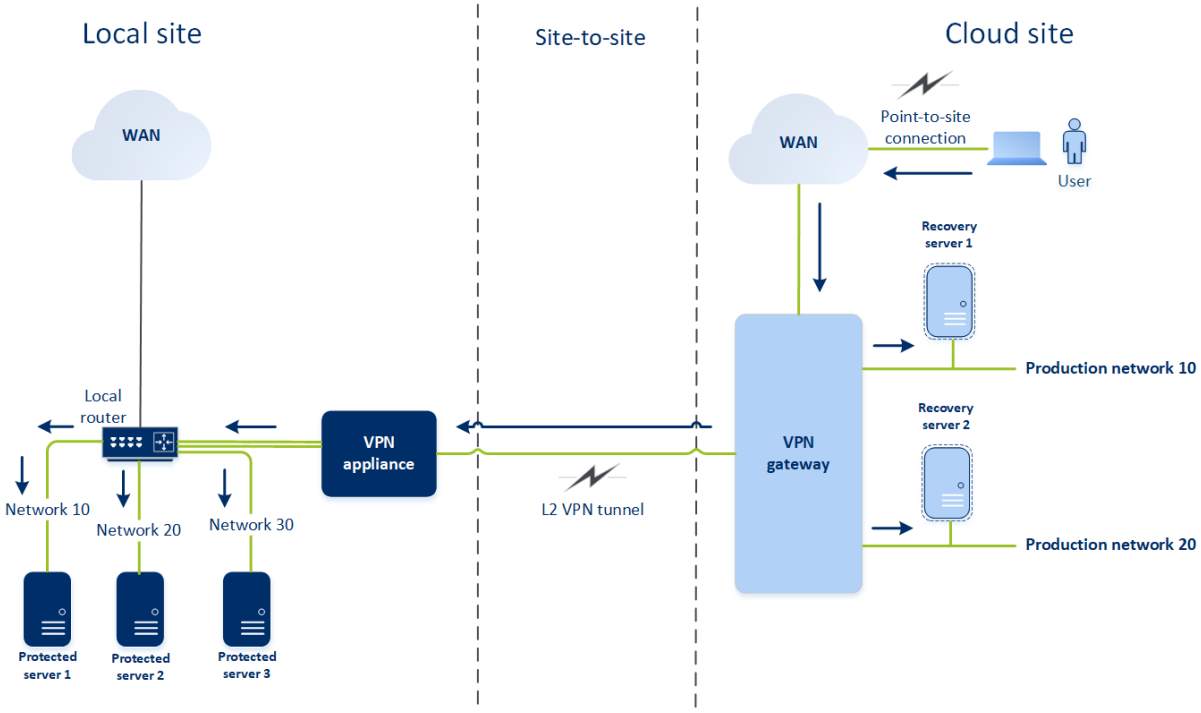
- Dans de nombreuses sociétés, les services d'entreprise et les ressources Web ne sont disponibles que sur le réseau d'entreprise. La connexion de point à site vous permet de vous connecter de façon sécurisée au site local.

© Acronis International GmbH, 2003-2026

- En cas de sinistre, lorsqu'une ressource bascule vers le site dans le Cloud et que votre réseau local est en panne, il se peut que vous deviez accéder directement à vos serveurs Cloud. Cela est possible via la connexion de point à site au site dans le Cloud.

Pour la connexion de point à site au site local, vous devez installer l'appliance VPN sur le site local, configurer la connexion site à site, puis la connexion de point à site au site local. Ainsi, vos employés travaillant à distance auront accès au réseau d'entreprise via le VPN de couche 2.

Le schéma ci-dessous montre le site local, le site dans le Cloud et les communications entre les serveurs surlignées en vert. Le tunnel VPN L2 relie vos sites locaux et dans le Cloud. Quand un utilisateur établit une connexion de point à site, les communications vers le site local sont réalisées par l'intermédiaire du site dans le Cloud.



La configuration de point à site utilise des certificats pour s'authentifier auprès du client VPN. Les autres identifiants utilisateur servent à l'authentification. Prenez connaissance des informations suivantes concernant la connexion de point à site au site local :

- Les utilisateurs doivent utiliser leurs identifiants Cyber Protect Cloud pour s'authentifier sur le client VPN. Ils doivent avoir le rôle utilisateur « Administrateur d'entreprise » ou « Cyberprotection ».
- Si vous avez régénéré la configuration OpenVPN, vous devez fournir la configuration mise à jour à tous les utilisateurs qui utilisent la connexion de point à site pour accéder au site dans le Cloud.

Configuration de l'accès VPN à distance de point à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

© Acronis International GmbH, 2003-2026

Si vous devez vous connecter à distance à votre site local, vous pouvez configurer la connexion de point à site au site local. Vous pouvez suivre la procédure ci-dessous ou regarder le tutoriel vidéo.

Prérequis

- La connectivité Open VPN site à site est configurée.
- L'appliance VPN est installée sur le site local.

Pour configurer la connexion de point à site au site local

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Activez l'option **Accès VPN au site local**.
4. Assurez-vous que l'utilisateur qui doit établir la connexion de point à site au site local dispose des éléments suivants :
   - Un compte utilisateur dans Cyber Protect Cloud. Les autres identifiants utilisateur servent à l'authentification dans le client VPN. Sinon, créez un compte utilisateur dans Cyber Protect Cloud.
   - Un rôle utilisateur « Administrateur d'entreprise » ou « Cyberprotection ».
5. Configurer le client OpenVPN :
   a. Téléchargez le client OpenVPN v2.4.0 ou version ultérieure depuis l'emplacement suivant https://openvpn.net/community-downloads/.

      Remarque
      Le client OpenVPN Connect n'est pas pris en charge.

   b. Installez le client OpenVPN sur la machine que vous souhaitez connecter au site local.
   c. Cliquez sur **Télécharger la configuration pour OpenVPN**. Le fichier de configuration est valide pour les utilisateurs de votre organisation possédant le rôle utilisateur « Administrateur d'entreprise » ou « Cyberprotection ».
   d. Importez la configuration téléchargée dans le client OpenVPN.
   e. Connectez-vous au client OpenVPN grâce à vos identifiants utilisateur Cyber Protect Cloud (voir l'étape 4 ci-dessus).
   f. [Facultatif] Si l'authentification à deux facteurs est activée pour votre organisation, alors vous devez fournir le code TOTP unique généré.

Important
Si vous activez l'authentification à deux facteurs pour votre compte, vous devez régénérer le fichier de configuration et le renouveler pour vos clients OpenVPN existants. Les utilisateurs doivent se reconnecter à Cyber Protect Cloud pour configurer l'authentification à deux facteurs pour leur compte.

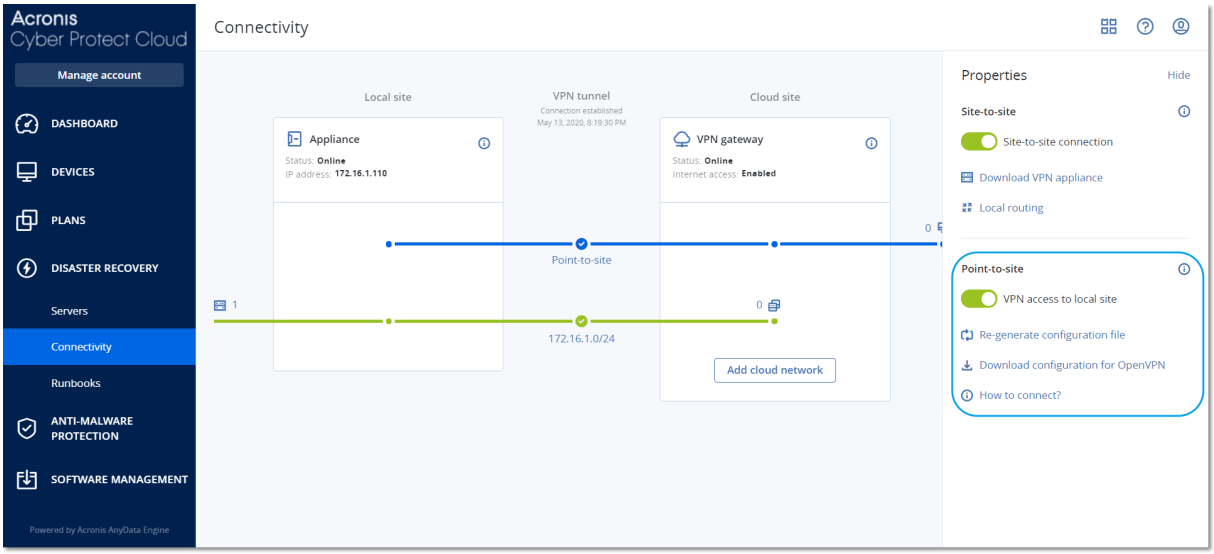
Vous pourrez ainsi vous connecter aux ordinateurs du site local.

© Acronis International GmbH, 2003-2026

Gestion des paramètres de la connexion de point à site

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**, puis cliquez sur **Afficher les propriétés** en haut à droite.



Accès VPN au site local

Cette option est utilisée pour gérer l'accès VPN au site local. Par défaut, elle est activée. Si elle est désactivée, l'accès point à site au site local ne sera pas autorisé.

Téléchargez la configuration pour OpenVPN

Cela lancera le téléchargement du fichier de configuration pour le client OpenVPN. Ce fichier est requis pour établir une connexion de point à site vers le site dans le Cloud.

Régénération de la configuration

Vous pouvez générer à nouveau le fichier de configuration pour le client OpenVPN.

Cela est nécessaire dans les cas suivants :

- Si vous pensez que le fichier de configuration est corrompu.
- L'authentification à deux facteurs a été activée pour votre compte.

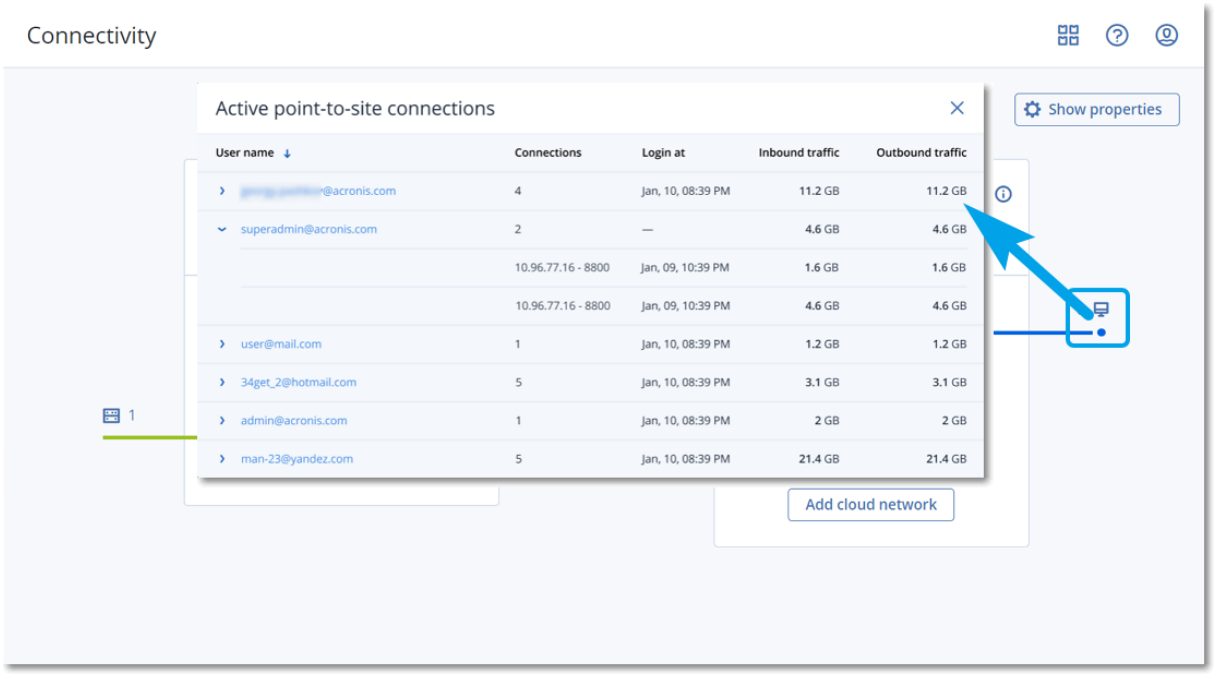
Dès que le fichier de configuration est mis à jour, il n'est plus possible de se connecter à l'aide de l'ancien fichier de configuration. Veillez à fournir le nouveau fichier aux utilisateurs autorisés à utiliser la connexion de point à site.

© Acronis International GmbH, 2003-2026

Connexions de point à site actives

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez consulter toutes les connexions point à point actives dans **Reprise d'activité après sinistre** > **Connectivité**. Cliquez sur l'icône de la machine sur la ligne bleue **Point à site** et vous pourrez consulter les informations détaillées sur les connexions point-à-site actives, groupées par nom d'utilisateur.



Recommandations pour la disponibilité des services de domaine Active Directory

Si vos ressources protégées ont besoin d'une authentification dans un contrôleur de domaine, nous vous recommandons de disposer d'une instance de contrôleur de domaine Active Directory sur le site de Disaster Recovery.

Contrôleur de domaine Active Directory pour la connectivité OpenVPN de couche 2

Avec la connectivité OpenVPN de couche 2, les adresses IP des ressources protégées sont conservées sur le site dans le Cloud lors d'un basculement test ou d'un basculement de la production. Par conséquent, lors d'un basculement test ou d'un basculement de la production, le contrôleur de domaine Active Directory possède la même adresse IP que dans le site local.

Grâce aux DNS personnalisés, vous pouvez définir votre propre serveur DNS personnalisé pour tous les serveurs Cloud. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 1062).

© Acronis International GmbH, 2003-2026

Contrôleur de domaine Active Directory pour la connectivité VPN IPsec de couche 3

Avec la connectivité VPN IPsec de couche 3, les adresses IP des ressources protégées ne sont pas conservées sur le site dans le Cloud. Par conséquent, nous vous recommandons de disposer d'une instance de contrôleur de domaine Active Directory supplémentaire en tant que serveur primaire sur le site dans le Cloud avant d'effectuer un basculement de la production.

Les recommandations pour une instance de contrôleur de domaine Active Directory dédiée et configurée en tant que serveur primaire sur le site dans le Cloud sont les suivantes :

- Désactivez le pare-feu Windows.
- Associez le serveur primaire au service Active Directory.
- Assurez-vous que le serveur primaire dispose d'un accès à Internet.
- Ajoutez la fonctionnalité Active Directory.

Grâce aux DNS personnalisés, vous pouvez définir votre propre serveur DNS personnalisé pour tous les serveurs Cloud. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 1062).

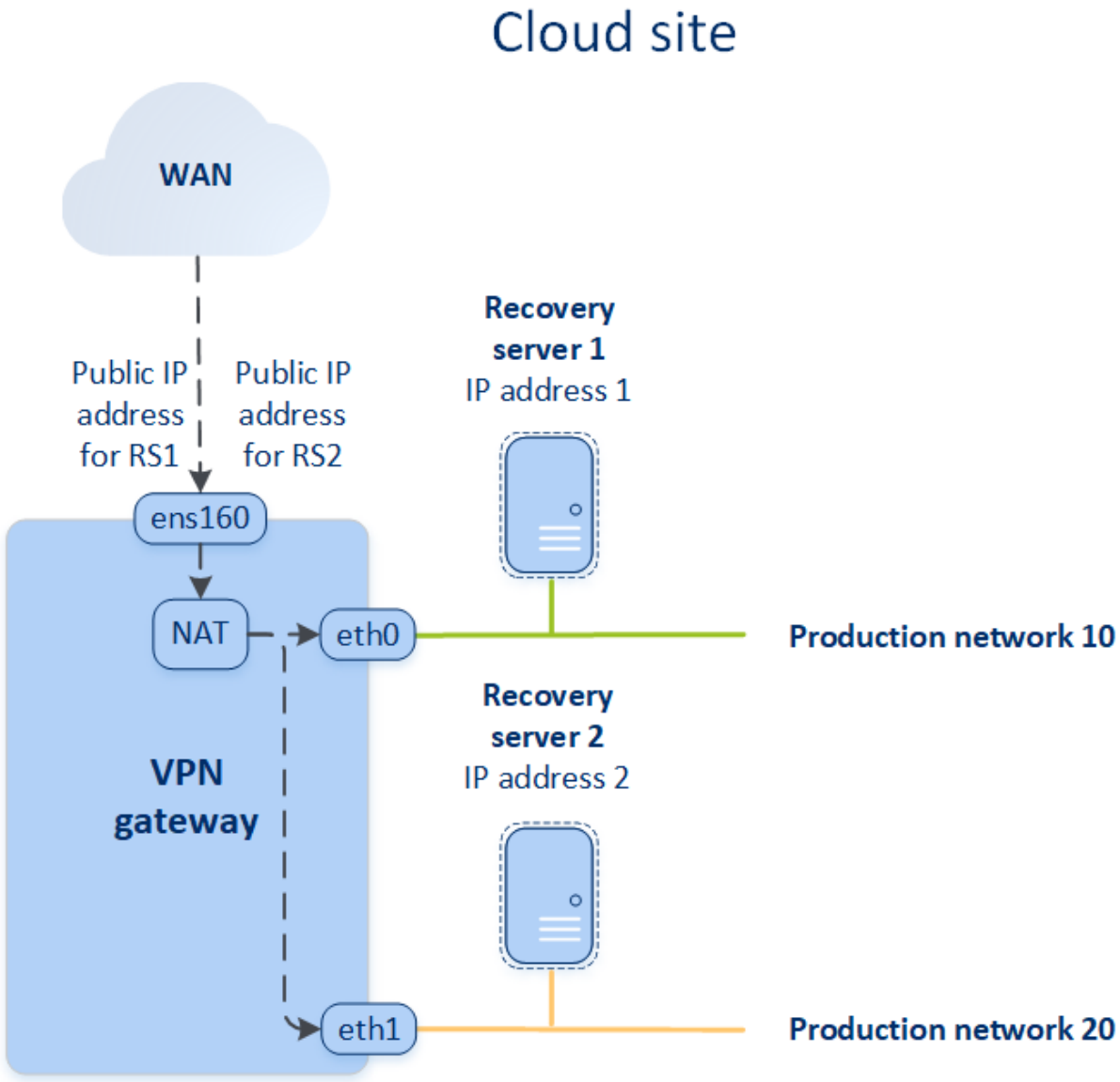
Gestion du réseau

Cette section décrit les scénarios de gestion des réseaux.

Adresses IP publique et de test

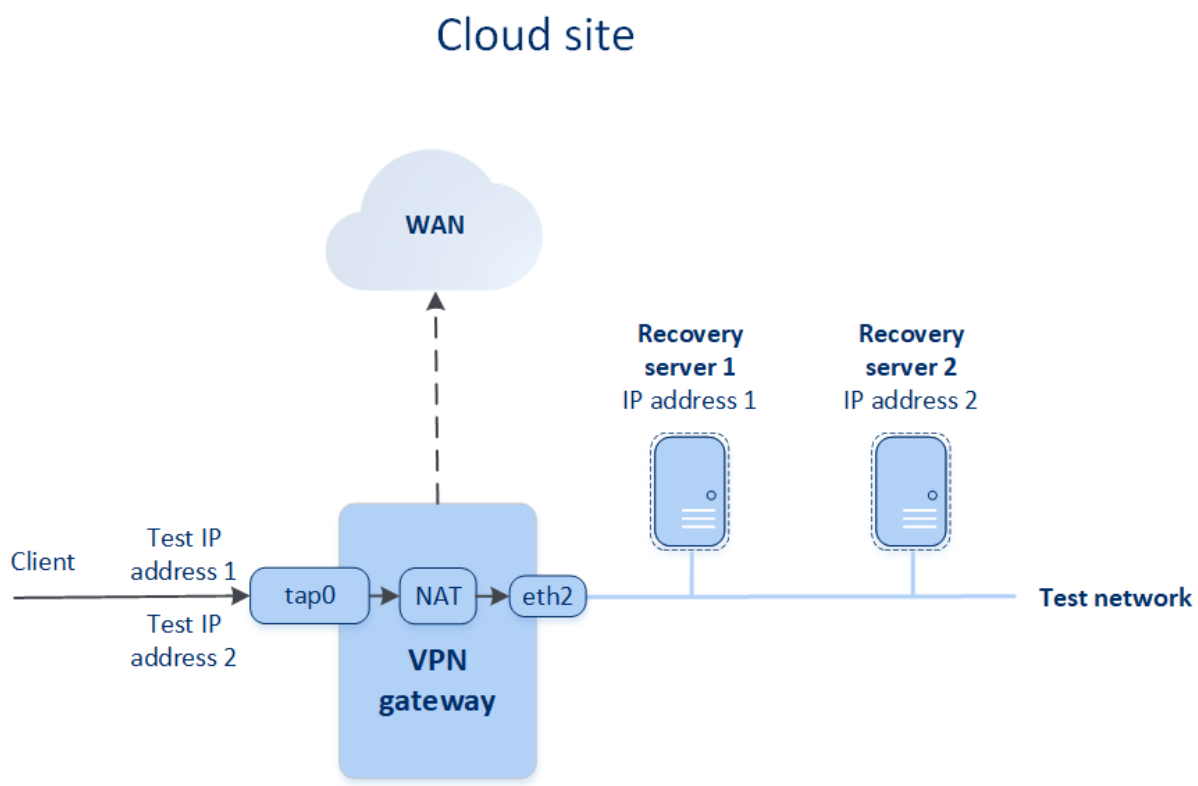
Si vous affectez l'adresse IP publique lors de la création d'un serveur de restauration, celui-ci devient disponible depuis Internet via cette adresse IP. Lorsqu'un paquet provenant d'Internet contient l'adresse IP publique de destination, la passerelle VPN le remappe à l'adresse IP de production associée en utilisant NAT, puis l'envoie au serveur de restauration correspondant.

© Acronis International GmbH, 2003-2026



Si vous affectez l'adresse IP de test lors de la création d'un serveur de restauration, ce serveur devient disponible dans le réseau de test via cette adresse IP. Lorsque vous effectuez le basculement test, l'ordinateur d'origine fonctionne toujours pendant le lancement simultané dans le cloud du serveur de restauration doté de la même adresse IP. Il n'existe aucun conflit d'adresse IP, car le réseau de test est isolé. Les serveurs de restauration du réseau de test sont accessibles avec leur adresse IP de test, qui est remappée aux adresses IP de production via NAT.

© Acronis International GmbH, 2003-2026



Pour plus d'informations à propos de l'Open VPN de site à site, consultez "OpenVPN de site à site – Informations complémentaires" (p. 1634).

Reconfiguration d'une adresse IP

Pour obtenir de bonnes performances de la reprise d'activité après sinistre, les adresses IP attribuées aux serveurs locaux et dans le Cloud doivent être cohérentes. S'il existe la moindre incohérence ou incompatibilité dans les adresses IP, vous verrez le point d'exclamation à côté du réseau correspondant dans **Disaster Recovery** > **Connectivité**.

Voici ci-dessous certains des motifs connus d'incohérence des adresses IP :

1. Un serveur de restauration a été migré d'un réseau à l'autre ou le masque du réseau ou le réseau cloud a été modifié. En conséquence, les serveurs cloud ont les adresses IP des réseaux auxquels ils ne sont pas connectés.
2. Le type de connectivité a été basculé de « sans connexion de site à site » à « connexion de site à site ». En conséquence, un serveur local est placé dans le réseau différent de celui ayant été créé pour le serveur de restauration dans le site dans le Cloud.
3. Le type de connectivité est passé d'OpenVPN de site à site à VPN IPsec multisite, ou de VPN IPsec multisite à OpenVPN de site à site. Pour plus d'informations sur ces scénarios, voir Basculement de connexions "Passage d'un VPN IPsec multisite à un VPN OpenVPN site à site" (p. 1048) et Réaffectation d'adresses IP.
4. Modification des paramètres de réseau suivants sur le site du matériel VPN :

© Acronis International GmbH, 2003-2026

- Ajout d'une interface via les paramètres du réseau
- Modification manuelle du masque du réseau via les paramètres de l'interface
- Modification du masque et de l'adresse du réseau via DHCP
- Modification manuelle de l'adresse et du masque du réseau via les paramètres de l'interface
- Modification du masque et de l'adresse du réseau via DHCP

En conséquence des actions répertoriées ci-dessus, le réseau du site dans le Cloud peut devenir un sous-ensemble ou un super-ensemble du réseau local, ou l'interface du matériel VPN peut rapporter les mêmes paramètres réseau pour différentes interfaces.

Pour résoudre le problème à l'aide de paramètres réseau

1. Cliquez sur le réseau nécessitant la reconfiguration d'une adresse IP.
   Vous verrez la liste des serveurs du réseau sélectionné, leur statut et leur adresse IP. Les serveurs dont les paramètres réseau sont incohérents sont identifiés par un point d'exclamation.
2. Pour modifier les paramètres réseau d'un serveur, cliquez sur **Accéder au serveur**. Pour modifier les paramètres réseau de tous les serveurs en même temps, cliquez sur **Modifier** dans le bloc de notification.
3. Modifiez les adresses IP au besoin en les définissant dans les champs **Nouvelle adresse IP** et **Nouvelle adresse IP test**.
4. Lorsque vous avez terminé, cliquez sur **Confirmer**.

Déplacer des serveurs vers un réseau approprié

Lorsque vous créez un plan de protection de reprise d'activité après sinistre et que vous l'appliquez aux terminaux sélectionnés, le système vérifie les adresses IP des terminaux et crée automatiquement des réseaux cloud s'il n'existe aucun réseau cloud correspondant à l'adresse IP. Par défaut, les réseaux cloud sont configurés avec les plages maximales recommandées par IANA pour un usage privé (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Vous pouvez restreindre la taille de votre réseau en modifiant le masque de réseau.

Dans le cas où les terminaux sélectionnés se trouvent sur plusieurs réseaux locaux, le réseau sur le site dans le cloud peut devenir un superensemble de réseaux locaux. Dans ce cas, pour reconfigurer les réseaux cloud :

1. Cliquez sur le réseau Cloud qui requiert la reconfiguration de la taille du réseau, puis cliquez sur **Modifier**.
2. Reconfigurez la taille du réseau à l'aide des paramètres corrects.
3. Créez les autres réseaux requis.
4. Cliquez sur l'icône de notification à côté du nombre de terminaux connectés au réseau.
5. Cliquez sur **Déplacer vers un réseau approprié**.
6. Sélectionnez les serveurs que vous souhaitez déplacer, puis cliquez sur **Déplacer**.

© Acronis International GmbH, 2003-2026

Réaffectation d'adresses IP

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous devez réaffecter les adresses IP des réseaux Clouds, ainsi que les serveurs Cloud, afin de terminer la configuration dans les cas suivants :

- Après être passé d'une connectivité OpenVPN de site à site à une connectivité VPN IPsec multi-site ou vice-versa.
- Après avoir appliqué un plan de protection (si la connectivité VPN IPsec multi-site est configurée).

Réseau dans le Cloud

Pour réaffecter l'adresse IP d'un réseau Cloud

1. Dans l'onglet **Connectivité**, cliquez sur l'adresse IP du réseau Cloud.
2. Dans la fenêtre contextuelle **Réseau**, cliquez sur **Modifier**.
3. Tapez la nouvelle adresse et le nouveau masque du réseau.
4. Cliquez sur **Terminé**.

Une fois que vous avez réaffecté l'adresse IP d'un réseau Cloud, vous devez réaffecter les serveurs Cloud qui appartiennent au réseau Cloud réaffecté.

Serveur Cloud

Pour réaffecter l'adresse IP d'un serveur

1. Dans l'onglet **Connectivité**, cliquez sur l'adresse IP du serveur dans le réseau Cloud.
2. Dans la fenêtre contextuelle **Serveurs**, cliquez sur **Changer l'adresse IP**.
3. Dans la fenêtre contextuelle **Changer l'adresse IP**, tapez la nouvelle adresse IP du serveur, ou utilisez l'adresse IP générée automatiquement et qui fait partie du réseau Cloud réaffecté.

   Remarque
   Disaster Recovery affecte automatiquement les adresses IP du réseau Cloud à tous les serveurs Cloud qui en font partie, avant la réaffectation de l'adresse IP du réseau. Vous pouvez vous servir des adresses IP suggérées pour réaffecter simultanément l'adresse IP de tous les serveurs Cloud.

4. Cliquez sur **Confirmer**.

Réinstallation de la passerelle VPN

En cas de problème de passerelle VPN que vous ne parvenez pas à résoudre, vous souhaiterez peut-être réinstaller la passerelle. Voici quelques problèmes possibles :

© Acronis International GmbH, 2003-2026

- La passerelle VPN est dans l'état **Erreur**.
- La passerelle VPN est dans l'état **En attente** depuis longtemps.
- La passerelle VPN est dans un état indéterminé depuis longtemps.

La réinstallation de la passerelle VPN comprend les actions automatiques suivantes : suppression totale de la machine virtuelle de la passerelle VPN existante ; installation d'une nouvelle machine virtuelle à partir du modèle et application des paramètres de la passerelle VPN précédente sur la nouvelle machine virtuelle.

Prérequis

Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour réinstaller la passerelle VPN

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur l'icône en forme d'engrenage de la passerelle VPN, puis sélectionnez **Réinstaller la passerelle VPN**.
3. Dans la boîte de dialogue **Réinstaller la passerelle VPN**, saisissez votre identifiant.
4. Cliquez sur **Réinstaller**.

Configuration de serveurs DNS personnalisés

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsque vous configurez une connectivité, Disaster Recovery crée l'infrastructure cloud de votre réseau. Le serveur DHCP cloud assigne automatiquement des serveurs DNS par défaut aux serveurs de restauration et aux serveurs primaires, mais vous pouvez modifier les paramètres par défaut et configurer des serveurs DNS personnalisés. Les nouveaux paramètres DNS seront appliqués lors de la prochaine demande adressée au serveur DHCP.

Prérequis

Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour configurer un serveur DNS personnalisé

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Par défaut (fourni par le site dans le Cloud)**.
4. Sélectionnez **Serveurs personnalisés**.
5. Saisissez l'adresse IP du serveur DNS.
6. [Facultatif] Si vous souhaitez ajouter un autre serveur DNS, cliquez sur **Ajouter**, puis saisissez l'adresse IP du serveur DNS.

© Acronis International GmbH, 2003-2026

Remarque
Une fois que vous avez ajouté les serveurs DNS personnalisés, vous pouvez aussi ajouter les serveurs DNS par défaut. De cette manière, si les serveurs DNS personnalisés sont indisponibles, Disaster Recovery utilisera les serveurs DNS par défaut.

7. Cliquez sur **Terminé**.

Suppression de serveurs DNS personnalisés

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez supprimer des serveurs DNS à partir de la liste des DNS personnalisés.

Prérequis

Des serveurs DNS personnalisés sont configurés.

Pour supprimer un serveur DNS personnalisé

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Serveurs personnalisés**.
4. Cliquez sur l'icône de suppression à côté du serveur DNS.

Remarque
L'option de suppression est désactivée lorsqu'un seul serveur DNS est disponible. Si vous souhaitez supprimer tous les serveurs DNS personnalisés, sélectionnez **Par défaut (fourni par le site dans le Cloud)**.

5. Cliquez sur **Terminé**.

Configuration du routage local

En plus d'étendre vos réseaux locaux au Cloud via l'appliance VPN, vous pouvez posséder d'autres réseaux locaux qui ne sont pas enregistrés dans l'appliance VPN, mais qui possèdent des serveurs qui doivent communiquer avec les serveurs Cloud. Pour établir la connectivité entre ces serveurs locaux et les serveurs dans le Cloud, vous devez configurer les paramètres de routage local.

Pour configurer le routage local

1. Accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**, puis sur **Routage local**.
3. Indiquez les réseaux locaux dans la notation CIDR.
4. Cliquez sur **Enregistrer**.

© Acronis International GmbH, 2003-2026

En conséquence, les serveurs des réseaux locaux indiqués pourront communiquer avec les serveurs dans le Cloud.

Téléchargement d'adresses MAC

Vous pouvez télécharger une liste d'adresses MAC, puis les extraire et les importer dans la configuration de votre serveur DHCP personnalisé.

Prérequis

- Vous devez définir au moins un type de connectivité vers le site dans le Cloud.
- Au moins un serveur primaire ou serveur de restauration avec une adresse MAC doit être configuré.

Télécharger la liste des adresses MAC

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Télécharger la liste des adresses MAC**, puis enregistrez le fichier CSV.

Utilisation des journaux

Disaster Recovery collecte les fichiers journaux pour l'appliance VPN et la passerelle VPN. Ces journaux sont enregistrés sous forme de fichiers .txt, qui sont compressés dans une archive .zip. Vous pouvez télécharger et extraire l'archive, puis vous servir des informations qu'elle contient à des fins de dépannage et de surveillance.

La liste suivante décrit les fichiers journaux qui font partie de l'archive zip, et les informations qu'ils contiennent.

`dnsmasq.config.txt` : le fichier contient des informations sur la configuration du service qui fournit les adresses DNS et DHCP.

`dnsmasq.leases.txt` : le fichier contient des informations sur les locations d'adresses DHCP actuelles.

`dnsmasq_log.txt` : le fichier contient les journaux du service dnsmasq.

`ebtables.txt` : le fichier contient des informations sur les tables de pare-feu.

`free.txt` : le fichier contient des informations sur la mémoire libre.

`ip.txt` : le fichier contient les journaux de la configuration des interfaces réseau, y compris leur nom pouvant être utilisé dans la configuration des paramètres **Capturer des paquets réseau**.

`NetworkManager_log.txt` : le fichier contient les journaux du service NetworkManager.

`NetworkManager_status.txt` : le fichier contient des informations sur l'état du service NetworkManager.

`openvpn@p2s_log.txt` : le fichier contient les journaux du service OpenVPN.

`openvpn@p2s_status.txt` : le fichier contient des informations sur l'état des tunnels VPN.

© Acronis International GmbH, 2003-2026

`ps.txt` : le fichier contient des informations sur les processus en cours d'exécution de la passerelle VPN ou de l'appliance VPN.

`resolf.conf.txt` : le fichier contient des informations sur la configuration des serveurs DNS.

`routes.txt` : le fichier contient des informations de routage réseau.

`uname.txt` : le fichier contient des informations sur la version actuelle du noyau du système d'exploitation.

`uptime.txt` : le fichier contient des informations sur la durée pendant laquelle le système d'exploitation n'a pas été redémarré.

`vpnserver_log.txt` : le fichier contient les journaux du service VPN.

`vpnserver_status.txt` : le fichier contient des informations sur l'état du serveur VPN.

Pour plus d'informations sur les fichiers journaux propres à la connectivité VPN IPsec, reportez-vous à "Fichiers journaux VPN IPsec multi-site" (p. 1052).

Téléchargement des journaux de l'appliance VPN

Vous pouvez télécharger et extraire l'archive qui contient les journaux de l'appliance VPN, puis vous servir des informations qu'elle contient à des fins de dépannage et de surveillance.

Télécharger les journaux de l'appliance VPN

1. Sur la page **Connectivité**, cliquez sur l'icône en forme d'engrenage à côté de l'appliance VPN.
2. Cliquez sur le bouton **Télécharger le journal**.
3. [Facultatif] Sélectionnez **Capturer des paquets réseau**, puis configurez les paramètres. Pour plus d'informations, voir "Capture des paquets réseau" (p. 1066).
4. Cliquez sur **Terminé**.
5. Lorsque l'archive .zip est prête à être téléchargée, cliquez sur **Télécharger le journal**, puis enregistrez-la au niveau local.

Téléchargement des journaux de la passerelle VPN

Vous pouvez télécharger et extraire l'archive qui contient les journaux de la passerelle VPN, puis vous servir des informations qu'elle contient à des fins de dépannage et de surveillance.

Télécharger les journaux de la passerelle VPN

1. Sur la page **Connectivité**, cliquez sur l'icône en forme d'engrenage à côté de la passerelle VPN.
2. Cliquez sur le bouton **Télécharger le journal**.
3. [Facultatif] Sélectionnez **Capturer des paquets réseau**, puis configurez les paramètres. Pour plus d'informations, voir "Capture des paquets réseau" (p. 1066).
4. Cliquez sur **Terminé**.
5. Lorsque l'archive .zip est prête à être téléchargée, cliquez sur **Télécharger le journal**, puis enregistrez-la au niveau local.

© Acronis International GmbH, 2003-2026

Capture des paquets réseau

Pour dépanner et analyser la communication entre le site de production local et un serveur principal ou de restauration, vous pouvez choisir de collecter les paquets réseau sur la passerelle VPN ou sur l'appliance VPN.

Une fois les 32 000 paquets réseau collectés ou la durée limite atteinte, la capture des paquets réseau s'arrête et les résultats sont écrits dans un fichier .libpcap ajouté dans l'archive .zip des journaux.

Le tableau suivant fournit plus de détails sur les paramètres **Capturer des paquets réseau** que vous pouvez configurer.

Paramètre	Description
Nom de l'interface réseau	L'interface réseau sur laquelle capturer des paquets réseau. Si vous souhaitez capturer des paquets réseau sur toutes les interfaces réseau, sélectionnez **Toutes**.
Limite de temps (secondes)	La limite de temps pour la capture des paquets réseau. La valeur maximale que vous pouvez définir est 1 800.
Filtrage	Un filtre supplémentaire à appliquer aux paquets réseau capturés. Vous pouvez saisir une chaîne contenant des protocoles, des ports, des instructions et leurs combinaisons, séparés par une espace, par exemple : « and », « or », « not », « (« , ») », « src », « dst », « net », « host », « port », « ip », « tcp », « udp », « icmp », « arp » et « esp ». Si vous souhaitez utiliser des parenthèses, entourez-les d'espaces. Vous pouvez également saisir des adresses IP et des adresses réseau, par exemple : « icmp or arp » et « port 67 or 68 ». Pour plus d'informations sur les valeurs que vous pouvez saisir, consultez l'aide Linux tpcdump.

Serveurs Cloud

Avec Disaster Recovery vers Cyber Protect Cloud, vous pouvez utiliser deux types de serveurs dans le cloud : primaires et de restauration.

Un serveur primaire est une machine virtuelle qui n'est pas liée à un ordinateur sur le site local. Vous pouvez utiliser des serveurs primaires pour protéger une application spécifique ou exécuter divers services auxiliaires (tels qu'un serveur Web).

Un serveur de restauration est une machine virtuelle qui est une réplique de la machine d'origine (serveur protégé). Le serveur de restauration est basé sur les sauvegardes du serveur protégé qui sont stockées dans le cloud. En cas de sinistre, les serveurs de restauration sont utilisés pour basculer les charges de travail des serveurs d'origine.

© Acronis International GmbH, 2003-2026

Configuration des serveurs de restauration

Un **serveur de restauration** : un réplica de la machine d'origine, basé sur les sauvegardes de serveur protégées stockées dans le Cloud. Les serveurs de restauration sont utilisés pour remplacer les ressources depuis les serveurs originaux en cas de sinistre.

Lorsque vous créez un serveur de restauration, vous devez préciser les paramètres de réseau suivants :

Paramètre	Description
Réseau cloud	(obligatoire) Réseau cloud auquel un serveur de restauration sera connecté.
Adresse IP en réseau de production	(obligatoire) : adresse IP de lancement d'une machine virtuelle pour un serveur de restauration. Cette adresse est utilisée dans les réseaux de test et de production. Avant le lancement, la machine virtuelle est configurée de façon à récupérer l'adresse IP via DHCP.
Adresse IP de test	(facultative) : adresse IP permettant d'accéder au serveur de restauration depuis le réseau client-production lors d'un basculement test et évitant la duplication de l'adresse IP de test dans le même réseau. Cette adresse IP est différente de l'adresse IP du réseau de production. Les serveurs du site local peuvent accéder aux serveurs de restauration lors du basculement test via l'adresse IP de test. L'accès inverse n'est cependant pas disponible. Une connexion Internet depuis le serveur de restauration dans le réseau de test est disponible si l'option **Accès Internet** a été choisie lors de la création du serveur de restauration.
Adresse IP publique	(facultative) : adresse IP permettant d'accéder au serveur de restauration depuis Internet. Si un serveur ne possède pas d'adresse IP publique, vous pouvez y accéder uniquement depuis le réseau local.
Accès Internet	(facultative) : adresse permettant au serveur de restauration d'accéder à Internet (aussi bien dans les cas de basculement test qu'en production).

Création d'un serveur de restauration

Pour créer un serveur de restauration qui sera une copie de votre ressource, procédez comme suit. Vous pouvez aussi regarder le tutoriel vidéo qui présente le processus.

© Acronis International GmbH, 2003-2026

Important
Lorsque vous effectuez un basculement, vous ne pouvez sélectionner que les points de restauration qui ont été créés après la création du serveur de restauration.

Prérequis

- Un plan de protection doit être appliqué à la machine d'origine que vous souhaitez protéger. Ce plan peut sauvegarder l'intégralité de la machine ou uniquement les disques requis pour le démarrage et la fourniture des services nécessaires à un stockage dans le Cloud.
- Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour créer un serveur de restauration

1. Dans l'onglet **Tous les terminaux**, sélectionnez l'ordinateur que vous voulez protéger.
2. Cliquez sur **Reprise d'activité après sinistre**, puis sur **Créer un serveur de restauration**.
3. Dans l'Assistant **Créer un serveur de restauration**, onglet **Configuration du serveur**, procédez comme suit :
   a. Sélectionnez le nombre de cœurs virtuels et la taille de la RAM.

      Remarque
      Vous pouvez voir les points de calcul de chaque option. Le nombre de points de calcul traduit le coût horaire de l'exécution du serveur de restauration. Pour plus d'informations, voir "Points de calcul" (p. 1082).

   b. [Facultatif] Modifiez le nom par défaut du serveur de restauration.
   c. [Facultatif] Ajoutez une description.
4. Dans l'onglet **Réseau**, procédez comme suit :
   a. Indiquez le serveur Cloud auquel le serveur sera connecté.
   b. Sélectionnez l'option **DHCP**.

Option DHCP	Description
Fourni par le site dans le cloud	Il s'agit du paramètre par défaut. L'adresse IP du serveur sera fournie par un serveur DHCP configuré automatiquement dans le cloud.
Personnalisé	L'adresse IP du serveur sera fournie par votre propre serveur DHCP dans le cloud.

   c. Spécifiez l'**Adresse MAC**.
      L'adresse MAC est un identificateur unique attribué à la carte réseau du serveur. Si vous utilisez un DHCP personnalisé, vous pouvez le configurer pour attribuer systématiquement une adresse IP spécifique à une adresse MAC donnée. De cette façon, vous vous assurez que le serveur de restauration aura toujours la même adresse IP. Vous pouvez exécuter des applications possédant des licences enregistrées avec l'adresse MAC.

© Acronis International GmbH, 2003-2026

d. Indiquez l'adresse IP que le serveur aura dans le réseau de production. Par défaut, l'adresse IP de la machine d'origine est sélectionnée.

Remarque
Si vous utilisez un serveur DHCP, ajoutez cette adresse IP à la liste d'exclusion du serveur, afin d'éviter les conflits d'adresse IP.
Si vous utilisez un serveur DHCP personnalisé, l'adresse IP que vous spécifiez dans **Adresse IP en réseau de production** doit être la même que celle configurée dans le serveur DHCP. Dans le cas contraire, le basculement test ne fonctionnera pas correctement, et il ne sera pas possible d'accéder au serveur via une adresse IP publique.

e. [Facultatif] Activez la case à cocher **Adresse IP test**, puis saisissez l'adresse IP.
Si vous sélectionnez ce paramètre, vous pourrez tester un basculement dans le réseau de test isolé et vous connecter au serveur de restauration via RDP ou SSH lors d'un basculement test. En mode de basculement test, la passerelle VPN remplace l'adresse IP de test par l'adresse IP de production au moyen du protocole NAT.
Si vous ne sélectionnez pas le paramètre, la console sera le seul moyen d'accéder au serveur lors d'un basculement test.

Remarque
Si vous utilisez un serveur DHCP, ajoutez cette adresse IP à la liste d'exclusion du serveur afin d'éviter les conflits d'adresse IP.

Vous pouvez sélectionner l'une des adresses IP proposées ou en saisir une autre.

f. [Facultatif] Activez la case à cocher **Accès Internet**.
Si vous sélectionnez ce paramètre, le serveur de restauration aura accès à Internet lors d'un basculement en environnement de production ou d'un basculement test. Par défaut, le port TCP 25 est ouvert pour les connexions sortantes vers des adresses IP publiques.

g. [Facultatif] Activez la case à cocher **Utiliser une adresse IP publique**.
Avec une adresse IP publique, le serveur de restauration devient accessible depuis Internet pendant un basculement ou un basculement test. Si vous ne sélectionnez pas cette option, le serveur sera disponible uniquement dans votre réseau de production.
L'option **Utiliser une adresse IP publique** nécessite que l'option **Accès Internet** soit sélectionnée.
L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes vers des adresses IP publiques.

Remarque
Si vous désélectionnez la case **Utiliser une adresse IP publique** ou supprimez le serveur de restauration, son adresse IP publique n'est pas réservée.

5. Dans l'onglet **Paramètres**, sélectionnez **Définir le seuil de l'objectif de point de restauration (RPO)**, puis définissez la valeur.

© Acronis International GmbH, 2003-2026

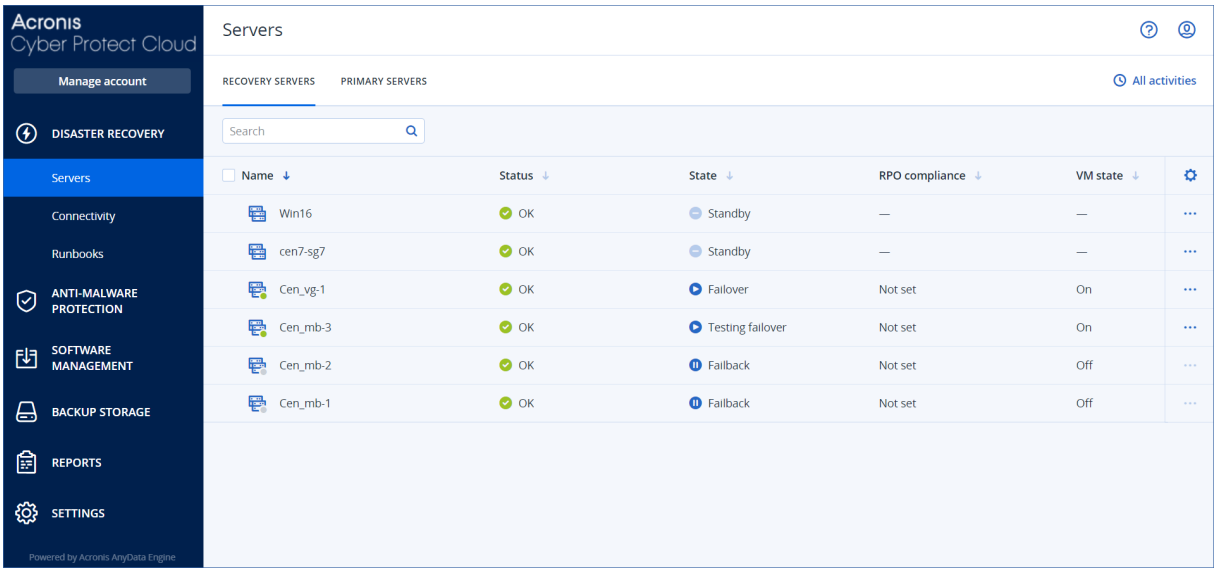
Le seuil des objectifs de point de restauration définit l'intervalle de temps maximum entre le dernier point de restauration convenant à un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.

6. [Facultatif] [Si les sauvegardes pour l'ordinateur sélectionné sont chiffrées à l'aide du chiffrement comme propriété de l'ordinateur] Spécifiez le mot de passe qui sera utilisé automatiquement lors de la création d'une machine virtuelle pour le serveur de restauration à partir de la sauvegarde chiffrée.
   a. Cliquez sur **Saisir le mot de passe**, puis saisissez le mot de passe de la sauvegarde chiffrée et définissez un nom pour les identifiants.
      Par défaut, la liste affiche la sauvegarde la plus récente.
   b. Pour afficher toutes les sauvegardes, sélectionnez **Afficher toutes les sauvegardes**.
   c. Cliquez sur **Enregistrer**.

Remarque
Le mot de passe que vous spécifiez sera stocké dans un magasin d'identifiants sécurisé, mais l'enregistrement des mots de passe peut être contraire à vos obligations de conformité.

7. Dans l'onglet **Règles de pare-feu du cloud**, modifiez les règles de pare-feu par défaut. Pour plus d'informations, voir "Définition de règles de pare-feu pour les serveurs Cloud" (p. 1078).
8. Cliquez sur **Créer**.

Le serveur de restauration apparaît dans l'onglet **Disaster Recovery** > **Serveurs** > **Serveurs de restauration** de la console Cyber Protect.



Opérations liées aux serveurs de restauration

Dans la console Cyber Protect, les serveurs primaires sont affichés dans l'onglet **Disaster Recovery** > **Serveurs** > **Serveurs de restauration**.

Mettre sous tension

© Acronis International GmbH, 2003-2026

Pour mettre un serveur de restauration sous tension

1. Dans l'onglet **Serveurs de restauration**, cliquez sur le serveur de restauration.
2. Cliquez sur **Mettre sous tension**.

Mise hors tension

Pour mettre un serveur de restauration hors tension

1. Dans l'onglet **Serveurs de restauration**, cliquez sur le serveur de restauration.
2. Cliquez sur **Mise hors tension**.
3. Dans l'écran **Mettez le serveur hors tension**, cliquez sur **Arrêter**.

Arrêt forcé

Pour forcer la mise hors tension d'un serveur de restauration

1. Dans l'onglet **Serveurs de restauration**, cliquez sur le serveur de restauration.
2. Cliquez sur **Mise hors tension**.
3. Dans l'écran **Mettez le serveur hors tension**, sélectionnez **Forcer l'arrêt du serveur**, puis cliquez sur **Arrêter**.

Arrêter

Pour arrêter un serveur de restauration

1. Dans l'onglet **Serveurs de restauration**, cliquez sur le serveur de restauration.
2. Cliquez sur **Arrêter**.

Modifier les paramètres

Pour modifier les paramètres d'un serveur de restauration

1. Dans l'onglet **Serveurs de restauration**, cliquez sur le serveur de restauration.
2. Cliquez sur **Arrêter**.
3. Cliquez sur **Modifier**, puis modifiez les paramètres.

Appliquez un plan de protection

Pour appliquer un plan à un serveur primaire

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Dans l'onglet **Plan**, cliquez sur **Créer**.
   Vous verrez un plan de protection prédéfini dans lequel vous ne pouvez modifier que la planification et les règles de rétention. Pour plus d'informations, voir Sauvegarde des serveurs dans le cloud.

© Acronis International GmbH, 2003-2026

Configuration des serveurs primaires

Un **serveur primaire** est une machine virtuelle qui ne possède pas d'ordinateur associé sur le site local, par rapport à un serveur de restauration. Les serveurs primaires servent à protéger une application par réplication, ou à exécuter divers services auxiliaires (tels qu'un serveur Web).

Généralement, un serveur primaire est utilisé pour la réplication des données en temps réel entre des serveurs exécutant des applications cruciales. Vous configurez vous-même la réplication à l'aide des outils natifs de l'application. Par exemple, la réplication Active Directory ou la réplication SQL peuvent être configurées entre les serveurs locaux et le serveur primaire.

Un serveur primaire peut également être inclus dans un groupe AlwaysOn Availability Group (AAG) ou dans un groupe de disponibilité de la base de données (DAG).

Ces méthodes nécessitent toutes les deux une connaissance approfondie de l'application, ainsi que les droits d'administrateur correspondants. Un serveur primaire consomme en continu des ressources de calcul et de l'espace sur le stockage rapide pour reprise d'activité après sinistre. Il nécessite une maintenance de votre côté : suivi de la réplication, installation des mises à jour logicielles et sauvegarde. Les avantages sont des RTO et RPO minimales, avec une faible charge sur l'environnement de production (comparé à la sauvegarde de serveurs entiers dans le Cloud).

Les serveurs primaires sont toujours lancés uniquement dans le réseau de production et possèdent les paramètres réseau suivants :

Paramètre	Description
Réseau cloud	(obligatoire) : réseau cloud auquel un serveur primaire sera connecté.
Adresse IP en réseau de production	(obligatoire) Adresse IP du serveur dans le réseau de production. Par défaut, il s'agit de la première adresse IP disponible de votre réseau de production.
Adresse IP publique	(facultative) Adresse IP permettant d'accéder au serveur primaire depuis Internet. Si un serveur ne possède pas d'adresse IP publique, vous pouvez y accéder uniquement depuis le réseau local, pas via Internet.
Accès Internet	(facultative) : permet à un serveur primaire d'accéder à Internet.

Création d'un serveur primaire

Prérequis

Vous devez définir au moins un type de connectivité vers le site dans le Cloud.

Pour créer un serveur primaire

1. Accédez à l'onglet **Disaster Recovery** > **Serveurs** > **Serveurs primaires**.
2. Cliquez sur **Créer**.

© Acronis International GmbH, 2003-2026

3. Dans l'assistant **Créer un serveur primaire**, onglet **Configuration du serveur**, procédez comme suit :
   a. Sélectionnez un modèle pour la nouvelle machine virtuelle.
   b. Sélectionnez le type de configuration (nombre de cœurs virtuels et taille de la RAM).
      Le tableau suivant indique la quantité maximale d'espace disque (en Go) pour chaque configuration.

Type	vCPU	RAM (Go)	Quantité maximale d'espace disque (Go)
F1	1	2	500
F2	1	4	1,000
F3	2	8	2,000
F4	4	16	4,000
F5	8	32	8,000
F6	16	64	16,000
F7	16	128	32,000
F8	16	256	64,000

   c. [Facultatif] Modifiez la taille du disque virtuel. Si vous avez besoin de plus d'un disque dur, cliquez sur **Ajouter un disque**, puis indiquez la taille du nouveau disque. Vous pouvez ajouter jusqu'à 10 disques pour un serveur primaire.
   d. Modifiez le nom par défaut du serveur de restauration.
   e. Ajoutez une description.
4. Dans l'onglet **Réseau**, procédez comme suit :
   a. Indiquez le réseau Cloud dans lequel le serveur primaire sera inclus.
   b. Sélectionnez l'option **DHCP**.

Option DHCP	Description
Fourni par le site dans le cloud	Il s'agit du paramètre par défaut. L'adresse IP du serveur sera fournie par un serveur DHCP configuré automatiquement dans le cloud.
Personnalisé	L'adresse IP du serveur sera fournie par votre propre serveur DHCP dans le cloud.

   c. Spécifiez l'**Adresse MAC**.
      L'adresse MAC est un identificateur unique attribué à l'adaptateur réseau du serveur. Si vous utilisez un DHCP personnalisé, vous pouvez le configurer pour toujours attribuer des adresses IP spécifiques à une adresse MAC donnée. Le serveur primaire obtient ainsi toujours la même adresse IP. Vous pouvez exécuter des applications possédant des licences enregistrées avec l'adresse MAC.

© Acronis International GmbH, 2003-2026

d. Indiquez l'adresse IP que le serveur aura dans le réseau de production.

   Par défaut, la première adresse IP gratuite issue de votre réseau de production est définie.

   Remarque

   Si vous utilisez un serveur DHCP, ajoutez cette adresse IP à la liste d'exclusion du serveur, afin d'éviter les conflits d'adresse IP.

   Si vous utilisez un serveur DHCP personnalisé, l'adresse IP que vous spécifiez dans **Adresse IP en réseau de production** doit être la même que celle configurée dans le serveur DHCP. Dans le cas contraire, le basculement test ne fonctionnera pas correctement, et il ne sera pas possible d'accéder au serveur via une adresse IP publique.

e. [Facultatif] Activez la case à cocher **Accès Internet**.

   Si vous sélectionnez cette option, le serveur primaire aura accès à Internet. Par défaut, le port TCP 25 est ouvert pour les connexions sortantes vers des adresses IP publiques.

f. [Facultatif] Activez la case à cocher **Utiliser une adresse IP publique**.

   Avec une adresse IP publique, le serveur primaire devient accessible depuis Internet. Si vous ne sélectionnez pas ce paramètre, le serveur sera disponible uniquement dans votre réseau de production.

   L'adresse IP publique s'affichera une fois la configuration terminée. Par défaut, le port TCP 443 est ouvert pour les connexions entrantes vers des adresses IP publiques.

   Remarque

   Si vous désélectionnez la case **Utiliser une adresse IP publique** ou supprimez le serveur de restauration, son adresse IP publique n'est pas réservée.

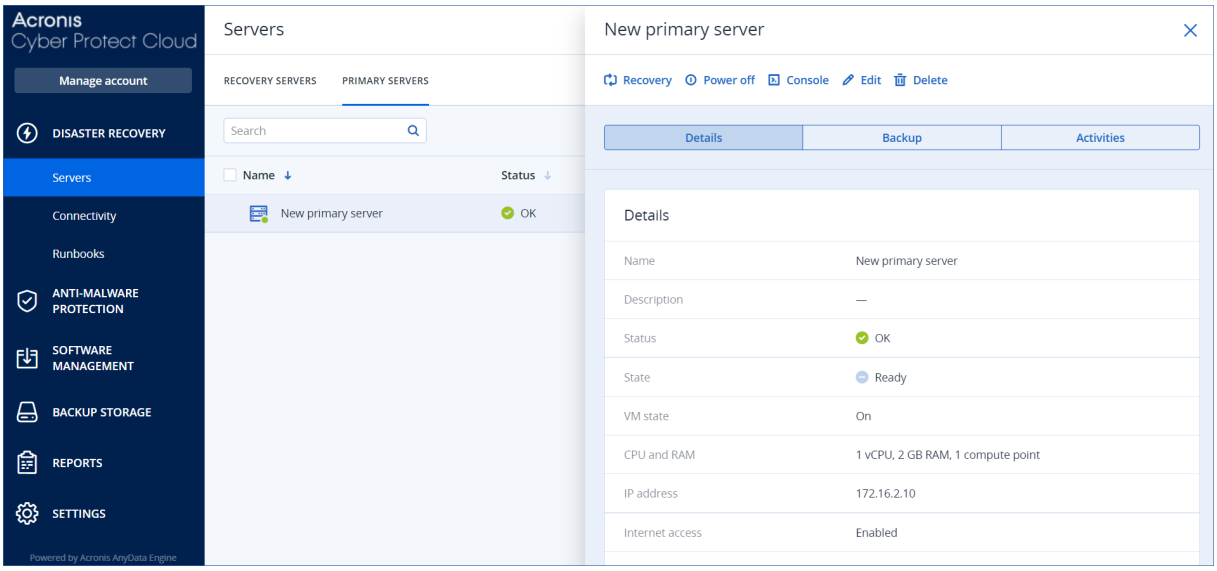
5. [Facultatif] Dans l'onglet **Paramètres**, sélectionnez **Définir le seuil de l'objectif de point de restauration (RPO)**, puis définissez la valeur.

   Le seuil des objectifs de point de restauration (RPO) définit l'intervalle de temps maximum entre le dernier point de restauration et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.

6. [Facultatif] Dans l'onglet **Règles de pare-feu du cloud**, modifiez les règles de pare-feu par défaut. Pour plus d'informations, voir "Définition de règles de pare-feu pour les serveurs Cloud" (p. 1078).
7. Cliquez sur **Créer**.

Le serveur primaire devient accessible dans le réseau de production. Vous pouvez gérer le serveur à l'aide de sa console, de RDP, de SSH ou de TeamViewer.

© Acronis International GmbH, 2003-2026



Opérations avec des serveurs primaires

Dans la console Cyber Protect, les serveurs primaires sont affichés dans l'onglet **Disaster Recovery** > **Serveurs** > **Serveurs primaires**.

Mettre sous tension

Pour mettre un serveur primaire sous tension

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Cliquez sur **Mettre sous tension**.

Mise hors tension

Pour mettre un serveur primaire hors tension

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Cliquez sur **Mise hors tension**.
3. Dans l'écran **Mettez le serveur hors tension**, cliquez sur **Arrêter**.

Arrêt forcé

Pour forcer l'arrêt d'un serveur primaire

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Cliquez sur **Mise hors tension**.
3. Dans l'écran **Mettez le serveur hors tension**, sélectionnez **Forcer l'arrêt du serveur**, puis cliquez sur **Arrêter**.

Arrêter

Pour arrêter un serveur primaire

© Acronis International GmbH, 2003-2026

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Cliquez sur **Arrêter**.

Modifier les paramètres

Pour modifier les paramètres d'un serveur primaire

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Cliquez sur **Arrêter**.
3. Cliquez sur **Modifier**, puis modifiez les paramètres.

Appliquez un plan de protection

Pour appliquer un plan à un serveur primaire

1. Dans l'onglet **Serveurs primaires**, cliquez sur le serveur primaire.
2. Dans l'onglet **Plan**, cliquez sur **Créer**.
   Vous verrez un plan de protection prédéfini dans lequel vous ne pouvez modifier que la planification et les règles de rétention. Pour plus d'informations, voir Sauvegarde des serveurs dans le cloud.

Affichage des détails sur les serveurs cloud

Pour afficher les détails des serveurs cloud, accédez à **Disaster Recovery** > **Serveurs**. Vous y verrez deux onglets : **Serveurs de restauration** et **Serveurs primaires**. Pour afficher toutes les colonnes facultatives, cliquez sur l'icône en forme d'engrenage.

Sélectionnez un serveur dans le Cloud pour afficher les informations suivantes le concernant.

Nom de la colonne	Description
Nom	Un nom de serveur Cloud que vous avez défini
Statut	Le statut reflétant le problème le plus grave au sein d'un serveur Cloud (basé sur les alertes actives)
État	L'état d'un serveur Cloud
État de la MV	L'état de l'alimentation d'une machine virtuelle associée au serveur Cloud
Emplacement actif	L'emplacement où le serveur dans le Cloud est hébergé. Par exemple, **Cloud**.
Seuil des objectifs de point de restauration	L'intervalle de temps maximum autorisé entre le dernier point de restauration pour un basculement et l'heure actuelle. La valeur peut être définie entre 15 et 60 minutes, 1 et 24 heures, 1 et 14 jours.
Conformité des objectifs de point de restauration	La conformité des objectifs de point de restauration (RPO) est le rapport entre les RPO réels et le seuil des RPO. La conformité des RPO s'affiche lorsque le seuil des RPO est défini. Elle est calculée comme suit :

© Acronis International GmbH, 2003-2026

	Conformité RPO = RPO réels/Seuil des RPO où **RPO réels = heure actuelle – heure du dernier point de restauration** **États de conformité des RPO** Selon la valeur du rapport entre les RPO réels et le seuil des RPO, les statuts suivants sont utilisés : • **Conformité**. La conformité des RPO < 1x. Un serveur définit le seuil des RPO. • **Dépassé**. La conformité des RPO <= 2x. Un serveur enfreint le seuil des RPO. • **Dépassement grave**. La conformité des RPO <= 4x. Un serveur enfreint le seuil de RPO plus de deux fois. • **Dépassement critique**. La conformité des RPO > 4x. Un serveur enfreint le seuil des RPO plus de quatre fois. • **En attente (aucune sauvegarde)**. Le serveur est protégé par le plan de protection, mais la sauvegarde est en cours de création et n'est pas encore terminée.
Objectifs de point de restauration (RPO) réels	Le temps passé depuis la création du dernier point de restauration
Dernier point de restauration	Date et heure auxquelles le dernier point de restauration a été créé

Sauvegarde de serveurs cloud

Les serveurs primaires et de restauration sont sauvegardés sans agent sur le site dans le cloud. Ces sauvegardes ont les restrictions suivantes.

- Le seul emplacement de sauvegarde possible est le stockage dans le cloud. Les serveurs primaires sont sauvegardés dans le **stockage de sauvegarde des serveurs primaires**.

  Remarque
  Les emplacements de sauvegarde Microsoft Azure ne sont pas pris en charge.

- Il n'est pas possible d'appliquer un plan de sauvegarde à plusieurs serveurs. Chaque serveur doit disposer de son propre plan de sauvegarde, même si tous les plans de sauvegarde ont les mêmes paramètres.
- Un seul plan de sauvegarde peut être appliqué à un serveur.
- La sauvegarde reconnaissant les applications n'est pas prise en charge.
- Le chiffrement n'est pas disponible.
- Aucune option de sauvegarde n'est disponible.

Lorsque vous supprimez un serveur primaire, ses sauvegardes sont également supprimées.

© Acronis International GmbH, 2003-2026

Un serveur de restauration est sauvegardé uniquement lorsqu'il se trouve en état de basculement. Sa sauvegarde poursuit la séquence de sauvegarde du serveur d'origine. Lorsqu'une restauration automatique est effectuée, le serveur d'origine peut poursuivre sa séquence de sauvegarde. Par conséquent, les sauvegardes du serveur de restauration peuvent uniquement être supprimées manuellement ou via l'application des règles de rétention. Lorsqu'un serveur de restauration est supprimé, ses sauvegardes sont toujours conservées.

Remarque
Les plans de sauvegarde pour les serveurs cloud s'exécutent en fonction de l'heure UTC.

Règles de pare-feu pour les serveurs Cloud

Vous pouvez configurer les règles de pare-feu pour contrôler le trafic entrant et sortant des serveurs primaire et de restauration sur votre site dans le Cloud.

Vous pouvez configurer des règles entrantes après avoir provisionné une adresse IP publique pour le serveur Cloud. Le port TCP 443 est autorisé par défaut, et toutes les autres connexions entrantes sont refusées. Vous pouvez modifier les règles de pare-feu par défaut, et ajouter ou supprimer des exceptions entrantes. Si une adresse IP n'est pas provisionnée, vous pouvez uniquement consulter les règles entrantes, mais pas les configurer.

Vous pouvez configurer des règles sortantes après avoir provisionné une connexion Internet pour le serveur Cloud. Le port TCP 25 est refusé par défaut, et toutes les autres connexions sortantes sont refusées. Vous pouvez modifier les règles de pare-feu par défaut, et ajouter ou supprimer des exceptions sortantes. Si une connexion Internet n'est pas provisionnée, vous pouvez uniquement consulter les règles sortantes, mais pas les configurer.

Remarque
Pour des raisons de sécurité, certaines règles de pare-feu prédéfinies ne sont pas modifiables.

Pour les connexions entrantes et sortantes :

- Ping de permis : Demande d'écho ICMP (type 8, code 0) et réponse par écho ICMP (type 0, code 0)
- ICMP de permis besoin de fragmenter (type 3, code 4)
- TTL de permis dépassé (type 11, code 0)

Pour les connexions entrantes uniquement :

- Partie non configurable : Tout refuser

Pour les connexions sortantes uniquement :

- Partie non configurable : Tout rejeter

Définition de règles de pare-feu pour les serveurs Cloud

Vous pouvez modifier les règles de pare-feu par défaut pour les serveurs primaire et de restauration dans le Cloud.

© Acronis International GmbH, 2003-2026

Pour modifier les règles de pare-feu d'un serveur sur votre site dans le Cloud

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Si vous souhaitez modifier les règles de pare-feu d'un serveur de restauration, cliquez sur **Serveurs de restauration**. Si vous souhaitez également modifier les règles de pare-feu d'un serveur primaire, cliquez sur l'onglet **Serveurs primaires**.
3. Cliquez sur le serveur, puis sur **Modifier**.
4. Cliquez sur l'onglet **Règles de pare-feu du Cloud**.
5. Si vous souhaitez modifier l'action par défaut pour les connexions entrantes :
   a. Dans le champ à liste déroulante **Entrantes**, sélectionnez l'action par défaut.

Action	Description
Tout refuser	Refuse tout le trafic entrant. Vous pouvez ajouter des exceptions et autoriser le trafic depuis des adresses IP, protocoles et ports spécifiques.
Tout autoriser	Autorise l'ensemble du trafic TCP et UDP entrant. Vous pouvez ajouter des exceptions et refuser le trafic depuis des adresses IP, protocoles et ports spécifiques.

Remarque
La modification de l'action par défaut invalide et supprime la configuration des règles entrantes existantes.

   b. [Facultatif] Si vous souhaitez sauvegarder les exceptions existantes, sélectionnez **Sauvegarder les exceptions remplies** dans la fenêtre de confirmation.
   c. Cliquez sur **Confirmer**.
6. Si vous souhaitez ajouter une exception :
   a. Cliquez sur **Ajouter une exception**.
   b. Spécifiez les paramètres de pare-feu.

Paramètre de pare-feu	Description
Protocole	Sélectionnez le protocole de connexion. Les options suivantes sont prises en charge : • **TCP** • **UDP** • **TCP+UDP**
Port de serveur	Sélectionnez les ports auxquels la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • un numéro de port spécifique (par exemple, `2298`) • une plage de numéros de port (par exemple, `6000 à 6700`)

© Acronis International GmbH, 2003-2026

Paramètre de pare-feu	Description
	• n'importe quel numéro de port. Utilisez * si vous souhaitez que la règle s'applique à n'importe quel numéro de port.
Adresse IP du client	Sélectionnez les adresses IP auxquelles la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • une adresse IP spécifique (par exemple, `192.168.0.0`) • une plage d'adresses IP qui utilisent la notation CIDR notation (par exemple, `192.168.0.0/24`) • n'importe quelle adresse IP. Utilisez * si vous souhaitez que la règle s'applique à n'importe quelle adresse IP.

7. Si vous souhaitez supprimer une exception entrante existante, cliquez sur l'icône de corbeille à côté de l'exception.
8. Si vous souhaitez modifier l'action par défaut pour les connexions sortantes :
   a. Dans le champ à liste déroulante **Sortantes**, sélectionnez l'action par défaut.

Action	Description
Tout refuser	Refuse tout le trafic sortant. Vous pouvez ajouter des exceptions et autoriser le trafic vers des adresses IP, protocoles et ports spécifiques.
Tout autoriser	Autorise tout le trafic sortant. Vous pouvez ajouter des exceptions et refuser le trafic depuis des adresses IP, protocoles et ports spécifiques.

Remarque
La modification de l'action par défaut invalide et supprime la configuration des règles sortantes existantes.

   b. [Facultatif] Si vous souhaitez sauvegarder les exceptions existantes, sélectionnez **Sauvegarder les exceptions remplies** dans la fenêtre de confirmation.
   c. Cliquez sur **Confirmer**.
9. Si vous souhaitez ajouter une exception :
   a. Cliquez sur **Ajouter une exception**.
   b. Spécifiez les paramètres de pare-feu.

Paramètre de pare-feu	Description
Protocole	Sélectionnez le protocole de connexion. Les options suivantes sont prises en charge : • **TCP**

© Acronis International GmbH, 2003-2026

Paramètre de pare-feu	Description
	• **UDP** • **TCP+UDP**
Port de serveur	Sélectionnez les ports auxquels la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • un numéro de port spécifique (par exemple, `2298`) • une plage de numéros de port (par exemple, `6000 à 6700`) • n'importe quel numéro de port. Utilisez `*` si vous souhaitez que la règle s'applique à n'importe quel numéro de port.
Adresse IP du client	Sélectionnez les adresses IP auxquelles la règle s'applique. Vous pouvez spécifier les valeurs suivantes : • une adresse IP spécifique (par exemple, `192.168.0.0`) • une plage d'adresses IP qui utilisent la notation CIDR notation (par exemple, `192.168.0.0/24`) • n'importe quelle adresse IP. Utilisez `*` si vous souhaitez que la règle s'applique à n'importe quelle adresse IP.

10. Si vous souhaitez supprimer une exception sortante existante, cliquez sur l'icône de corbeille à côté de l'exception.
11. Cliquez sur **Enregistrer**.

Vérification des activités de pare-feu dans le Cloud

Après la mise à jour de la configuration des règles du pare-feu d'un serveur cloud, un journal de l'activité de mise à jour devient disponible dans la console Cyber Protect. Vous pouvez le consulter et vérifier les informations suivantes :

- le nom d'utilisateur de la personne ayant mis la configuration à jour
- la date et l'heure de la mise à jour
- les paramètres de pare-feu des connexions entrantes et sortantes
- les actions par défaut des connexions entrantes et sortantes
- les protocoles, ports et adresses IP des exceptions pour les connexions entrantes et sortantes

Pour consulter les détails d'un changement de configuration des règles d'un pare-feu dans le Cloud

1. Dans la console Cyber Protect, cliquez sur **Surveillance** > **Activités**.
2. Cliquez sur l'activité correspondante, puis sur **Toutes les propriétés**.
   La description d'une activité doit être **Mise à jour de la configuration du serveur dans le Cloud**.
3. Dans le champ **Contexte**, examinez les informations qui vous intéressent.

© Acronis International GmbH, 2003-2026

Points de calcul

Dans Disaster Recovery vers Cyber Protect Cloud, des points de calcul sont utilisés pour les serveurs primaires et les serveurs de restauration pendant le basculement en environnement de test et en environnement de production. Les points de calcul reflètent les ressources de calcul utilisées pour l'exécution des serveurs (machines virtuelles) dans le cloud.

La consommation des points de calcul pendant la reprise d'activité après sinistre dépend des paramètres du serveur et de la durée pendant laquelle le serveur se trouve dans l'état de basculement. Plus le serveur est puissant et plus cette période est longue, plus le nombre de points de calcul consommés est élevé. Et plus le nombre de points de calcul consommés est élevé, plus le prix que vous payez est important.

Tous les serveurs qui fonctionnent dans Cyber Protect Cloud seront facturés en points de calcul, en fonction de leur configuration (« flavor ») et indépendamment de leur état (sous tension ou hors tension).

Les serveurs de restauration qui sont en état de veille ne consomment pas de points de calcul et ne seront pas facturés en points de calcul.

Dans le tableau ci-dessous, vous pouvez voir un exemple de huit serveurs dans le cloud avec différentes configurations, et les points de calcul correspondants qu'ils consommeront par heure. Vous pouvez modifier les configurations des serveurs dans l'onglet **Détails**.

Type	CPU	RAM	Points de calcul
F1	1 vCPU	2 Go	1
F2	1 vCPU	4 Go	2
F3	2 vCPU	8 Go	4
F4	4 vCPU	16 Go	8
F5	8 vCPU	32 Go	16
F6	16 vCPU	64 Go	32
F7	16 vCPU	128 Go	64
F8	16 vCPU	256 Go	128

Grâce aux informations du tableau, vous pouvez estimer facilement le nombre de points de calcul consommés par un serveur (machine virtuelle).

Par exemple, si vous souhaitez protéger avec Disaster Recovery une machine virtuelle comportant 4 vCPU* de 16 Go de mémoire RAM et une machine virtuelle comportant 2 vCPU avec 8 Go de mémoire RAM, la première machine virtuelle consomme 8 points de calcul par heure et la seconde machine virtuelle, 4 points de calcul par heure. Si les deux machines virtuelles se trouvent dans une situation de basculement, la consommation totale est de 12 points de calcul par heure, soit

© Acronis International GmbH, 2003-2026

288 points de calcul pour la journée complète (12 points de calcul x 24 heures = 288 points de calcul).

* vCPU fait référence à un processeur (CPU) physique affecté à une machine virtuelle et dépendant de l'heure.

Remarque
Si le quota de **Points de calcul** est dépassé, tous les serveurs primaires et de restauration seront arrêtés. Il ne sera plus possible d'utiliser ces serveurs jusqu'au début de la période de facturation suivante ou jusqu'à ce que vous augmentiez le quota. La période de facturation par défaut est un mois complet.

Basculement test

Un basculement test consiste à démarrer un serveur de restauration dans un VLAN de test isolé de votre réseau de production. Vous pouvez tester plusieurs serveurs de restauration à la fois et vérifier leur interaction. Dans le réseau de test, les serveurs communiquent à l'aide de leur adresse IP de production, mais ils ne peuvent pas démarrer de connexions TCP ou UDP à des ressources situées sur votre réseau local.

Lors du basculement test, la machine virtuelle (serveur de restauration) n'est pas finalisée. L'agent lit le contenu des disques virtuels directement depuis la sauvegarde et accède de façon aléatoire aux différentes parties de la sauvegarde. Le risque est que les performances du serveur de restauration dans l'état de basculement test soient plus lentes que d'habitude.

Réalisation d'un basculement test

Bien que le basculement test soit facultatif, nous vous recommandons d'en exécuter régulièrement, à une fréquence adéquate pour vous en matière de coût et de fiabilité. Une bonne pratique consiste à créer un runbook (dossier d'exploitation), c'est-à-dire un ensemble d'instructions décrivant comment lancer l'environnement de production dans le Cloud.

Important
Vous devez créer un serveur de restauration à l'avance afin de protéger vos terminaux d'un sinistre.

Vous ne pouvez effectuer un basculement que depuis des points de restauration créés après la création du serveur de restauration du terminal.

Vous devez créer au moins un point de restauration avant de basculer vers un serveur de restauration. Le nombre maximal de points de restauration pris en charge est de 100.

Pour effectuer un basculement test

1. Sélectionnez la machine d'origine ou le serveur de restauration que vous souhaitez tester.
2. Cliquez sur **Disaster Recovery**.
   La description du serveur de restauration s'ouvre.
3. Cliquez sur **Basculement**.

© Acronis International GmbH, 2003-2026

4. Sélectionnez le type de basculement **Basculement test**.
5. Sélectionnez le point de restauration (sauvegarde), puis cliquez sur **Démarrer**.
6. Si la sauvegarde sélectionnée est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur :
   a. Saisissez le mot de passe de chiffrement pour l'ensemble de sauvegardes.

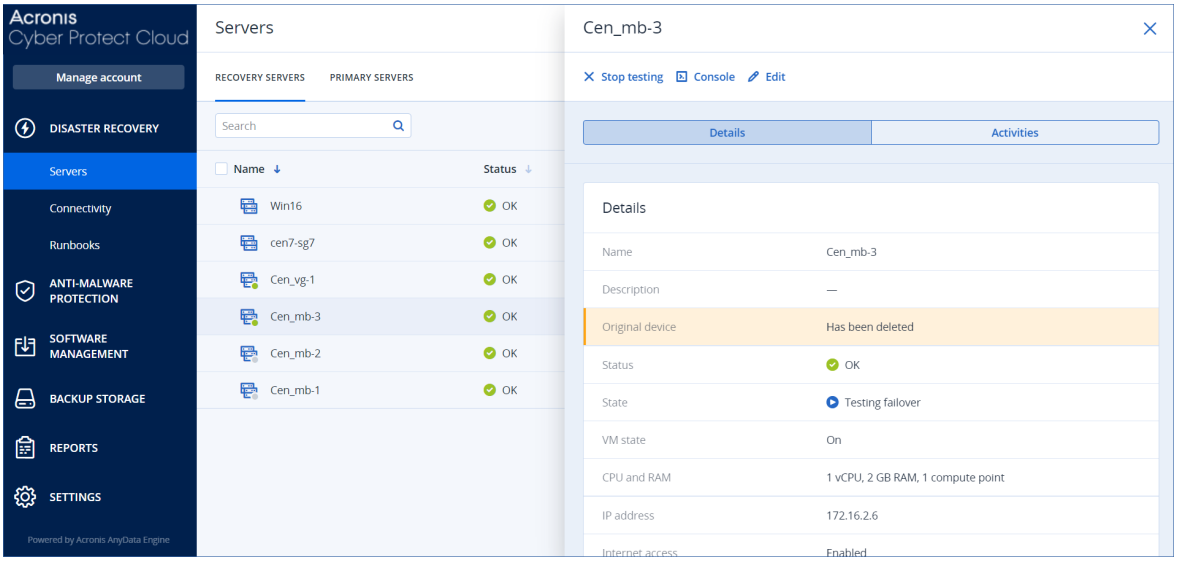
      Remarque
      Le mot de passe ne sera enregistré que temporairement et utilisé uniquement pour le basculement test en cours. Le mot de passe est supprimé automatiquement du magasin des identifiants si le basculement test est arrêté ou une fois que le basculement test est terminé.

   b. [Facultatif] Pour enregistrer le mot de passe de l'ensemble de sauvegardes et l'utiliser dans les opérations de basculement ultérieures, cochez la case **Stocker le mot de passe dans un magasin d'identifiants sécurisé** et saisissez un nom pour les identifiants dans le champ **Nom des identifiants**.

      Important
      Le mot de passe sera stocké dans un magasin d'identifiants sécurisé et sera appliqué automatiquement dans les opérations de basculement ultérieures. Toutefois, l'enregistrement des mots de passe peut entrer en conflit avec vos obligations de conformité.

   c. Cliquez sur **Terminé**.

   Quand le serveur de restauration démarre, son état est modifié en **Test de basculement**.



7. Testez le serveur de restauration à l'aide de l'une des méthodes suivantes :
   - Dans **Disaster Recovery** > **Serveurs**, sélectionnez le serveur de restauration, puis cliquez sur **Console**.
   - Connectez-vous au serveur de restauration via RDP ou SSH, à l'aide de l'IP de production que vous avez indiquée lors de la création du serveur de restauration. Testez la connexion de

© Acronis International GmbH, 2003-2026

l'intérieur et de l'extérieur du réseau de production (comme décrit dans « Connexion de point à site »).

- Exécutez un script au sein du serveur de restauration.

  Le script peut vérifier l'écran de connexion, le démarrage des applications, la connexion Internet, et la capacité d'autres machines à se connecter au serveur de restauration.
- Si le serveur de restauration a accès à Internet et à une adresse IP publique, vous voudrez peut-être utiliser TeamViewer.

8. Une fois le test terminé, cliquez sur **Arrêter le test**.

   Le serveur de restauration est arrêté. Toutes les modifications apportées au serveur de restauration lors du basculement test ne sont pas conservées.

Basculement test automatisé

Avec le basculement test automatisé, le serveur de restauration est testé automatiquement une fois par mois, sans aucune interaction manuelle.

Le processus de basculement test automatisé se compose des étapes suivantes :

1. Création d'une machine virtuelle à partir du dernier point de restauration
2. Prise d'instantané de la machine virtuelle
3. Analyse visant à déterminer si le système d'exploitation de la machine virtuelle démarre correctement
4. Envoi d'une notification pour vous informer de statut du basculement test

Remarque
Le basculement test automatisé consomme des points de calcul.

Vous pouvez configurer le basculement test automatisé dans les paramètres du serveur de restauration. Pour plus d'informations, voir "Configuration du basculement test automatisé" (p. 1086).

Veuillez noter que, dans de très rares cas, le basculement test automatisé peut être ignoré et ne pas être exécuté à l'heure planifiée. Cela s'explique par le fait que le basculement de la production est prioritaire sur le basculement test automatisé. Par conséquent, les ressources matérielles (processeur et mémoire RAM) allouées au basculement test automatisé peuvent être temporairement limitées afin de garantir que les ressources nécessaires à un basculement de production simultané soient suffisantes.

Si le basculement test automatisé est ignoré, quelle qu'en soit la raison, une alerte est générée.

Remarque
Le basculement test automatisé échoue si les sauvegardes de l'ordinateur original sont chiffrées à l'aide du chiffrement comme propriété de l'ordinateur, et que le mot de passe de chiffrement n'est pas spécifié lors de la création du serveur de restauration. Pour plus d'informations sur la spécification du mot de passe de chiffrement, voir "Création d'un serveur de restauration" (p. 1067).

© Acronis International GmbH, 2003-2026

Configuration du basculement test automatisé

En configurant le basculement test automatisé, vous pouvez tester votre serveur de restauration tous les mois, sans aucune intervention manuelle.

Pour configurer le basculement test automatisé

1. Dans la console, accédez à **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Cliquez sur **Modifier**.
3. Dans la section **Basculement test automatisé**, champ **Planification**, sélectionnez **Tous les mois**.
4. [Facultatif] Dans la zone **Délai d'attente de capture d'écran**, changez la valeur par défaut de la durée maximale (en minutes) pendant laquelle le système essaie d'effectuer un basculement test automatisé.
5. [Facultatif] Si vous souhaitez conserver la valeur **Délai d'attente de capture d'écran** par défaut et souhaitez qu'elle soit renseignée automatiquement lorsque vous activez le basculement test automatisé des autres serveurs de restauration, sélectionnez **Définir comme délai d'attente par défaut**.
6. Cliquez sur **Enregistrer**.

Affichage du statut du basculement test automatisé

Vous pouvez afficher les détails d'un basculement test automatisé effectué, notamment son statut, ses heures de début et de fin, sa durée et l'instantané de la machine virtuelle.

Remarque
L'instantané de la machine virtuelle est conservée jusqu'à ce que le basculement test automatisé soit réexécuté et génère un nouvel instantané.

Pour afficher le statut du basculement test automatisé d'un serveur de restauration

1. Dans la console, accédez à **Reprise d'activité après sinistre** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Dans la section **Basculement test automatisé**, vérifiez les détails du dernier basculement test automatisé.
3. [Facultatif] Pour afficher l'instantané de la machine virtuelle, cliquez sur **Afficher l'instantané**.

Désactivation du basculement test automatisé

Vous pouvez désactiver le basculement test automatisé si vous souhaitez économiser les ressources n'avez pas besoin d'exécuter le basculement test automatisé pour un serveur de restauration donné.

Pour désactiver le basculement test automatisé

© Acronis International GmbH, 2003-2026

1. Dans la console, accédez à **Disaster Recovery** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Cliquez sur **Modifier**.
3. Dans l'assistant, cliquez sur l'onglet **Basculement test automatisé**.
4. Désactivez l'interrupteur **Basculement test automatisé**.
5. Cliquez sur **Enregistrer**.

Basculement de la production

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsqu'un serveur de restauration est créé, il reste en mode **En attente**. La machine virtuelle correspondante n'existe pas avant que vous ayez démarré un basculement. Avant de démarrer un processus de basculement, vous devez créer au moins une sauvegarde d'image de disque (avec volume amorçable) de la machine d'origine.

Lors du démarrage du processus de basculement, vous sélectionnez le point de restauration (sauvegarde) de l'ordinateur d'origine depuis lequel une machine virtuelle avec les paramètres prédéfinis sera créée. L'opération de basculement utilise la fonctionnalité « exécution d'une machine virtuelle à partir d'une sauvegarde ». Le serveur de restauration reçoit l'état de transition **Finalisation**. Ce processus implique le transfert des disques virtuels du serveur depuis le stockage des sauvegardes (stockage « froid ») vers le stockage pour reprise d'activité après sinistre (stockage « chaud »).

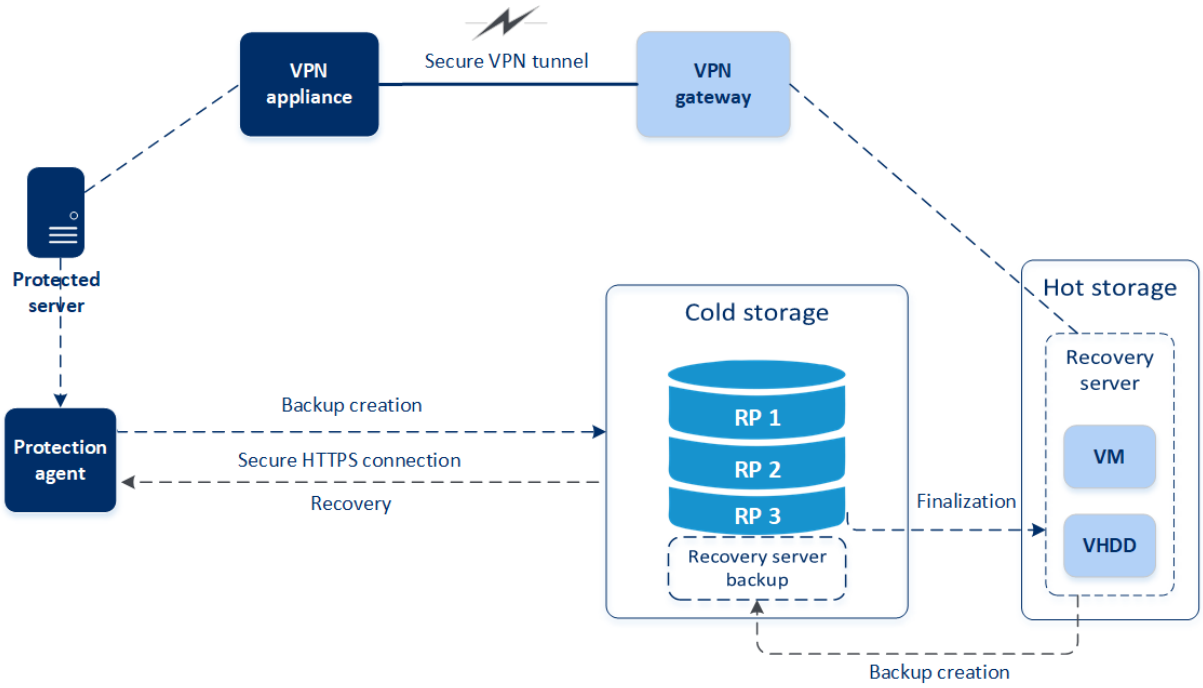
Remarque
Lors de la **finalisation**, le serveur est accessible et opérationnel bien que ses performances soient inférieures à la normale. Vous pouvez ouvrir la console du serveur en cliquant sur le lien **La console est prête**. Le lien est disponible dans la colonne **État de la MV** de l'écran **Disaster Recovery** > **Serveurs** et dans la vue **Détails** du serveur.

Une fois la **Finalisation** terminée, les performances du serveur sont rétablies. L'état du serveur est modifié en **Basculement**. La ressource est désormais basculée de l'ordinateur d'origine vers le serveur de restauration du site dans le Cloud.

Si le composant de restauration possède un agent de protection, le service de l'agent est interrompu pour éviter toute interférence (notamment le démarrage d'une sauvegarde ou le signalement de statuts obsolètes au composant de sauvegarde).

Dans le diagramme ci-dessous, vous pouvez voir les processus de basculement et de restauration automatique.

© Acronis International GmbH, 2003-2026



Réalisation d'un basculement

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Un basculement est le processus consistant à déplacer une ressource de vos locaux vers le Cloud. Il s'agit aussi de l'état où la ressource reste dans le Cloud.

Lorsque vous démarrez un basculement, le serveur de restauration démarre dans le réseau de production. Pour éviter tout problème et interférence, assurez-vous que la ressource originale n'est pas en ligne et qu'il est impossible d'y accéder via VPN.

Pour éviter toute interférence de sauvegarde dans la même archive dans le cloud, révoquez manuellement le plan de protection de la ressource ayant l'état **Basculement**. Pour plus d'informations sur la révocation de plans, reportez-vous à Révocation d'un plan de protection.

Important
Vous devez créer un serveur de restauration à l'avance afin de protéger vos terminaux d'un sinistre.

Vous ne pouvez effectuer un basculement que depuis des points de restauration créés après la création du serveur de restauration du terminal.

Vous devez créer au moins un point de restauration avant de basculer vers un serveur de restauration. Le nombre maximal de points de restauration pris en charge est de 100.

Vous pouvez suivre la procédure ci-dessous ou regarder le tutoriel vidéo.

Pour réaliser un basculement

© Acronis International GmbH, 2003-2026

1. Vérifiez que la machine d'origine n'est pas disponible sur le réseau.
2. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
3. Cliquez sur **Basculement**.
4. Sélectionnez **Basculement en production**.
5. Sélectionnez le point de restauration (sauvegarde), puis cliquez sur **Démarrer**.
6. [Si la sauvegarde sélectionnée est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur]
   a. Saisissez le mot de passe de chiffrement pour l'ensemble de sauvegardes.

      Remarque
      Le mot de passe ne sera enregistré que temporairement et utilisé uniquement pour le basculement en cours. Le mot de passe est supprimé automatiquement du magasin des identifiants une fois que l'opération de basculement est terminée et que le serveur revient à l'état de **veille**.

   b. [Facultatif] Pour enregistrer le mot de passe de l'ensemble de sauvegardes et l'utiliser dans les opérations de basculement ultérieures, cochez la case **Stocker le mot de passe dans un magasin d'identifiants sécurisé** et saisissez un nom pour les identifiants dans le champ **Nom des identifiants**.

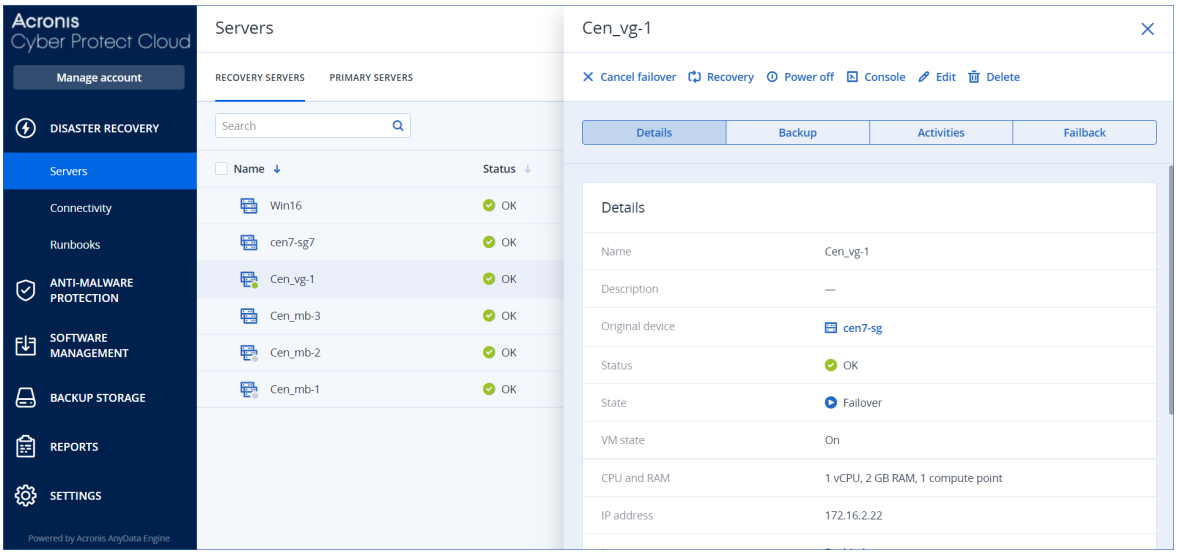
      Important
      Le mot de passe sera stocké dans un magasin d'identifiants sécurisé et sera appliqué automatiquement dans les opérations de basculement ultérieures. Toutefois, l'enregistrement des mots de passe peut entrer en conflit avec vos obligations de conformité.

   c. Cliquez sur **Terminé**.

   Lorsque le serveur de restauration démarre, son état est modifié en **Finalisation**, puis, au bout d'un certain temps, en **Basculement.**

Important
Il est essentiel de comprendre que le serveur est disponible aussi bien dans l'état **Finalisation** que **Basculement**. Lors de la **finalisation**, vous pouvez accéder à la console du serveur en cliquant sur le lien **La console est prête**. Le lien est disponible dans la colonne **État de la MV** de l'écran **Disaster Recovery** > **Serveurs** et dans la vue **Détails** du serveur.

© Acronis International GmbH, 2003-2026



7. Assurez-vous que le serveur de restauration est démarré en consultant sa console. Cliquez sur **Disaster Recovery** > **Serveurs**, sélectionnez le serveur de restauration, puis cliquez sur **Console**.
8. Assurez-vous que le serveur de restauration est accessible à l'aide de l'adresse IP de production que vous avez indiquée lors de la création du serveur de restauration.

Une fois le serveur de restauration finalisé, un nouveau plan de protection est automatiquement créé et lui est appliqué. Ce plan de protection se base sur le plan de protection utilisé pour créer le serveur de restauration, avec certaines limitations. Dans ce plan, vous ne pouvez modifier que la planification et les règles de rétention. Pour en savoir plus, consultez « Sauvegarde des serveurs Cloud ».

Comment exécuter un basculement des serveurs à l'aide d'un DNS local

Si votre site local utilise des serveurs DNS pour résoudre les noms d'ordinateur, la communication entre les serveurs de restauration risque d'échouer après un basculement. Cela s'explique par le fait que les serveurs DNS dans le cloud sont différents de ceux du site local. Par défaut, les nouveaux serveurs cloud utilisent les serveurs DNS du site cloud, mais vous pouvez configurer des paramètres DNS personnalisés. Pour plus d'informations, voir "Configuration de serveurs DNS personnalisés" (p. 1062).

Comment exécuter un basculement à l'aide d'un serveur DHCP

Il se peut que le serveur DHCP de votre infrastructure locale se situe sur un hôte Windows ou Linux. Lorsqu'un tel hôte est basculé vers le site dans le Cloud, un problème de duplication du serveur DHCP survient, car la passerelle VPN dans le Cloud joue également le rôle de DHCP. Pour résoudre ce problème, effectuez l'une des actions suivantes :

- Si seul l'hôte DHCP a été basculé vers le Cloud, mais que les autres serveurs locaux se trouvent toujours dans le site local, vous devez alors vous connecter à l'hôte DHCP et désactiver le serveur DHCP qui s'y trouve. Il n'y aura ainsi aucun conflit et seule la passerelle VPN fera office de serveur DHCP.

© Acronis International GmbH, 2003-2026

- Si vos serveurs dans le Cloud ont déjà obtenu leurs adresses auprès de l'hôte DHCP, vous devez alors vous connecter à l'hôte DHCP et désactiver le serveur DHCP qui s'y trouve. Vous devez également vous connecter aux serveurs Cloud et renouveler le bail DHCP pour attribuer de nouvelles adresses IP allouées par le bon serveur DHCP (hébergé sur la passerelle VPN).

Remarque
Les instructions ne sont pas valides lorsque votre serveur DHCP dans le cloud est configuré avec l'option **DHCP personnalisé**, et que certains des serveurs principaux ou de restauration obtiennent leur adresse IP depuis ce serveur DHCP.

Arrêt d'un basculement

Vous pouvez arrêter un basculement en production à tout moment, pendant chaque phase du processus.

Remarque
L'arrêt d'un basculement annule toutes les modifications qui ont été effectuées à partir du moment où le basculement a été démarré, sauf les sauvegardes du serveur de restauration.

Pour arrêter un basculement en production

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs** > **Serveurs de restauration**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur le serveur de restauration.
4. Cliquez sur **Arrêter le basculement**.
5. Dans la fenêtre de confirmation qui s'affiche, cochez la case, puis cliquez sur **Arrêter le basculement**.
   Le basculement est arrêté. Le serveur de restauration revient à l'état **Veille**.

Restauration automatique

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Une restauration automatique est un processus consistant à déplacer la ressource du Cloud vers une machine physique ou virtuelle sur votre site local. Vous pouvez exécuter une restauration automatique sur un serveur de restauration dont l'état est **Basculement**, et continuer d'utiliser le serveur sur votre site local.

Vous pouvez exécuter un basculement automatique vers une machine cible virtuelle ou physique sur votre site local. Lors du processus de restauration automatique, vous pouvez transférer les données de sauvegarde vers votre site local alors que la machine virtuelle dans le cloud continue à s'exécuter. Cette technologie vous permet de bénéficier d'une période d'interruption d'activité très

© Acronis International GmbH, 2003-2026

courte, qui est estimée et affichée dans la console Cyber Protect. Vous pouvez consulter cette information et l'utiliser pour planifier vos activités et, si nécessaire, avertir vos clients d'une période d'interruption d'activité à venir. Si vous effectuez une restauration automatique avec agent par l'intermédiaire d'un support amorçable, la période d'interruption d'activité est encore plus courte, car le transfert vers le site local ne porte que sur les données modifiées.

Pour effectuer une restauration automatique sur une machine physique cible, vous pouvez utiliser la restauration automatique avec agent via un support de démarrage. Pour plus d'informations, voir "Exécution d'une restauration automatique avec agent via un support de démarrage" (p. 1094).

Pour effectuer une restauration automatique sur une machine virtuelle cible, vous pouvez utiliser la restauration automatique avec agent via un support de démarrage ou la restauration automatique sans agent via l'agent d'hyperviseur. Pour plus d'informations, voir "Exécution d'une restauration automatique avec agent via un support de démarrage" (p. 1094) et "Exécution d'une restauration automatique sans agent via un agent d'hyperviseur" (p. 1098).

Dans des cas précis où vous ne pouvez pas utiliser la procédure de restauration automatique en mode automatisé, vous pouvez exécuter une restauration automatique en mode manuel. Pour plus d'informations, voir "Restauration automatique en mode manuel" (p. 1102).

Remarque
Les opérations de runbook prennent en charge la restauration automatique en mode manuel uniquement. Cela signifie que si vous démarrez le processus de restauration automatique en exécutant un runbook qui inclut une étape **Serveur de restauration automatique**, la procédure nécessitera une interaction manuelle : vous devez restaurer l'ordinateur manuellement, et confirmer ou annuler le processus de restauration automatique à partir de l'onglet **Disaster Recovery** > **Serveurs**.

Restauration automatique avec agent via un support de démarrage

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le processus de restauration automatique avec agent via un support de démarrage est optimisé pour effectuer une restauration automatique vers la machine physique ou virtuelle d'origine. Pendant ce processus, seules les données modifiées sont transférées vers le site local.

Le processus de restauration automatique avec agent via un support de démarrage vers une machine virtuelle ou physique cible comprend les phases suivantes :

1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.
2. **Transfert de données**. Lors de cette phase, l'exécution de la machine virtuelle dans le Cloud est maintenue pendant que les données sont transférées du site dans le Cloud vers le site local. Vous pouvez démarrer la phase suivante, le basculement, à tout moment durant la phase de

© Acronis International GmbH, 2003-2026

transfert de données, mais vous devriez tenir compte des relations suivantes.

Plus vous restez longtemps dans la phase Transfert de données,

- plus longtemps la machine virtuelle dans le cloud continue à s'exécuter ;
- plus la quantité de données qui sera transférée à votre site local sera importante ;
- plus cela vous coûtera cher (vous dépensez plus de points de calcul) ;
- plus la période d'interruption d'activité lors de la phase de basculement sera courte.

Si vous souhaitez réduire l'interruption d'activité au minimum, démarrez la phase de basculement une fois que 90 % au moins des données ont été transférés sur le site local.

Si vous pouvez vous permettre une période d'interruption d'activité plus longue et que vous ne souhaitez pas dépenser plus de points de calcul pour l'exécution de la machine virtuelle dans le Cloud, vous pouvez démarrer la phase de basculement plus tôt.

Remarque

Le processus de transfert de données utilise une technologie de flashback. Cette technologie compare les données disponibles sur la machine cible aux données de la machine virtuelle dans le cloud. Si une partie des données est déjà disponible sur la machine cible, elles ne sont pas retransférées. Cette technologie accélère la phase de transfert de données.

C'est la raison pour laquelle nous vous recommandons de restaurer le serveur sur la machine d'origine sur votre site local.

3. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données restantes, y compris le dernier incrément de sauvegarde, sont transférées sur le site local. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.
4. **Validation**. Lors de cette phase, l'ordinateur sur le site local est prêt et vous pouvez le redémarrer à l'aide d'un support de démarrage Linux. Vous pouvez vérifier que la machine virtuelle fonctionne correctement et :
   - Si tout fonctionne comme prévu, vous pouvez confirmer la restauration automatique. Après la confirmation de la restauration automatique, la machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**. Le processus de restauration automatique est alors terminé.
   - En cas d'anomalie, vous pouvez annuler le basculement et revenir à la phase de planification.

Remarque

Une fois que le support de démarrage a été redémarré, vous ne pourrez plus le réutiliser. Si vous détectez une anomalie au cours de la phase de validation, vous devez enregistrer un nouveau support de démarrage et redémarrer le processus de restauration automatique.

Toutefois, étant donné qu'une technologie de flashback est utilisée, les données figurant déjà sur le site local ne seront pas retransférées et le processus de restauration automatique sera accéléré.

© Acronis International GmbH, 2003-2026

Exécution d'une restauration automatique avec agent via un support de démarrage

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez exécuter une restauration automatique avec agent via un support de démarrage vers une machine cible physique ou virtuelle sur votre site local.

Remarque
Le processus de transfert de données utilise une technologie de flashback. Cette technologie compare les données disponibles sur la machine cible aux données de la machine virtuelle dans le cloud. Si une partie des données est déjà disponible sur la machine cible, elles ne sont pas retransférées. Cette technologie accélère la phase de transfert de données.

C'est la raison pour laquelle nous vous recommandons de restaurer le serveur sur la machine d'origine sur votre site local.

Prérequis

- L'agent que vous allez utiliser pour exécuter une restauration automatique est en ligne et n'est pas actuellement utilisé pour une autre opération de restauration automatique.
- Votre connexion Internet est stable.
- Un support de démarrage enregistré est disponible. Pour plus d'informations, voir Création d'un support de démarrage afin de restaurer des systèmes d'exploitation dans le Guide de l'utilisateur Cyber Protection.
- La machine physique cible est la machine d'origine sur votre site local ou une machine dont le firmware est identique à celui de la machine d'origine.
- Il existe au moins une sauvegarde complète de la machine virtuelle dans le cloud.

Pour effectuer une restauration automatique vers une machine physique

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans le champ **Type de restauration automatique**, sélectionnez **Avec agent via un support de démarrage**.
5. Dans le champ **Support de démarrage cible**, cliquez sur **Spécifier**, sélectionnez le support de démarrage, puis cliquez sur **Terminé**.

   Remarque
   Nous vous recommandons d'utiliser un support de démarrage prêt à l'emploi, car il est déjà configuré. Pour plus d'informations, voir Création d'un support de démarrage afin de restaurer des systèmes d'exploitation dans le Guide de l'utilisateur Cyber Protection.

© Acronis International GmbH, 2003-2026

6. [Facultatif] Pour modifier le mappage de disque par défaut, cliquez dans le champ **Mappage de disque** sur **Spécifier**, mappez les disques de la sauvegarde vers les disques de la machine cible, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer le transfert de données**, puis sur **Démarrer** dans la fenêtre de confirmation.

Remarque
S'il n'y a pas de sauvegarde de la machine virtuelle dans le cloud, le système effectuera une sauvegarde automatiquement avant la phase de transfert des données.

La phase transfert de données démarre. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre affiche la quantité de données déjà transférées vers le site local, ainsi que la quantité totale de données à transférer. La quantité totale de données comprend les données de la dernière sauvegarde avant le démarrage de la phase de transfert de données, ainsi que les sauvegardes des données nouvellement générées (incréments de sauvegarde), car la machine virtuelle continue à s'exécuter lors de la phase de transfert de données. C'est la raison pour laquelle les valeurs **Progression** augmentent au fil du temps. Étant donné que le système utilise une technologie de flashback pendant le transfert de données et ne transfère pas les données déjà disponibles sur la machine cible, la progression peut être plus rapide que dans le calcul initial effectué par la console.
Estimation de l'interruption d'activité	Ce paramètre indique la durée d'indisponibilité de la machine virtuelle dans le cloud si vous démarrez la phase de basculement maintenant. La valeur est calculée en fonction des valeurs du paramètre **Progression** et diminue au fil du temps. Étant donné que le système utilise une technologie de flashback pendant le transfert de données et ne transfère pas les données déjà disponibles sur la machine cible, l'interruption d'activité peut être plus courte que la valeur affichée initialement dans la console.

8. Cliquez sur **Basculement**, puis cliquez une nouvelle fois sur **Basculement** dans la fenêtre de confirmation.

La phase de basculement commence. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre montre la progression de la restauration de la machine sur le site local.
Temps restant estimé	Ce paramètre indique l'heure approximative à laquelle la phase de basculement sera terminée et où vous pourrez démarrer la machine virtuelle sur le site local.

© Acronis International GmbH, 2003-2026

Remarque
Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

9. Une fois la phase de **basculement** terminée, redémarrez le support de démarrage, puis vérifiez que la machine physique sur votre site local fonctionne comme prévu.
   Pour plus d'informations, voir Récupération de disques à l'aide d'un support de démarrage dans le Guide de l'utilisateur Cyber Protection.
10. Cliquez sur **Confirmer la restauration automatique**, puis sur **Confirmer** dans la fenêtre de confirmation pour finaliser le processus.
    La machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

Remarque
Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

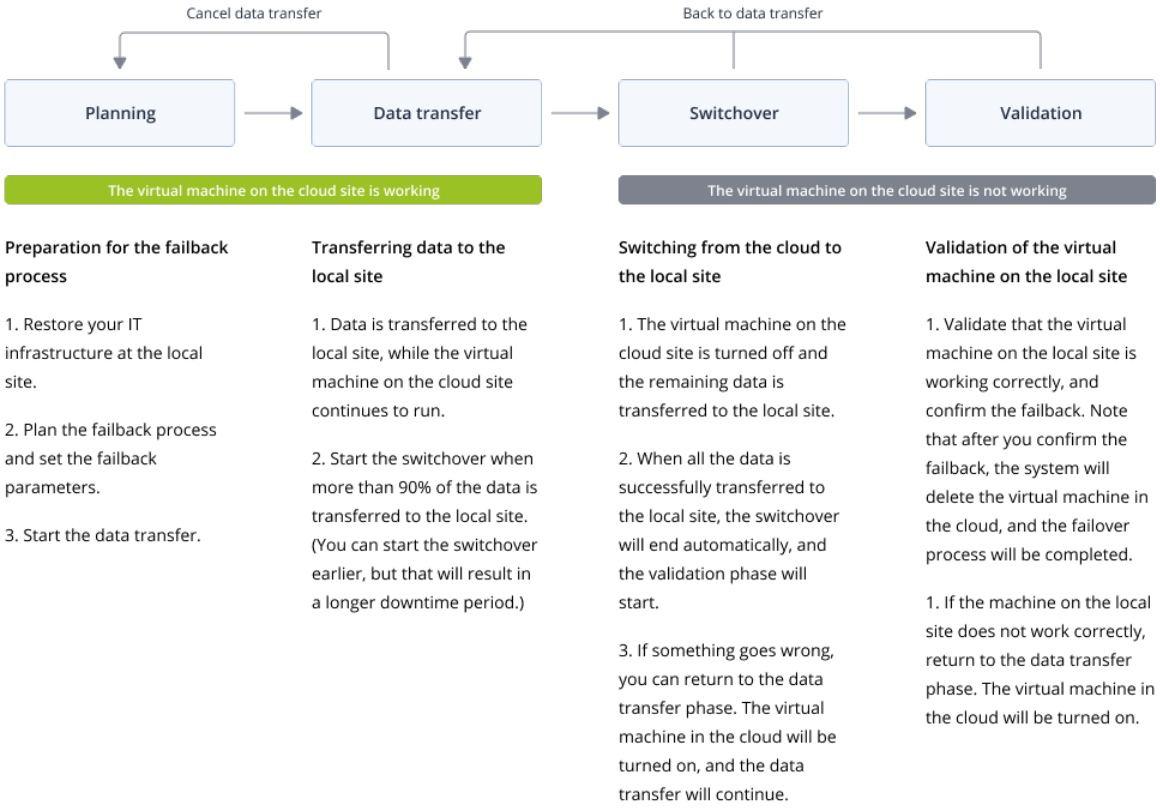
Restauration automatique sans agent via un agent d'hyperviseur

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La restauration automatique sans agent via un processus d'agent d'hyperviseur est optimisée pour la restauration automatique vers une nouvelle machine virtuelle. Si vous souhaitez effectuer une restauration automatique vers la machine virtuelle d'origine, suivez la procédure de restauration automatique avec agent via un support de démarrage.

La restauration automatique sans agent via un agent d'hyperviseur se déroule en quatre phases.

© Acronis International GmbH, 2003-2026



1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.

   Remarque
   Pour diminuer la durée totale du processus de restauration automatique, nous vous recommandons de démarrer la phase de transfert de données immédiatement après avoir configuré vos serveurs locaux, puis de poursuivre avec la configuration du réseau et le reste de l'infrastructure locale lors de la phase de transfert de données.

2. **Transfert de données**. Lors de cette phase, l'exécution de la machine virtuelle dans le Cloud est maintenue pendant que les données sont transférées du site dans le Cloud vers le site local. Vous pouvez démarrer la phase suivante, le basculement, à tout moment durant la phase de transfert de données, mais vous devriez tenir compte des relations suivantes.
   Plus vous restez longtemps dans la phase Transfert de données,
   - plus longtemps la machine virtuelle dans le cloud continue à s'exécuter ;
   - plus la quantité de données qui sera transférée à votre site local sera importante ;
   - plus cela vous coûtera cher (vous dépensez plus de points de calcul) ;
   - plus la période d'interruption d'activité lors de la phase de basculement sera courte.

© Acronis International GmbH, 2003-2026

Si vous souhaitez réduire l'interruption d'activité au minimum, démarrez la phase de basculement une fois que 90 % au moins des données ont été transférés sur le site local.

Si vous pouvez vous permettre une période d'interruption d'activité plus longue et que vous ne souhaitez pas dépenser plus de points de calcul pour l'exécution de la machine virtuelle dans le Cloud, vous pouvez démarrer la phase de basculement plus tôt.

Si vous annulez le processus de restauration automatique lors de la phase Transfert de données, les données transférées ne seront pas supprimées du site local. Pour éviter d'éventuels problèmes, supprimez manuellement les données transférées avant de lancer un nouveau processus de restauration automatique. Le processus de transfert de données suivant reprendra au début.

3. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données restantes, y compris le dernier incrément de sauvegarde, sont transférées sur le site local. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

   Vous pouvez consulter le temps estimé pour finir cette phase (période d'interruption d'activité) dans la console Cyber Protect. Lorsque toutes les données sont transférées sur le site local (il n'y a aucune perte de données et la machine virtuelle située sur le site local est une copie parfaite de la machine virtuelle dans le cloud), la phase de basculement est terminée. La machine virtuelle sur le site local est restaurée et la phase de validation démarre automatiquement.
4. **Validation**. Pendant cette phase, la machine virtuelle sur le site local est prête et démarre automatiquement. Vous pouvez vérifier si elle fonctionne correctement et :
   - Si tout fonctionne comme prévu, vous pouvez confirmer la restauration automatique. Après la confirmation de la restauration automatique, la machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**. Le processus de restauration automatique est alors terminé.
   - En cas d'anomalie, vous pouvez annuler le basculement et revenir à la phase de transfert de données.

Exécution d'une restauration automatique sans agent via un agent d'hyperviseur

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez effectuer une restauration automatique sans agent vers une machine virtuelle cible sur votre site local via un agent d'hyperviseur.

Prérequis

- L'agent que vous allez utiliser pour exécuter une restauration automatique est en ligne et n'est pas actuellement utilisé pour une autre opération de restauration automatique.
- Votre connexion Internet est stable.
- Il existe au moins une sauvegarde complète de la machine virtuelle dans le cloud.

© Acronis International GmbH, 2003-2026

Pour effectuer une restauration automatique sans agent vers une machine virtuelle via un agent d'hyperviseur

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans la section **Paramètres de restauration automatique**, sélectionnez dans le champ **Type de restauration automatique** l'option **Sans agent via l'agent d'hyperviseur**, puis configurez les autres paramètres.

   Notez que par défaut, certains des **paramètres de restauration automatique** sont remplis automatiquement avec des valeurs suggérées, mais vous pouvez les modifier.

   Le tableau suivant fournit plus de détails sur les **paramètres de restauration automatique**.

Paramètre	Description
Taille de la sauvegarde	Quantité de données qui sera transférée à votre site local lors du processus de restauration automatique. Une fois que vous aurez lancé le processus de restauration automatique vers une machine virtuelle cible, la **Taille de la sauvegarde** augmentera lors de la phase de transfert de données, car la machine virtuelle dans le cloud continuera à s'exécuter et à générer de nouvelles données. Pour calculer l'interruption d'activité estimée qui surviendra lors du processus de restauration automatique vers une machine virtuelle cible, partez de 10 % de la **Taille de la sauvegarde** (puisque nous vous recommandons de démarrer la phase de basculement quand 90 % des données ont été transférés vers votre site local) et divisez cette valeur par celle de la vitesse de votre connexion Internet. **Remarque** La valeur de la vitesse de votre connexion Internet diminuera quand vous exécuterez simultanément plusieurs processus de restauration automatique.
Emplacement de machine cible	Emplacement de restauration automatique : hôte VMware ESXi ou Microsoft Hyper-V. Vous pouvez faire votre choix parmi tous les hôtes qui possèdent un agent enregistré avec le service de cyberprotection.
Agent	Agent qui exécutera l'opération de restauration automatique. Vous pouvez utiliser un agent pour effectuer une opération de restauration automatique à la fois. Vous pouvez sélectionner un agent qui est en ligne et qui n'est pas actuellement utilisé pour un autre processus de restauration automatique, qui possède une version compatible avec la fonctionnalité de restauration automatique, et qui dispose des droits

© Acronis International GmbH, 2003-2026

Paramètre	Description
	d'accès à la sauvegarde. Notez que vous pouvez installer plusieurs agents sur des hôtes VMware ESXi, et démarrer un processus de restauration automatique séparé sur chacun d'eux. Ces processus de restauration automatique peuvent être exécutés simultanément.
Paramètres de machine cible	Paramètres de machine virtuelle : • **Processeurs virtuels**. Sélectionnez le nombre de processeurs virtuels. • **Mémoire**. Sélectionnez la quantité de mémoire dont disposera la machine virtuelle. • **Unités**. Sélectionnez les unités pour la mémoire. • [Facultatif] **Adaptateurs réseau**. Pour ajouter un adaptateur réseau, cliquez sur **Ajouter**, puis sélectionnez un réseau dans le champ **Réseau**. Quand les changements vous conviennent, cliquez sur **Terminé**.
Chemin d'accès	(Pour les hôtes Microsoft Hyper-V) Dossier sur l'hôte où votre machine sera stockée. Assurez-vous que l'espace disponible sur l'hôte est suffisant pour la machine.
Magasin de données	(Pour les hôtes VMware ESXi) Magasin de données sur l'hôte où votre machine sera stockée. Assurez-vous que l'espace disponible sur l'hôte est suffisant pour la machine.
Mode de provisionnement	Méthode d'allocation du disque virtuel. Pour les hôtes Microsoft Hyper-V : • **En expansion dynamique** (Valeur par défaut). • **Taille fixe**. Pour les hôtes Microsoft Hyper-V : • **Dynamique** (Valeur par défaut). • **Statique**.
Nom de machine cible	Le nom de la machine cible. Par défaut, le nom de la machine cible est le même que celui du serveur de restauration. Le nom de la machine cible doit être spécifique à l'**emplacement de la machine cible** sélectionné.

5. Cliquez sur **Démarrer le transfert de données** et, dans la fenêtre de confirmation, cliquez sur **Démarrer**.

© Acronis International GmbH, 2003-2026

Remarque
S'il n'y a pas de sauvegarde de la machine virtuelle dans le cloud, le système effectuera une sauvegarde automatiquement avant la phase de transfert des données.

La phase **Transfert de données** démarre. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre affiche la quantité de données déjà transférées vers le site local, ainsi que la quantité totale de données à transférer. La quantité totale de données comprend les données de la dernière sauvegarde avant le démarrage de la phase de transfert de données, ainsi que les sauvegardes des données nouvellement générées (incréments de sauvegarde), car la machine virtuelle continue à s'exécuter lors de la phase de transfert de données. Pour cette raison, les deux valeurs du paramètre **Progression** augmentent au fil du temps.
Estimation de l'interruption d'activité	Ce paramètre indique la durée d'indisponibilité de la machine virtuelle dans le cloud si vous démarrez la phase de basculement maintenant. La valeur est calculée en fonction des valeurs du paramètre **Progression** et diminue au fil du temps.

6. Cliquez sur **Basculement**, puis cliquez une nouvelle fois sur **Basculement** dans la fenêtre de confirmation.
   La phase de basculement commence. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre montre la progression de la restauration de la machine sur le site local.
Temps restant estimé	Ce paramètre indique l'heure approximative à laquelle la phase de basculement sera terminée et où vous pourrez démarrer la machine virtuelle sur le site local.

Remarque
Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

7. Une fois que la phase de **basculement** est terminée et que la machine virtuelle de votre site local est démarrée automatiquement, vérifiez qu'elle fonctionne comme prévu.
8. Cliquez sur **Confirmer la restauration automatique** et, dans la fenêtre de confirmation, cliquez sur **Confirmer** pour finaliser le processus.
   La machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

© Acronis International GmbH, 2003-2026

Remarque
Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

Restauration automatique en mode manuel

Remarque
Nous vous recommandons d'utiliser le processus de restauration automatique en mode manuel uniquement lorsque l'équipe de support vous l'indique.

Vous pouvez également démarrer un processus de restauration automatique en mode manuel. Dans ce cas, le transfert de données depuis la sauvegarde dans le cloud vers le site local n'est pas effectué automatiquement. Il doit être effectué manuellement après l'arrêt de la machine virtuelle dans le cloud. Le processus de restauration automatique en mode manuel est beaucoup plus lent et vous devez vous attendre à une interruption d'activité plus longue.

Le processus de restauration automatique en mode manuel se compose des phases suivantes :

1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.
2. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données générées récemment sont sauvegardées. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus. Lorsque la sauvegarde est terminée, restaurez manuellement la machine sur le site local. Vous pouvez restaurer le disque à l'aide d'un support de démarrage, ou restaurer la machine tout entière à partir du stockage de sauvegarde dans le Cloud.
3. **Validation**. Lors de cette phase, vous vérifiez que la machine physique ou virtuelle sur le site local fonctionne correctement, et confirmez la restauration automatique. Après la confirmation, la machine virtuelle sur le site dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

Réalisation d'une restauration automatique en mode manuel

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez exécuter une restauration automatique en mode manuel vers une machine cible physique ou virtuelle sur votre site local.

© Acronis International GmbH, 2003-2026

Pour effectuer une restauration automatique en mode manuel

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans le champ **Cible**, sélectionnez **Machine physique**.
5. Cliquez sur l'icône en forme d'engrenage, puis activer le paramètre **Utiliser le mode manuel**.
6. [Facultatif] Calculez le temps d'arrêt estimé qui surviendra lors du processus de restauration automatique en divisant la valeur **Taille de la sauvegarde** par la vitesse de votre connexion Internet.

   Remarque
   La valeur de la vitesse de votre connexion Internet diminuera quand vous exécuterez simultanément plusieurs processus de restauration automatique.

7. Cliquez sur **Basculement** et, dans la fenêtre de confirmation, cliquez une nouvelle fois sur **Basculement**.
   La machine virtuelle sur le site dans le Cloud est désactivée.

   Remarque
   Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

8. Restaurez le serveur depuis la sauvegarde dans le cloud vers la machine physique ou virtuelle sur votre site local. Pour plus d'informations, voir Restauration d'une machine dans le Guide de l'utilisateur Cyber Protection.
9. Assurez-vous que la restauration est terminée et que la machine restaurée fonctionne correctement, puis cliquez sur **La machine a été restaurée**.
10. Si tout fonctionne comme prévu, cliquez sur **Confirmer la restauration automatique** et, dans la fenêtre de confirmation, cliquez une nouvelle fois sur **Confirmer**.
    Le serveur de restauration et le point de restauration sont disponibles pour le prochain basculement. Pour créer de nouveaux points de restauration, appliquez un plan de protection au nouveau serveur local.

    Remarque
    Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

© Acronis International GmbH, 2003-2026

Restauration automatique depuis Cyber Protect Cloud vers une machine virtuelle Azure

Vous pouvez effectuer une restauration automatique depuis Cyber Protect Cloud vers la machine virtuelle Azure d'origine en suivant la procédure décrite dans "Réalisation d'une restauration automatique en mode manuel" (p. 1102) et en utilisant l'une des options de restauration suivantes à l'étape 8.

Options de restauration

- Restauration sans agent

  Prend en charge la restauration uniquement vers une nouvelle machine virtuelle Azure qui est créée automatiquement.

  Configurer la connexion Azure dans la console Cyber Protect (**Terminaux** > **Ajouter** > **Machine virtuelle Microsoft Azure**).

  Une machine virtuelle d'appliance de sauvegarde est déployée dans l'abonnement Azure pour gérer la restauration.

  Flux de restauration :

  1. Dans l'écran **Stockage de sauvegarde**, sélectionnez une sauvegarde.
  2. Restaurer en tant que machine virtuelle Azure.

  Vous pouvez utiliser le même flux pour les sauvegardes physiques, virtuelles ou avec agent.

  Pour réduire les coûts encourus, la machine virtuelle de l'appliance, lorsqu'elle est utilisée uniquement pour la restauration, peut être mise sous tension uniquement pendant la restauration, puis éteinte manuellement.
- Restauration avec agent

  Prend en charge la restauration sur la même machine virtuelle Azure (si la machine virtuelle d'origine avec l'agent est disponible) ou une nouvelle machine virtuelle Azure sur laquelle un nouvel agent est installé.

  Le processus se compose des étapes suivantes :

  1. Créez manuellement une machine virtuelle Windows ou Linux vierge dans Azure.
  2. Installez l'agent de protection.
  3. Utilisez l'agent pour parcourir et restaurer des sauvegardes à partir du stockage dans le cloud Acronis.

  Pour plus d'informations, voir Restaurer des ordinateurs Microsoft Azure et Amazon EC2.

Orchestration (runbooks)

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

© Acronis International GmbH, 2003-2026

Un runbook est un ensemble d'instructions décrivant comment lancer l'environnement de production dans le cloud. Vous pouvez créer des runbooks dans la console Cyber Protect.

Les runbooks vous permettent d'effectuer les opérations suivantes :

- Automatisez le basculement d'un ou de plusieurs serveurs.
- Vérifiez automatiquement le résultat du basculement en envoyant une commande ping à l'adresse IP du serveur et en vérifiant la connexion au port que vous spécifiez.
- Définissez la séquence d'opérations pour les serveurs exécutant des applications distribuées.
- Incluez des opérations manuelles dans votre workflow.
- Vérifier l'intégrité de votre solution de reprise d'activité après sinistre en exécutant des runbooks en mode test

Pour accéder à l'écran **Runbooks**, allez dans **Disaster Recovery** > **Runbooks**.

Création d'un runbook

Un runbook se compose d'étapes exécutées consécutivement. Une étape se compose d'actions qui commencent simultanément.

Pour créer un runbook, suivez les instructions de la procédure suivante ou de la vidéo de formation.

Pour créer un runbook

1. Dans la console Cyber Protection, accédez à **Disaster Recovery** > **Runbooks**.
2. Cliquez sur **Créer un runbook**.
3. Cliquez sur **Ajouter une étape**.
4. Cliquez sur **Ajouter une action**, puis sélectionnez l'action que vous souhaitez ajouter à l'étape.

Action	Description
Basculer le serveur	Effectue le basculement d'un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 1107). **Remarque** Si la sauvegarde du serveur que vous sélectionnez est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur, l'action de **Basculer le serveur** est mise en pause et passe automatiquement à **Interaction requise**. Pour poursuivre l'exécution du runbook, vous devez fournir le mot de passe de la sauvegarde chiffrée.
Restaurer le serveur automatiquement	Effectue la restauration automatique d'un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 1107).

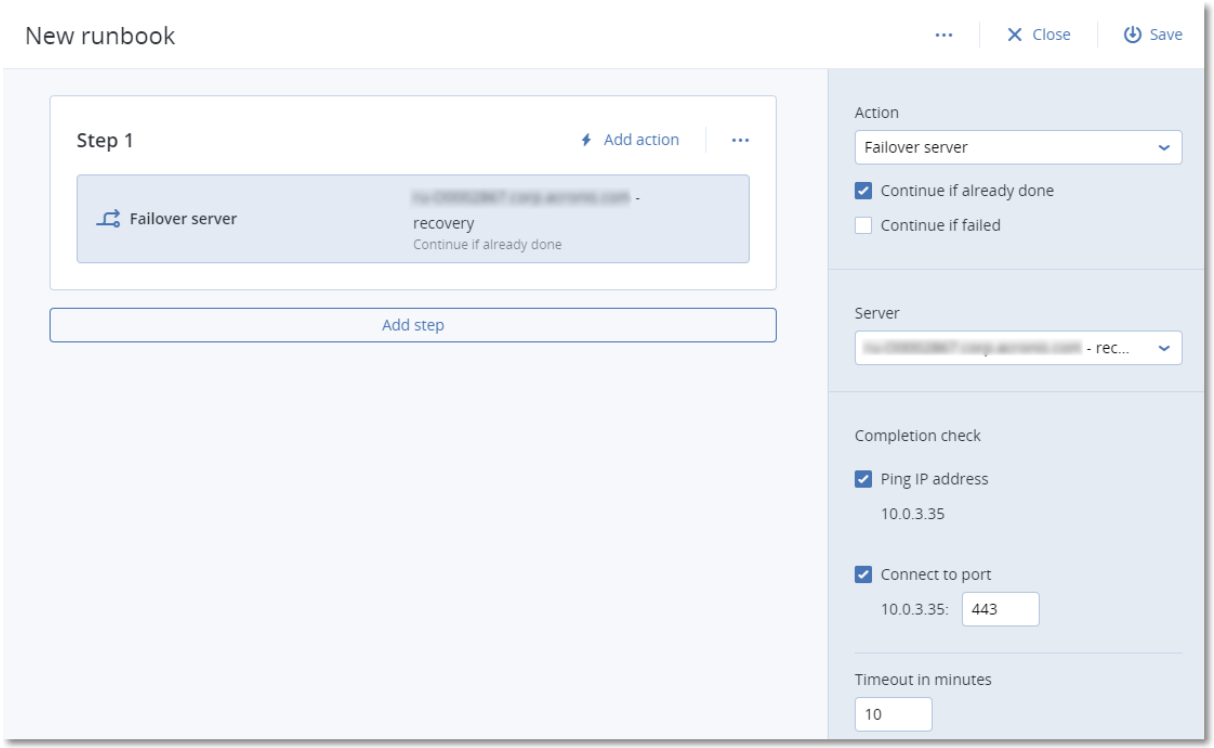
© Acronis International GmbH, 2003-2026

Action	Description
	Remarque Les opérations de runbook prennent en charge la restauration automatique en mode manuel uniquement. Cela signifie que si vous démarrez le processus de restauration automatique en exécutant un runbook qui inclut une étape **Restaurer le serveur automatiquement**, la procédure nécessitera une interaction manuelle : vous devez restaurer l'ordinateur manuellement, et confirmer ou annuler le processus de restauration automatique à partir de l'onglet **Disaster Recovery** > **Serveurs**.
Démarrer le serveur	Démarre un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 1107). **Remarque** L'action **Démarrer le serveur** ne s'applique qu'aux opérations de basculement test dans les runbooks. Si vous essayez d'exécuter une telle action, elle échoue et affiche le message d'erreur suivant : Échec : l'action ne s'applique pas à l'état actuel du serveur.
Arrêter le serveur	Arrête un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 1107). **Remarque** L'action **Arrêter le serveur** ne s'applique pas aux opérations de basculement test dans les runbooks. Si vous essayez d'exécuter une telle action, elle échoue et affiche le message d'erreur suivant : Échec : l'action ne s'applique pas à l'état actuel du serveur.
Opération manuelle	Une opération manuelle nécessite une interaction de la part de l'utilisateur. Pour définir cette action, vous devez entrer une description. Lorsqu'une séquence de runbook atteint une opération manuelle, le runbook est mis en pause et ne reprend que lorsqu'un utilisateur effectue l'opération manuelle requise, par exemple, clique sur le bouton de confirmation.
Exécuter le runbook	Exécute un autre runbook. Pour définir cette action, vous devez choisir un runbook. Un runbook ne peut contenir qu'une seule exécution d'un runbook donné. Par exemple, si vous avez ajouté l'action « Exécuter le runbook A », vous pouvez ajouter l'action « Exécuter le runbook B », mais vous ne pouvez pas ajouter une autre action « Exécuter le runbook A ».

5. Définissez les paramètres de runbook de l'action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 1107).

© Acronis International GmbH, 2003-2026

6. [Facultatif] Pour ajouter une description de l'étape :
   a. Cliquez sur l'icône représentant des points de suspension, puis cliquez sur **Description**.
   b. Entrez une description de l'étape.
   c. Cliquez sur **Terminé**.
7. Répétez les étapes 3 à 6 jusqu'à ce que vous ayez créé la séquence d'étapes et d'actions souhaitée.
8. [Facultatif] Pour changer le nom par défaut du runbook :
   a. Cliquez sur l'icône représentant des points de suspension.
   b. Entrez le nom du runbook.
   c. Entrez une description du runbook.
   d. Cliquez sur **Terminé**.
9. Cliquez sur **Enregistrer**.
10. Cliquez sur **Fermer**.



Paramètres du runbook

Les paramètres du runbook sont des paramètres spécifiques que vous devez configurer pour définir une action de runbook. Il existe deux catégories de paramètres de runbook : les paramètres d'action et les paramètres de vérification d'achèvement.

Les paramètres d'action définissent le comportement du runbook en fonction de l'état initial de l'action ou du résultat.

© Acronis International GmbH, 2003-2026

Les paramètres de vérification d'achèvement garantissent que le serveur est disponible et fournit les services nécessaires. En cas d'échec de la vérification d'achèvement, l'action est considérée comme ayant échoué.

Le tableau suivant décrit les paramètres de runbook configurables pour chaque action.

Paramètre de runbook	Catégorie	Disponible pour l'action	Description
Continuer si l'action a déjà été effectuée	Paramètre d'action	• **Basculer le serveur** • **Démarrer le serveur** • **Arrêter le serveur** • **Restaurer le serveur automatiquement**	Ce paramètre définit le comportement du runbook lorsque l'action requise est déjà effectuée (par exemple, lorsqu'un basculement a déjà été effectué ou qu'un serveur est déjà en fonctionnement). Lorsqu'il est activé, le runbook émet un avertissement et continue le processus. Lorsqu'il est désactivé, l'action échoue et le runbook échoue également. Par défaut, ce paramètre est activé.
Continuer si l'action a échoué	Paramètre d'action	• **Basculer le serveur** • **Démarrer le serveur** • **Arrêter le serveur** • **Restaurer le serveur automatiquement**	Ce paramètre définit le comportement du runbook lorsque l'action requise échoue. Lorsqu'il est activé, le runbook affiche un avertissement, puis continue. Lorsqu'il est désactivé, l'action et le runbook échouent. Par défaut, ce paramètre est désactivé.
Ping adresse IP	Vérification de l'achèvement	• **Démarrer le serveur**	Le logiciel va procéder au ping de l'adresse IP de production du serveur Cloud jusqu'à ce que le serveur réponde ou que le délai d'expiration soit dépassé, selon la première éventualité.
Se connecter au port (443 par défaut)	Vérification de l'achèvement	• **Basculer le serveur** • **Démarrer le serveur**	Le logiciel va essayer de se connecter au serveur Cloud à l'aide de son adresse IP de production et du port que vous indiquez, jusqu'à ce qu'une connexion soit établie ou que le délai d'expiration soit dépassé, selon la première éventualité. De cette manière, vous pouvez vérifier la bonne exécution de l'application qui

© Acronis International GmbH, 2003-2026

Paramètre de runbook	Catégorie	Disponible pour l'action	Description
			écoute le port indiqué.
Délai d'expiration en minutes	Vérification de l'achèvement	• **Basculer le serveur** • **Démarrer le serveur**	Le délai d'expiration par défaut est de 10 minutes.

Opérations avec les runbooks

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour accéder à la liste des opérations, survolez un runbook, puis cliquez sur l'icône en forme de points de suspension. Lorsqu'un runbook n'est pas en cours d'exécution, les opérations suivantes sont disponibles :

- **Exécuter**
- **Modifier**
- **Cloner**
- **Supprimer**

Exécution d'un runbook

À chaque fois que vous cliquez sur **Exécuter**, vous êtes invité à saisir les paramètres d'exécution. Ces paramètres s'appliquent à toutes les opérations de basculement ou de restauration automatique incluses dans le runbook. Les runbooks indiqués dans les opérations **Exécuter le runbook** héritent de ces paramètres du runbook principal.

- **Mode basculement et restauration automatique**
  Choisissez si vous souhaitez réaliser un basculement test (par défaut) ou un basculement réel (production). Le mode de restauration automatique correspondra au mode de basculement choisi.
- **Point de restauration en mode basculement**
  Choisissez le point de restauration le plus récent (par défaut) ou sélectionnez un moment donné dans le passé. Dans le deuxième cas, les points de restauration situés le plus près avant la date et l'heure choisis seront sélectionnés pour chaque serveur.

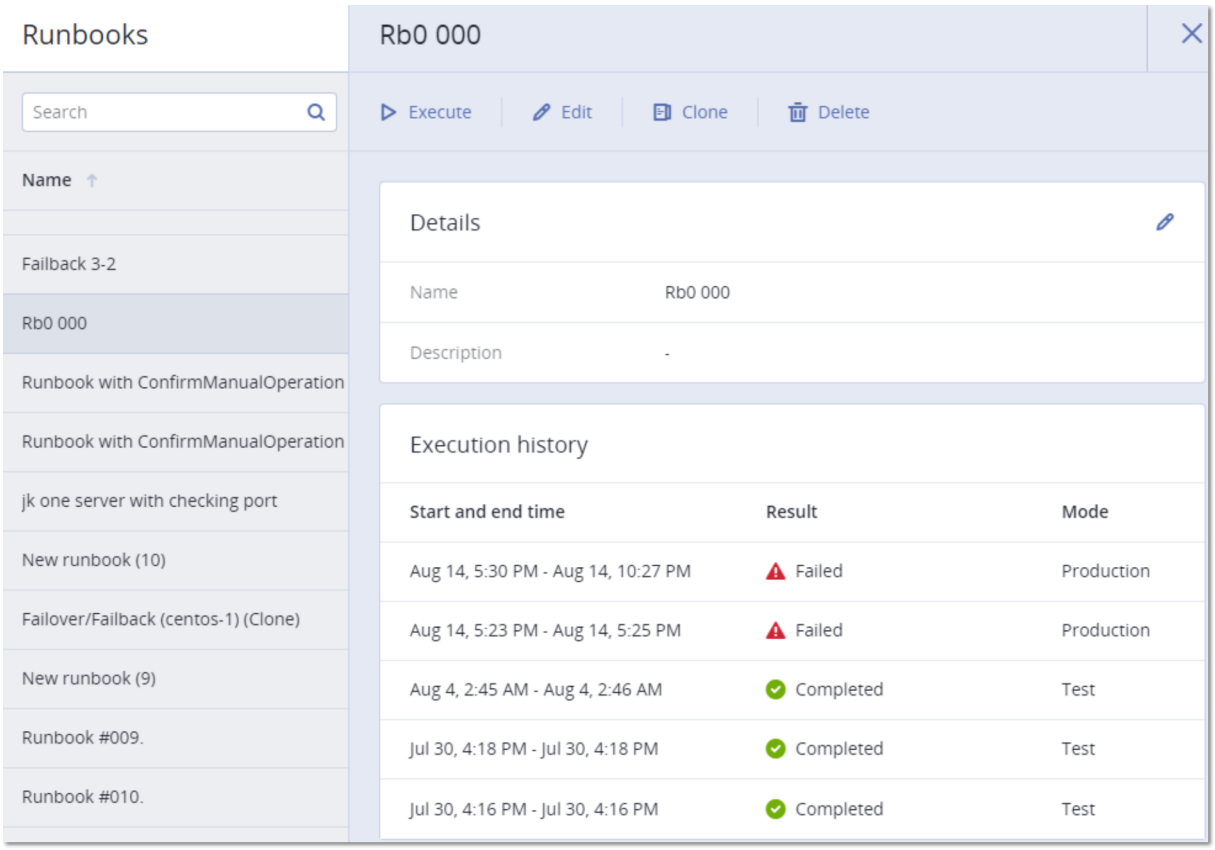
Arrêt de l'exécution d'un runbook

Lors de l'exécution d'un runbook, vous pouvez sélectionner **Arrêter** dans la liste des opérations. Le logiciel terminera toutes les actions déjà démarrées, à l'exception de celles qui nécessitent une intervention de l'utilisateur.

© Acronis International GmbH, 2003-2026

Affichage de l'historique d'exécution

Lorsque vous sélectionnez un runbook dans l'onglet **Runbooks**, le logiciel affiche les détails du runbook et son historique d'exécution. Cliquez sur la ligne correspondant à une exécution spécifique pour afficher le journal d'exécution.



Suppression du site de reprise d'activité après sinistre

Vous pouvez supprimer le site de reprise d'activité après sinistre. Cette action supprimera automatiquement la passerelle VPN, les connexions VPN et tous les runbooks qui ont été configurés sur le site.

Prérequis

Aucun serveur cloud n'est disponible sur le site de reprise d'activité après sinistre.

Pour supprimer le site de reprise d'activité après sinistre

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Afficher les propriétés**.
3. Cliquez sur **Supprimer le site de reprise d'activité après sinistre**.
4. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

© Acronis International GmbH, 2003-2026

Disaster Recovery vers Microsoft Azure

Disaster Recovery vers Microsoft Azure est une solution de reprise d'activité après sinistre économique intégrée au service Acronis Cyber Protection. Elle exploite la puissance et la flexibilité de la plate-forme de niveau entreprise Microsoft Azure en tant que site DR cible. Cette solution utilise des sauvegardes à froid (points de restauration), qui peuvent être stockées dans Microsoft Azure, Acronis Cyber Protect Cloud ou un stockage dans le cloud hébergé par un partenaire. La configuration et l'orchestration de l'ensemble du site DR sont gérées de manière centralisée à partir de la console Cyber Protect. Votre propre abonnement Microsoft Azure est utilisé comme site DR cible.

L'automatisation et l'orchestration comprennent les fonctionnalités suivantes :

- Configuration initiale du site DR
- Basculement test automatisé avec vérification des captures d'écran par intelligence artificielle
- Basculement orchestré
- Restauration automatique sur des machines physiques et des machines virtuelles, avec une interruption d'activité quasi nulle
- Runbooks pour automatiser les scénarios clés de reprise d'activité après sinistre
- Workers à la demande (agents temporaires) qui éliminent le besoin d'appliances virtuelles permanentes
- Reprise d'activité après sinistre sur site froid – Les sauvegardes sont stockées dans le stockage, mais aucune ressource de calcul (machine virtuelle) n'est en cours d'exécution tant qu'un sinistre ne survient pas. La reprise d'activité sur site froid offre une restauration économique avec une utilisation minimale de l'infrastructure Azure.
- Reprise d'activité sur site tiède (à venir dans les prochaines versions) – les sauvegardes sont répliquées de manière incrémentielle dans le stockage tiède Azure et, en cas de sinistre, sont prêtes à être exécutées en tant que machines virtuelles Azure. La reprise d'activité sur site tiède offre un objectif de délai de restauration (RTO) proche de zéro.

Vous conservez le contrôle total sur l'infrastructure sous-jacente et les fonctionnalités de Microsoft Azure, avec la flexibilité d'utiliser les services Azure natifs ou d'intégrer des solutions personnalisées - telles que des pare-feu tiers et des appliances SD-WAN - en les connectant aux réseaux de restauration sélectionnés sur le site DR. Cette solution prend également en charge le basculement de postes de travail Windows exécutant Windows 10 ou Windows 11.

Remarque
Pour utiliser Disaster Recovery sur Microsoft Azure, vous devez disposer d'un abonnement activé à Microsoft Azure.

© Acronis International GmbH, 2003-2026

Exigences logicielles pour Disaster Recovery vers Microsoft Azure

Systèmes d'exploitation pris en charge

La protection via un serveur de restauration dans Microsoft Azure a été testée pour les systèmes d'exploitation suivants :

- Ubuntu 20.x, 21.x, 22.10, 23.04
- Debian 10.x, 11.x
- Red Hat Enterprise Linux 8.x, 9.x
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server
- Windows Server 2025 – toutes les options d'installation, sauf Nano Server
- Windows 10
- Windows 11

Le logiciel peut fonctionner avec d'autres systèmes d'exploitation Windows ou d'autres distributions Linux, mais cela n'est pas garanti.

Plates-formes de virtualisation prises en charge

La protection de machines virtuelles à l'aide d'un serveur de restauration a été testée pour les plates-formes de virtualisation suivantes :

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 avec Hyper-V
- Windows Server 2012/2012 R2 avec Hyper-V
- Windows Server 2016 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2019 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Windows Server 2022 avec Hyper-V – toutes les options d'installation, excepté Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Machines virtuelles basées sur un noyau (KVM) — Invités entièrement virtualisés (HVM) uniquement. Les invités paravirtualisés (PV) ne sont pas pris en charge.

Les ressources Linux qui ont des sauvegardes sans agent à partir d'un SE invité et des volumes avec des configurations de LVM (Logical Volume Manager) sont prises en charge.

© Acronis International GmbH, 2003-2026

Les ressources Windows qui ont des sauvegardes sans agent à partir d'un SE invité et des configurations de LDM (disques dynamiques) sont prises en charge.

Le logiciel peut fonctionner avec d'autres plates-formes de virtualisation ou d'autres versions, mais cela n'est pas garanti.

Limites

Les plates-formes et configurations suivantes ne sont pas prises en charge dans Disaster Recovery vers Microsoft Azure :

1. Plateformes non prises en charge :
   - Agents pour Virtuozzo
   - macOS
2. Configurations non prises en charge :

   Microsoft Windows
   - Le service Active Directory avec réplication FRS n'est pas pris en charge.
   - Les supports amovibles sans formatage GPT ou MBR (dits « super disquettes ») ne sont pas pris en charge.

   Linux
   - Systèmes de fichiers sans table de partition.
   - Les ressources Linux qui sont sauvegardées avec un agent d'un SE invité et dont les volumes ont les configurations Logical Volume Manager avancées suivantes : volumes agrégés par bandes, volumes en miroir, volumes RAID 0, RAID 4, RAID 5, RAID 6 ou RAID 10.

   Remarque
   Les ressources ayant plusieurs systèmes d'exploitation installés ne sont pas prises en charge.
3. Modes de tenant non pris en charge :
   - La reprise d'activité après sinistre n'est pas disponible lorsque le mode de conformité est activé pour le tenant.
4. Types de sauvegarde non pris en charge :
   - Les points de restauration de la protection continue des données (CDP) sont incompatibles.

     Important
     Si vous créez un serveur de restauration à partir d'une sauvegarde disposant d'un point de restauration CDP, lors de la restauration automatique ou lors de la création d'une sauvegarde d'un serveur de restauration, vous perdrez les données contenues dans le point de restauration CDP.
   - Les sauvegardes de données d'investigation ne peuvent pas être utilisées pour créer des serveurs de restauration.

Les serveurs Cloud ne sont pas chiffrés.

© Acronis International GmbH, 2003-2026

Licence de Disaster Recovery pour Microsoft Azure

Pour activer Disaster Recovery sur Microsoft Azure, l'élément d'offre **DR et sauvegarde directe sur Azure** doit être activé pour votre tenant. Cet élément d'offre permet :

- Disaster Recovery (DR) vers Azure qui utilise l'abonnement Azure du client.
- Sauvegarde directe vers Azure.

Un quota de l'élément d'offre est consommé lorsqu'un serveur de restauration est créé ou qu'une sauvegarde directe vers Azure est activée. Un quota par ressource est utilisé, même si la DR et la sauvegarde directe sont toutes deux actives.

Le quota pour cet élément d'offre qui est affecté à votre tenant représente le nombre maximum de ressources qui peuvent être protégées. Un terminal qui utilise à la fois Disaster Recovery vers Azure et la sauvegarde directe vers Azure consomme un quota.

Quota inconditionnel : surconsommation

Lorsque le quota inconditionnel de l'offre est réduit, les serveurs de restauration existants peuvent devenir non licenciés. Le nombre de serveurs de restauration non licenciés dépend de la surconsommation. Les serveurs de restauration qui étaient en basculement test ou de production restent fonctionnels mais deviennent non licenciés. Les serveurs de restauration non licenciés dans l'état En attente ont des opérations DR limitées. Vous ne pouvez pas mettre sous tension les serveurs non licenciés tant qu'ils ne sont pas à nouveau licenciés.

L'augmentation du quota d'éléments de l'offre affecte automatiquement des licences aux terminaux non licenciés et efface les alertes associées.

Alertes générées

Les alertes suivantes sont générées lorsqu'il y a des problèmes causés par des licences manquantes.

- **Le serveur de restauration n'est pas sous licence** - Cette alerte est générée lorsqu'un serveur devient non sous licence.
- **La protection Disaster Recovery a été désactivée pour une ressource** - Cette alerte est générée lorsqu'il n'y a pas de licences disponibles.
- **Échec du basculement test automatisé** - Cette alerte est générée lorsqu'un basculement est bloqué en raison d'une licence manquante.

Travailler avec Disaster Recovery vers Microsoft Azure

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Le workflow de base utilisant la reprise d'activité après sinistre est le suivant :

© Acronis International GmbH, 2003-2026

1. Configurez votre site DR dans Microsoft Azure. Pour plus d'informations, voir "Création d'un site de reprise d'activité après sinistre dans Microsoft Azure" (p. 1118).
2. Créez un serveur de restauration de la ressource que vous souhaitez protéger. Pour plus d'informations, voir "Création de serveurs de restauration dans Microsoft Azure" (p. 1127).
3. [Facultatif] Configurez la connectivité de votre site local vers le site cloud dans Microsoft Azure en utilisant les services natifs Azure, tels que le VPN site à site Azure ou Azure ExpressRoute. Pour plus d'informations, voir "Connectivité et réseaux dans Microsoft Azure" (p. 1120).
4. [Facultatif] Configurer les runbooks. Pour plus d'informations, voir "Création d'un runbook dans Microsoft Azure" (p. 1153).
5. Configurer le basculement test automatisé ou effectuer un basculement test. Pour plus d'informations, voir "Configuration du basculement test automatisé dans Microsoft Azure" (p. 1137) et "Exécution d'un basculement test dans Microsoft Azure" (p. 1134).
6. [En cas de sinistre] Effectuer un basculement de production. Pour plus d'informations, voir "Exécution d'un basculement de production dans Microsoft Azure" (p. 1133).
7. [Après le sinistre] Effectuez une restauration automatique vers le site local. Pour plus d'informations, voir "Restauration automatique dans Microsoft Azure" (p. 1139).

Gestion de l'accès à votre abonnement Microsoft Azure

Disaster Recovery à Microsoft Azure nécessite que vous vous connectiez à un abonnement Microsoft Azure dans la console Cyber Protect.

Vous pouvez configurer les abonnements Microsoft Azure dans l'écran **Infrastructure** > **Clouds publics**. Vous pouvez également gérer vos abonnements en effectuant les tâches suivantes : renouveler l'accès à l'abonnement, afficher les propriétés et les activités de l'abonnement ou supprimer l'abonnement.

Le tableau suivant fournit les liens vers la procédure correspondante pour la tâche que vous souhaitez accomplir.

Tâche	Lien
Ajouter l'accès à un abonnement Microsoft Azure	"Ajout de l'accès à un abonnement Microsoft Azure" (p. 762)
Renouveler l'accès à un abonnement Microsoft Azure	"Renouvellement de l'accès à un abonnement Microsoft Azure" (p. 763)
Supprimer l'accès à un abonnement Microsoft Azure	"Suppression de l'accès à un abonnement Microsoft Azure" (p. 764)

Problèmes de configuration inter-abonnements dans Microsoft Azure

Si vous utilisez deux abonnements différents pour Microsoft Azure — par exemple, un pour la sauvegarde directe vers Microsoft Azure (« Abonnement 1 ») et un autre pour la configuration du

© Acronis International GmbH, 2003-2026

site DR dans Microsoft Azure (« Abonnement 2 ») — mais que vous supprimez l'accès à « Abonnement 1 », les problèmes suivants se produiront :

- Le basculement échouera

  Vous ne pouvez pas démarrer un basculement, car les données de sauvegarde sont stockées dans « Abonnement 1 ».
- La restauration automatique échouera

  Si l'accès à « Abonnement 1 » est supprimé après qu'un basculement a été effectué, il ne sera pas possible d'accéder à toutes les données de sauvegarde qui sont stockées dans l'abonnement. Par conséquent, il ne sera pas possible d'effectuer des opérations de sauvegarde de machines virtuelles en basculement et en restauration automatique. Tant que les données de sauvegarde restent dans « Abonnement 1 », les opérations de basculement ou de restauration reposent sur un accès et des autorisations valides à l'emplacement de stockage d'origine. La suppression de l'accès rompt cette dépendance, même si des opérations DR sont démarrées dans un abonnement différent.

Important
Ne supprimez ni ne révoquez l'accès à l'abonnement Azure d'origine si les sauvegardes qui y sont stockées sont encore utilisées ou nécessaires.

Création d'un plan de protection de reprise d'activité après sinistre avec Microsoft Azure

Le plan de protection de reprise d'activité après sinistre est un plan de protection dans lequel le module **Reprise d'activité après sinistre** est activé.

Pour Microsoft Azure, l'emplacement du site DR doit être configuré. Il n'est pas possible d'appliquer un plan de protection avec un emplacement DR Azure s'il n'a pas été configuré.

© Acronis International GmbH, 2003-2026

Remarque

- L'application d'un plan de protection de reprise d'activité après sinistre crée des serveurs de restauration dans le cloud. Les réseaux cloud existants ne sont ni modifiés ni recréés.
- Une fois que vous aurez configuré la reprise d'activité après sinistre, vous serez en mesure d'effectuer un basculement test ou de production à partir de n'importe quel point de restauration (sauvegarde) généré après la création du serveur de restauration pour le terminal. Les points de restauration générés avant que le terminal ne soit protégé par la reprise d'activité après sinistre (avant la création du serveur de restauration) ne peuvent pas être utilisés.
- Un plan de protection de reprise d'activité après sinistre ne peut pas être activé si l'adresse IP d'un terminal ne peut pas être détectée. Par exemple, lorsque des machines virtuelles sont sauvegardées sans agent et qu'aucune adresse IP ne leur a été affectée. Dans ce cas, nous vous recommandons de créer manuellement un serveur de restauration.
- Lorsque vous appliquez un plan de protection, les serveurs de restauration sont configurés dans le sous-réseau qui a été configuré dans les règles de mappage lors de la configuration de l'emplacement du site DR, en fonction de l'adresse IP du terminal d'origine. Si l'adresse IP correspond à l'un des réseaux locaux d'origine spécifiés, le serveur de restauration sera créé dans le réseau de restauration Azure et le sous-réseau correspondants. Le dernier octet de l'adresse IP privée sera pris à partir de l'adresse IP de l'ordinateur d'origine.

Pour créer un plan de protection de reprise d'activité après sinistre

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les machines que vous souhaitez protéger.
3. Cliquez sur **Protection**, puis sur **Création d'un plan**.
   Les paramètres par défaut du plan de protection s'affichent.
4. Configurez les options de sauvegarde.
   Pour utiliser la fonctionnalité de reprise d'activité après sinistre, le plan doit sauvegarder l'intégralité de l'ordinateur, ou uniquement les disques requis pour le démarrage et la fourniture des services nécessaires, vers un stockage dans le cloud ou dans Microsoft Azure.
5. Activez le module **Reprise d'activité après sinistre** en activant l'interrupteur à côté du nom du module.
6. Dans le champ **Emplacement**, sélectionnez **Microsoft Azure**.
7. Cliquez sur **Créer**.
   Le plan est créé et appliqué aux ordinateurs sélectionnés. Les serveurs de restauration avec les paramètres par défaut sont créés.

Gestion du site de reprise d'activité après sinistre dans Microsoft Azure

Vous pouvez créer et configurer votre site de reprise d'activité après sinistre (DR) dans Microsoft Azure, soit dans le cadre de la création d'un plan de protection de reprise d'activité après sinistre,

© Acronis International GmbH, 2003-2026

soit via une procédure distincte, à partir de l'écran **Disaster Recovery**.

Lorsqu'un plan de protection de reprise d'activité après sinistre est appliqué, l'infrastructure réseau cloud du serveur de restauration est créée uniquement si elle n'existe pas déjà. Les serveurs et réseaux cloud existants ne sont pas modifiés ni recréés.

Un plan de protection de reprise d'activité après sinistre ne peut pas être activé si l'adresse IP d'un terminal ne peut pas être détectée. Par exemple, lorsque des machines virtuelles sont sauvegardées sans agent et qu'aucune adresse IP ne leur a été affectée. Dans ce cas, nous vous recommandons de créer manuellement un serveur de restauration.

Lorsque vous appliquez un plan de protection, les serveurs de restauration sont configurés dans le sous-réseau qui est configuré dans les règles de mappage lors de la configuration de l'emplacement du site DR, et sont basés sur l'adresse IP du terminal d'origine. Si l'adresse IP correspond à l'un des réseaux locaux d'origine spécifiés, le serveur de restauration sera créé dans le réseau de restauration Azure et le sous-réseau correspondants. Le dernier octet de l'adresse IP privée sera pris à partir de l'adresse IP de l'ordinateur d'origine.

Création d'un site de reprise d'activité après sinistre dans Microsoft Azure

Prérequis

- Vous disposez d'un abonnement à Microsoft Azure.
- Votre compte Microsoft a l'un des rôles Entra ID suivants : administrateur d'application cloud, administrateur d'application ou administrateur global.
- Votre compte Microsoft a le rôle de Propriétaire pour l'abonnement Azure.
- L'élément de l'offre DR et sauvegarde directe vers Azure est activé pour votre tenant.

À partir de tous les terminaux

Pour créer un site DR dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les ressources que vous souhaitez protéger.
3. Dans le menu **Actions**, cliquez sur **Protéger**.
4. Créez un plan de protection et configurez les paramètres suivants :
   a. Dans le module **Sauvegarde**, dans le champ **Où sauvegarder**, sélectionnez l'emplacement de stockage des sauvegardes de vos ressources.
   b. Activez le module **Reprise d'activité après sinistre**, puis cliquez sur le champ **Emplacement**.

© Acronis International GmbH, 2003-2026

Remarque
Si seul l'élément de l'offre **DR et sauvegarde directe sur Azure** est activé pour votre tenant, l'emplacement ne sera pas présélectionné et vous verrez un lien **Configurer**.
Si les éléments de l'offre **DR vers Acronis ou cloud hybride** et **DR et sauvegarde directe sur Azure** sont tous deux activés pour votre tenant, Cyber Protect Cloud sera présélectionné en tant qu'emplacement.

c. Dans l'assistant **Configuration du site de reprise d'activité après sinistre**, dans l'onglet **Emplacement du site**, sélectionnez **Cloud Microsoft Azure**, puis cliquez sur **Suivant**.
d. Dans l'onglet **Abonnement Azure**, procédez comme suit :
   - Si votre abonnement Microsoft Azure a déjà été ajouté à la console Cyber Protect, cliquez dessus, puis cliquez sur **Suivant**.
   - Si vous souhaitez ajouter un nouvel abonnement Microsoft Azure, cliquez sur **Ajouter abonnement**, ajoutez l'abonnement, cliquez dessus, puis cliquez sur **Suivant**.
e. Dans l'onglet **Région cible**, dans le champ **Région Azure**, sélectionnez la région Azure pour le site DR.
f. Dans l'onglet **Réseau de restauration**, configurez les réseaux de restauration pour le basculement de production et basculement test, puis cliquez sur **Suivant**.

Option	Description
Configuration par défaut	Utilisez cette option si vous souhaitez que les réseaux de production et de test dans Azure soient créés automatiquement, avec un réseau pour chaque environnement.
Configuration avancée	Utilisez cette option si vous souhaitez sélectionner vos réseaux Azure existants comme réseaux de production et de test et configurer le mappage.

g. Dans l'onglet **Résumé**, passez en revue les paramètres de votre site DR, puis cliquez sur **Configurer**.

Le plan de protection est appliqué avec succès aux ressources sélectionnées. Le site DR est créé dans Azure, dans la région Azure sélectionnée. Sur l'écran **Disaster Recovery** > **Connectivité**, vous pouvez afficher les réseaux de production et de test, ainsi que les serveurs de restauration créés, en mode **En attente**.

De la connectivité

Pour créer un site DR dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery**.
2. Cliquez sur **Configurer**.
3. Dans l'assistant **Configuration du site de reprise d'activité après sinistre**, dans l'onglet **Emplacement du site**, sélectionnez **Cloud Microsoft Azure**, puis cliquez sur **Suivant**.
4. Dans l'onglet **Abonnement Azure**, procédez comme suit :

© Acronis International GmbH, 2003-2026

- Si votre abonnement Microsoft Azure a déjà été ajouté à la console Cyber Protect, cliquez dessus, puis cliquez sur **Suivant**.
- Si vous souhaitez ajouter un nouvel abonnement Microsoft Azure, cliquez sur **Ajouter abonnement**, ajoutez l'abonnement, cliquez dessus, puis cliquez sur **Suivant**.

5. Dans l'onglet **Région cible**, dans le champ **Région Azure**, sélectionnez la région Azure pour le site DR.
6. Dans l'onglet **Réseau de restauration**, configurez les réseaux de restauration pour le basculement de production et basculement test, puis cliquez sur **Suivant**.

Option	Description
Configuration par défaut	Utilisez cette option si vous souhaitez que les réseaux de production et de test dans Azure soient créés automatiquement, avec un réseau pour chaque environnement.
Configuration avancée	Utilisez cette option si vous souhaitez sélectionner vos réseaux Azure existants comme réseaux de production et de test et configurer le mappage.

7. Dans l'onglet **Résumé**, passez en revue les paramètres de votre site DR, puis cliquez sur **Configurer**.

   Le site DR est créé dans Azure, situé dans la région Azure sélectionnée. Dans l'écran **Disaster Recovery** > **Connectivité**, vous pouvez afficher les réseaux de production et de test.

Suppression du site DR à partir de Microsoft Azure

Vous pouvez supprimer le site DR à partir de Microsoft Azure si vous n'en avez plus besoin ou si vous souhaitez modifier l'emplacement du site DR.

Prérequis

Il n'y a pas de serveur de restauration sur le site DR.

Pour supprimer le site DR à partir de Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Cliquez sur **Supprimer le site de reprise d'activité après sinistre**.
3. Dans la fenêtre **Supprimer le site de reprise d'activité après sinistre**, saisissez votre identifiant, puis cliquez sur **Supprimer**.

Connectivité et réseaux dans Microsoft Azure

Disaster Recovery vers Microsoft Azure permet l'orchestration des tests, des basculements et des restaurations automatiques, ainsi que la sélection de réseaux de restauration (réseaux virtuels Azure et sous-réseaux) pour les scénarios de basculement de production et basculement test. Vous pouvez configurer ces réseaux lors de la configuration initiale du site DR ou ultérieurement : depuis l'écran **Connectivité**, ou individuellement pour chaque serveur de restauration.

© Acronis International GmbH, 2003-2026

Vous conservez le contrôle total sur la mise en réseau et la connectivité Azure, et vous avez la flexibilité d'exploiter les capacités de la plate-forme Azure ou d'apporter des solutions personnalisées, telles que des pare-feu tiers ou des appliances SD-WAN sur le site DR, en les connectant aux réseaux de restauration sélectionnés.

Voici un aperçu des principaux services de mise en réseau Azure, de leur pertinence pour les cas d'utilisation de reprise d'activité après sinistre et de liens pour plus d'informations.

Pare-feu Azure

Le pare-feu Azure fournit un filtrage centralisé à états du trafic réseau sur plusieurs VNets et sous-réseaux. Il aide à appliquer des règles de sécurité entre les ressources après un basculement et prend en charge les scénarios où les environnements DR doivent respecter les stratégies de conformité ou de segmentation de l'entreprise.

Vous pouvez utiliser le pare-feu Azure pour contrôler le trafic sortant et entrant vers et depuis les machines virtuelles basculées (par exemple, pour limiter l'accès Internet et autoriser uniquement les sources figurant sur la liste d'autorisation). Pour une exposition gérée, placez le pare-feu Azure entre le réseau sur site (via VPN) et les réseaux virtuels Azure DR.

Pour plus d'informations, voir la documentation Microsoft Azure.

Groupes de sécurité réseau (NSG)

Les NSG permettent de définir des règles granulaires pour autoriser ou refuser le trafic réseau vers des machines virtuelles ou des sous-réseaux. Ils opèrent au niveau de la carte réseau de la machine virtuelle et du sous-réseau.

Vous pouvez appliquer des NSG pour contrôler l’accès aux machines virtuelles de restauration, garantir l’isolement des basculements test ou exposer uniquement les ports nécessaires (par exemple, RDP et HTTP). Les NSG sont essentiels pour activer en toute sécurité la connectivité en fonction du mode de la machine virtuelle de restauration : test ou production.

Pour plus d'informations, voir la documentation Microsoft Azure.

Serveurs DNS

Les VNets Azure prennent en charge les configurations de serveur DNS personnalisées ou l'intégration avec Azure DNS. Cela permet de contrôler la manière dont la résolution de noms fonctionne dans l'environnement DR.

Assurez-vous que les machines virtuelles DR résolvent les noms correctement, soit vers d'autres services restaurés dans Azure, soit vers des systèmes externes. Un DNS personnalisé est essentiel lors de la restauration d'environnements intégrés à AD ou pour permettre le transfert DNS vers des systèmes sur site.

Pour plus d'informations, voir la documentation Microsoft Azure.

© Acronis International GmbH, 2003-2026

Routage de sous-réseau (itinéraires définis par l'utilisateur)

Azure permet la création de routes personnalisées (UDR) pour contrôler le flux de trafic entre les sous-réseaux et vers les réseaux sur site, en remplaçant le routage système par défaut.

Créez des itinéraires pour diriger le trafic des machines virtuelles de restauration via des pare-feu, vers des passerelles VPN ou des points d'inspection. Cela permet d'appliquer des stratégies de routage et d'assurer la connectivité vers les environnements sur site via VPN ou ExpressRoute.

Pour plus d'informations, voir la documentation Microsoft Azure.

Adresses IP publiques

Les machines virtuelles Azure peuvent se voir affecter des adresses IP publiques (statiques ou dynamiques) pour permettre un accès direct à Internet si nécessaire. Cela est utile pour exposer des services ou un accès distant.

Affectez des adresses IP publiques aux ressources de basculement qui nécessitent un accès externe (par exemple, les serveurs Web et la gestion à distance). Évitez pour les ressources sensibles. Utilisez plutôt Bastion ou VPN lorsque cela est possible.

Pour plus d'informations, voir la documentation Microsoft Azure.

Azure Bastion

Azure Bastion permet un accès RDP/SSH sécurisé, basé sur navigateur, aux machines virtuelles sans exposer d'adresses IP publiques. Il fonctionne via le portail Azure et utilise le chiffrement TLS.

Accédez en toute sécurité aux machines virtuelles restaurées pour le diagnostic ou la reconfiguration manuelle après un basculement. Cela est particulièrement utile lors d'un basculement test où l'exposition à Internet n'est pas souhaitée.

Pour plus d'informations, voir la documentation Microsoft Azure.

Azure VPN site à site

Le VPN site à site fournit une connexion IPsec chiffrée entre votre réseau sur site et les réseaux virtuels Azure, permettant une connectivité hybride.

Assurez un accès fluide aux ressources restaurées à partir de réseaux sur site. Critique pour accéder aux applis internes ou restaurer les dépendances croisées avec les systèmes encore en cours d'exécution sur site.

Pour plus d'informations, voir la documentation Microsoft Azure.

Azure ExpressRoute

ExpressRoute offre une connectivité privée dédiée entre votre centre de données et Azure, contournant Internet pour améliorer la vitesse, la fiabilité et la sécurité.

© Acronis International GmbH, 2003-2026

Recommandé pour la DR de niveau entreprise avec de grands ensembles de données ou des exigences de faible latence. Utilisez-le pour connecter des systèmes sur site avec des machines virtuelles DR dans Azure sans avoir recours à un VPN.

Pour plus d'informations, voir la documentation Microsoft Azure.

Gestion de la mise en réseau dans Microsoft Azure

Les réseaux de restauration sont des réseaux virtuels Azure (VNets) et des sous-réseaux où vos systèmes de sauvegarde (serveurs de restauration) s'exécuteront si vos systèmes principaux tombent en panne.

Il existe deux types de réseaux de restauration : les réseaux de restauration de production et les réseaux de restauration de test.

Réseau de restauration de production

Les réseaux de restauration de production sont utilisés lors d'une véritable catastrophe lorsque vous devez déplacer vos services vers Azure. Les ressources (machines virtuelles) basculées sont connectées à ces réseaux de restauration afin que les opérations de l'entreprise puissent reprendre.

Voici un exemple de réseau de production :

VNet : `dr-prod-vnet-91a4e5bf`

Sous-réseau : `subnet-one (10.0.10.0/24)`

Réseau de test de restauration

Les réseaux de test de restauration sont utilisés lors de basculements test manuels ou automatisés pour vérifier que la reprise d'activité après sinistre fonctionne sans affecter vos systèmes de production.

Pour éviter les conflits d'adresses IP ou les fuites de données, les réseaux de restauration de test doivent être isolés de l'environnement de production. Pour éviter tout chevauchement avec les réseaux de production, il est de bonne pratique d'utiliser un VNet dédié.

Pour plus d'informations sur la planification et la conception de VNets, voir la documentation Microsoft Azure.

Bonnes pratiques pour la Disaster Recovery configuration réseau

Lorsque vous configurez les réseaux de restauration dans Disaster Recovery vers Microsoft Azure, nous vous recommandons de suivre les bonnes pratiques suivantes :

- Séparer les VNets et sous-réseaux de production et de test
  Conservez les environnements de test et de production isolés.
- Utilisez les balises et conventions de nommage Azure

© Acronis International GmbH, 2003-2026

Étiquetez clairement les réseaux (par exemple, `dr-prod` et `dr-test`) pour faciliter l'identification et l'automatisation.

- Planifiez soigneusement les plages d'adresses IP

  Assurez-vous que les VNets et les sous-réseaux ne sont pas en conflit avec les réseaux sur site s'il existe une connectivité entre le site de DR et les environnements sur site, par exemple via un VPN IPsec ou ExpressRoute.

  Maintenez des schémas d'adressage cohérents pour faciliter le routage et l'intégration de l'identité.
- Préconfigurez les ressources réseau requises

  Les groupes de sécurité réseau, les tables de routage, le DNS personnalisé et les adresses IP publiques doivent être configurés à l'avance pour les réseaux de restauration de test et de production.

Recommandations pour la disponibilité des services de domaine Active Directory

Si vos ressources protégées doivent s'authentifier auprès d'un contrôleur de domaine, nous vous recommandons de disposer d'une instance de contrôleur de domaine Active Directory (AD DC) sur le site DR de Microsoft Azure.

Recommandations pour la disponibilité d'AD DS sur le site DR dans Azure

Les recommandations pour une instance dédiée de contrôleur de domaine Active Directory (AD DC) sur le site DR sont les suivantes :

- Désactivez le pare-feu Windows.
- Joignez le contrôleur de domaine (AD DC) au service Active Directory.
- Assurez-vous que la machine virtuelle Azure dispose d'un accès à Internet.
- Ajoutez la fonctionnalité Active Directory.
- Déployer au moins un contrôleur de domaine sur le site DR dans Azure

  Les ressources restaurées doivent s'authentifier, appliquer des stratégies de groupe et résoudre des noms. Il convient de déployer une machine virtuelle Azure supplémentaire de contrôleur de domaine à l'avance, avant le basculement.
- Utiliser un contrôleur de domaine répliqué (non en lecture seule)

  Les contrôleurs de domaine en lecture seule (RODC) peuvent ne pas prendre en charge tous les scénarios d'authentification après un basculement. Déployer un contrôleur de domaine inscriptible et le répliquer avec votre forêt AD sur site.
- Assurez-vous que la configuration DNS est correcte

  Les machines virtuelles restaurées doivent résoudre les noms de domaine et localiser les contrôleurs de domaine. Configurez le réseau virtuel de restauration pour utiliser l'adresse IP du ou des contrôleurs de domaine basés sur Azure comme serveur DNS personnalisé.
- Répliquer SYSVOL et assurer la synchronisation de l'heure

© Acronis International GmbH, 2003-2026

Les stratégies de groupe et les opérations de domaine reposent sur la réplication SYSVOL et une heure correcte. Assurez-vous que SYSVOL est synchronisé et configurez les paramètres NTP ou de synchronisation de l'heure pour garantir la cohérence entre Azure et les environnements sur site.

Configuration du réseau de restauration de test

Pour garantir qu'un basculement test n'interfère pas avec les opérations de production, configurez un réseau virtuel (VNet) isolé dans Azure à des fins de test. Vérifiez que le VNet de test ne comporte aucune connexion de routage ni d'appairage réseau avec le VNet de production. Testez la connectivité à partir d'une machine virtuelle dans le VNet de test pour vous assurer qu'elle ne peut pas accéder aux ressources de production.

Ajout d'un réseau de restauration de production à partir de Microsoft Azure

Après la configuration du site DR, vous pouvez ajouter des réseaux de restauration de production supplémentaires à partir de ceux qui existent dans Microsoft Azure.

Pour ajouter un réseau de production de restauration à partir de Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Dans le volet **Réseaux de production**, cliquez sur **Ajouter un réseau**.
3. Dans la fenêtre **Ajouter un réseau de production**, dans le champ **Réseau virtuel**, sélectionnez un réseau virtuel.
4. Dans le champ **Sous-réseau**, sélectionnez le sous-réseau.
5. [Facultatif] Pour définir ce sous-réseau par défaut, sélectionnez **Définir ce sous-réseau comme « Par défaut » pour le mappage**.
   Lorsque vous appliquez le plan de protection de reprise d'activité après sinistre aux terminaux d'origine, les serveurs de restauration sont configurés dans le sous-réseau par défaut.
6. Dans le champ **Mappage sur le réseau local**, cliquez sur **Ajouter**.
   Vous pouvez définir des règles de mappage en entrant un ou plusieurs réseaux locaux source au format CIDR. Le service comparera ensuite l'adresse IP du terminal d'origine aux règles de mappage. Si l'adresse IP correspond à l'un des réseaux locaux source spécifiés, le serveur de restauration sera créé dans le réseau et le sous-réseau de restauration Azure correspondants.
7. Saisissez un ou plusieurs réseaux locaux source au format CIDR.
8. Pour ajouter le réseau, cliquez sur **Terminé**.

Ajout d'un réseau de restauration de test à partir de Microsoft Azure

Après la configuration du site DR, vous pouvez ajouter des réseaux de restauration test supplémentaires à partir de ceux qui existent dans Microsoft Azure.

Pour ajouter un réseau de restauration de test à partir de Microsoft Azure

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Connectivité**.
2. Dans le volet **Réseaux de test**, cliquez sur **Ajouter un réseau**.
3. Dans la fenêtre **Ajouter un réseau de test**, dans le champ **Réseau virtuel**, sélectionnez un réseau virtuel.
4. Dans le champ **Sous-réseau**, sélectionnez le sous-réseau.
5. [Facultatif] Pour définir ce sous-réseau par défaut, sélectionnez **Définir ce sous-réseau comme « Par défaut » pour le mappage**.
   Lorsque vous appliquez le plan de protection de reprise d'activité après sinistre aux terminaux d'origine, les serveurs de restauration sont configurés dans le sous-réseau par défaut.
6. Dans le champ **Mappage sur le réseau local**, cliquez sur **Ajouter**.
   Vous pouvez définir des règles de mappage en entrant un ou plusieurs réseaux locaux source au format CIDR. Le service comparera ensuite l'adresse IP du terminal d'origine aux règles de mappage. Si l'adresse IP correspond à l'un des réseaux locaux source spécifiés, le serveur de restauration sera créé dans le réseau et le sous-réseau de restauration Azure correspondants.
7. Saisissez un ou plusieurs réseaux locaux source au format CIDR.
8. Pour ajouter le réseau, cliquez sur **Terminé**.

Serveurs de restauration dans Microsoft Azure

Un serveur de restauration est une réplica de l'ordinateur d'origine qui est créée à partir de la sauvegarde (point de restauration) du serveur protégé qui est stockée dans le cloud - Cyber Protect Cloud ou Microsoft Azure. En cas de sinistre, la ressource est basculée du serveur d'origine vers le serveur de restauration dans Microsoft Azure.

Les serveurs de restauration sont créés manuellement ou automatiquement, lorsque vous appliquez un plan de protection de reprise d'activité après sinistre à une ressource.

Aucun point de calcul n'est facturé pour l'exécution de vos serveurs de restauration dans Microsoft Azure. Toute utilisation de calcul est facturée directement à votre abonnement Microsoft Azure.

La configuration de l'adresse MAC pour les serveurs de restauration n'est pas disponible dans Disaster Recovery vers Microsoft Azure.

Gestion des serveurs de restauration

Les opérations suivantes avec les serveurs de restauration sont disponibles dans Disaster Recovery pour Microsoft Azure :

Opération	Description
Mettre sous tension	[Pour les serveurs en état de basculement] Allumez la machine virtuelle Azure (serveur de restauration).
Mise hors tension	[Pour les serveurs dans l'état de basculement] Éteindre la machine virtuelle Azure (serveur de restauration).

© Acronis International GmbH, 2003-2026

Opération	Description
	L'opération d'arrêt arrête la machine virtuelle Azure, mais ne désalloue pas les ressources. La machine virtuelle sera dans l'état Arrêtée (Allocuée). Dans cet état, une machine virtuelle Azure continue de réserver le processeur et la mémoire, entraînant des frais de calcul comme si elle était en cours d'exécution. Cet état préserve l'adresse IP et le placement du serveur de la machine virtuelle.
Arrêt forcé	[Pour les serveurs en état de basculement] Éteindre de force le serveur de restauration.
Modifier les paramètres	Modifiez les paramètres du serveur de restauration, tels que les configurations de mise en réseau ou les seuils de l'objectif de point de restauration (RPO), dans la console Cyber Protect.
Basculement de la production	Basculez les ressources vers le serveur de restauration dans le réseau de production.
Basculement test	Testez le serveur de restauration dans le réseau de test isolé sans impact sur la production. Pour éviter les conflits lors du basculement, assurez-vous que les réseaux de production et de test sont configurés correctement. Les opérations de basculement test doivent être réalisées régulièrement pour valider la fonctionnalité du serveur de restauration.
Se connecter (à la console)	[Pour les serveurs en état de basculement] Après avoir cliqué sur **Connexion** et avoir été redirigé vers Azure, vous pouvez vous connecter à la machine virtuelle Azure en utilisant les options Azure natives, telles que : • Affectation d'une adresse IP publique et connexion via le protocole de bureau à distance (RDP) ou SSH. • Utilisation d'Azure Bastion, un service sécurisé pour se connecter à la machine virtuelle sans adresse IP publique.

Création de serveurs de restauration dans Microsoft Azure

Les serveurs de restauration sont créés automatiquement lorsque vous appliquez un plan de protection de reprise d'activité après sinistre à une ressource. Si aucun plan de protection de reprise d'activité après sinistre n'est appliqué à la ressource, vous pouvez créer un serveur de restauration manuellement.

Prérequis

- Un plan de sauvegarde est appliqué à la ressource.
- Le site DR dans Microsoft Azure est configuré.

Pour créer un serveur de restauration dans Microsoft Azure

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource que vous souhaitez protéger avec Disaster Recovery, puis, dans le menu **Actions**, cliquez sur **Reprise d'activité après sinistre**.
3. Cliquez sur **Créer un serveur de restauration**.
4. Dans l'assistant **Créer un serveur de restauration**, dans l'onglet **Configuration du serveur**, configurez les paramètres, puis cliquez sur **Suivant**.

Paramètre	Description
CPU et RAM	Taille de la machine virtuelle Azure. L'utilisation de l'ordinateur est facturée directement à votre abonnement Microsoft Azure par Microsoft ou votre partenaire. Si certaines tailles de machines virtuelles Azure ne sont pas disponibles, vérifiez les limitations de votre abonnement Azure. Les types de machine virtuelle Azure suivants sont exclus de la sélection : • Série A (dépréciée dans Microsoft Azure) • Types de machines virtuelles basés sur l'architecture de processeur ARM Les paramètres par défaut sont automatiquement déterminés en fonction de la configuration d'origine du processeur et de la RAM du terminal. La RAM est arrondie à la taille de machine virtuelle de la famille B la plus proche qui est égale ou supérieure à la valeur de RAM d'origine, et le nombre de cœurs de processeur le plus bas disponible qui satisfait l'exigence de RAM est sélectionné. Si les données de RAM de l'ordinateur d'origine ne sont pas disponibles (par exemple, pour les machines virtuelles Azure qui utilisent des sauvegardes sans agent), une taille minimale de machine virtuelle de la famille B est sélectionnée par défaut. Si la série ou la taille de machine virtuelle sélectionnée n'est pas disponible dans la région ou l'abonnement cible, le système sélectionne automatiquement la taille disponible la plus proche de n'importe quelle série de la famille B dans cette région.
Type de disque	Type de disque de la machine virtuelle Azure. Le type de disque que vous sélectionnez sera appliqué à tous les disques du serveur de restauration. Seuls les types de disque de stockage à redondance locale (LRS) sont disponibles pour la sélection. Premium SSD v2 et Ultra SSD ne sont pas disponibles pour la sélection. Le SSD Premium v2 est automatiquement affecté lors d'un basculement, si des disques à secteur 4K sont détectés dans la sauvegarde de la ressource d'origine.
Nom	Nom du serveur de restauration visible dans la console Cyber Protect. Ce nom n'est pas utilisé pour la machine virtuelle Azure.
Description	Description du serveur de restauration

5. Dans l'onglet **Réseau**, configurez les paramètres du réseau de production et du réseau de test, puis cliquez sur **Suivant**.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Réseau	(Pour le réseau de production) Le réseau virtuel Azure (VNet) et le sous-réseau pour le basculement de production. Lors d'un basculement de production, le serveur sera connecté à ce réseau Azure.
Adresse IP en réseau de production	(Pour le réseau de production) Par défaut, le dernier octet de l'adresse IP de l'ordinateur d'origine est dérivé à partir de la plage du réseau de production, mais vous pouvez modifier l'adresse IP à tout moment avant le basculement. Lorsque le serveur est en état de basculement, vous pouvez modifier l'adresse IP directement dans Azure.
Réseau	(Pour le réseau de test) Le VNet Azure et le sous-réseau pour le basculement test. Nous recommandons que le réseau de test soit isolé dans un VNet séparé. Pendant un basculement test, le serveur sera connecté à ce réseau Azure.
Adresse IP en réseau de test	(Pour le réseau de test) Par défaut, le dernier octet de l'adresse IP de la machine d'origine est dérivé dans la plage du réseau de test, mais vous pouvez modifier l'adresse IP à tout moment avant le basculement. Lorsque le serveur est dans l'état de test de basculement, vous pouvez modifier l'adresse IP directement dans Azure.

Remarque

- Par défaut, aucune adresse IP publique n'est affectée au serveur de restauration, pour des raisons de sécurité. Sans adresse IP publique, le serveur de restauration n'est accessible que depuis le réseau local. Si nécessaire, affectez une adresse IP publique directement dans le portail Azure.
- Par défaut, l'accès à Internet est activé pour les ressources dans Azure. Aucune configuration supplémentaire n'est nécessaire pour autoriser le trafic Internet sortant. Si vous devez restreindre ou isoler l'accès Internet sortant dans un réseau de test, vous devez configurer les contrôles de sécurité appropriés, tels que des règles de groupe de sécurité réseau (NSG), des itinéraires définis par l'utilisateur (UDR) ou des stratégies de pare-feu Azure, selon vos besoins.

6. Dans l'onglet **Basculement test automatisé**, procédez comme suit :
   a. [Facultatif] Activez l'interrupteur **Basculement test automatisé**.
   b. [Facultatif] Configurez les paramètres.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Planification	Le basculement test automatisé s'exécute une fois par mois.
Délai de démarrage de la machine virtuelle / Minutes	Définit la durée maximale pendant laquelle le système tente de démarrer une machine virtuelle dans Azure et de prendre des captures d'écran pour vérifier si le système d'exploitation a été chargé avec succès. Cette durée avant expiration n'inclut pas le temps passé à restaurer les données à partir d'une archive de sauvegarde à froid, car cette durée dépend de la taille de l'archive. Par ailleurs, les heures de calcul des machines virtuelles Azure ne sont pas comptabilisées pendant le temps de restauration des données.
Utiliser comme délai d'attente par défaut	Sélectionnez cette case à cocher si vous souhaitez utiliser la valeur **Délai de démarrage de la machine virtuelle / Minutes** comme valeur par défaut. Dans ce cas, cette valeur sera automatiquement renseignée lorsque vous activerez le basculement test automatisé pour d'autres serveurs de restauration.

c. Cliquez sur **Suivant**.

7. Dans l'onglet **Paramètres**, procédez comme suit :
   a. [Facultatif] Le seuil de l'objectif de point de restauration (RPO) définit l'intervalle de temps maximal autorisé entre le dernier point de restauration et l'heure actuelle. Vous pouvez définir une valeur comprise entre 15 et 60 minutes, 1 et 24 heures, ou 1 et 14 jours.
   b. [Facultatif] [Si les sauvegardes pour l'ordinateur sélectionné sont chiffrées à l'aide du chiffrement comme propriété de l'ordinateur] Spécifiez le mot de passe qui sera utilisé automatiquement lors de la création d'une machine virtuelle pour le serveur de restauration à partir de la sauvegarde chiffrée.
      a. Cliquez sur **Saisir le mot de passe**, puis saisissez le mot de passe de la sauvegarde chiffrée et définissez un nom pour les identifiants.
         Par défaut, la liste affiche la sauvegarde la plus récente.
      b. Pour afficher toutes les sauvegardes, sélectionnez **Afficher toutes les sauvegardes**.
      c. Cliquez sur **Enregistrer**.

      Remarque
      Le mot de passe que vous spécifiez sera stocké dans un magasin d'identifiants sécurisé, mais l'enregistrement des mots de passe peut être contraire à vos obligations de conformité.

8. Cliquez sur **Créer**.

Le serveur de restauration est créé et se trouve en état En attente. Aucun point de calcul n'est facturé. Toute utilisation de calcul est facturée directement à votre abonnement Azure.

© Acronis International GmbH, 2003-2026

Remarque
Vous pouvez configurer des règles de pare-feu pour la machine virtuelle uniquement dans le portail Azure. Par défaut, pour les machines virtuelles dans le basculement de test et de production, toutes les connexions entrantes sont interdites et toutes les connexions sortantes vers Internet sont autorisées au sein du réseau virtuel de production et de test.

Modification des paramètres du serveur de restauration

Lorsque vous créez et appliquez un plan de protection de reprise d'activité après sinistre, un serveur de restauration est créé avec les paramètres par défaut. Vous pouvez modifier ces paramètres par défaut si nécessaire.

Pour modifier les paramètres d'un serveur de restauration dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs de restauration**.
2. Cliquez sur le serveur dont vous souhaitez modifier les paramètres, puis cliquez sur **Modifier**.
3. Modifier les paramètres du serveur de restauration.
4. Cliquez sur **Enregistrer**.

Suppression d'un serveur de restauration

Vous pouvez supprimer les serveurs de restauration que vous avez créés dans Microsoft Azure.

Pour supprimer un serveur de restauration dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs de restauration**.
2. Cliquez sur le serveur que vous souhaitez supprimer, puis cliquez sur <**Supprimer**.
3. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Basculement dans Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Basculement de la production

Le basculement est le processus qui transfère la ressource du serveur d'origine sur votre site local vers le serveur de restauration.

Lorsqu'un serveur de restauration est créé, il reste en mode **En attente**. La machine virtuelle correspondante n'existe pas dans Microsoft Azure tant que vous n'avez pas démarré un basculement. Avant de démarrer un basculement, vous devez créer au moins une sauvegarde d'image de disque (avec volume amorçable) de la machine d'origine.

© Acronis International GmbH, 2003-2026

Lors du démarrage du basculement, vous sélectionnez le point de restauration (sauvegarde) de la machine d'origine à partir duquel une machine virtuelle avec les paramètres prédéfinis sera créée dans Microsoft Azure.

Lorsque le basculement est terminé, l'état du serveur de restauration change en **Basculement**. La ressource est maintenant basculée de la machine d'origine vers le serveur de restauration dans Microsoft Azure.

Si le serveur de restauration dispose d'un agent de protection, pour éviter les interférences (comme le démarrage d'une sauvegarde ou le rapport de statuts obsolètes au composant de sauvegarde), le service de l'agent est arrêté.

Basculement test

Le basculement test est un processus de création d'une machine virtuelle temporaire dans un réseau virtuel Azure (VNet) isolé et de test des procédures de restauration, des configurations et de la fonctionnalité des applications. Pour plus d'informations, voir "Basculement test dans Microsoft Azure" (p. 1133).

Basculement test automatisé

Le basculement test automatisé dans Microsoft Azure valide l'intégrité de la sauvegarde en démarrant une machine virtuelle de serveur de restauration à partir de la dernière sauvegarde et en effectuant une capture d'écran pour confirmer que le système d'exploitation a démarré avec succès. Si elle est activée, la fonction du basculement test automatisé est lancée une fois par mois. Pour plus d'informations, voir "Basculement test automatisé dans Microsoft Azure" (p. 1136).

Gestion des conflits d'adresse IP dans le basculement

Si l'adresse IP configurée dans le réseau de production est déjà utilisée au moment du basculement de production, une autre adresse IP disponible du même réseau sera affectée automatiquement.

Si l'adresse IP du réseau de test configurée est déjà utilisée au moment du basculement test, une autre adresse IP disponible du réseau de test sera affectée.

Restauration de serveur de restauration en basculement vers un moment donné précédent

Pour restaurer un serveur en basculement, initiez un nouveau basculement à partir d'un autre point de restauration pour restaurer les opérations.

Widgets de basculement

Pendant le basculement de production et de test, vous pouvez voir des informations sur les performances de basculement (vitesse de restauration) et les goulets d'étranglement dans l'onglet **Activités** des détails du serveur de restauration. Pour afficher le widget **Goulet d'étranglement**, développez l'activité **Création de la machine virtuelle**, puis dans la sous-activité **Copie des**

© Acronis International GmbH, 2003-2026

données de la sauvegarde vers les disques de la machine virtuelle, développez **Goulet d'étranglement**.

Exécution d'un basculement de production dans Microsoft Azure

Lorsque vous effectuez un basculement de production, la ressource est transférée de l'ordinateur d'origine vers le serveur de restauration dans Microsoft Azure.

Pour effectuer un basculement de production dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs de restauration**.
2. Cliquez sur le serveur sur lequel vous souhaitez effectuer un basculement, puis cliquez sur **Basculement**.
3. Dans la fenêtre **Basculement de serveur**, sélectionnez **Basculement de la production**, puis sélectionnez le point de restauration (sauvegarde) à partir duquel le serveur cloud sera démarré.
4. Cliquez sur **Démarrer**.

Lorsque le basculement est terminé, le service commence à s'exécuter sur la machine virtuelle dans Azure. En cliquant sur **Connexion**, vous serez redirigé vers la machine virtuelle dans Azure.

Basculement test dans Microsoft Azure

Le basculement test est un élément essentiel de la stratégie Disaster Recovery as a Service (DRaaS) dans Microsoft Azure. Il permet aux organisations de valider les processus de restauration sans affecter les environnements de production. Cela se fait en simulant la restauration d'une machine virtuelle (VM) à partir d'un point de restauration (sauvegarde) sélectionné. Le processus crée une VM temporaire dans un réseau virtuel Azure (VNet) isolé afin de tester les procédures de restauration, les configurations et le bon fonctionnement des applications. Bien qu'ils soient facultatifs, les basculements test réguliers sont fortement recommandés pour garantir des processus de restauration fiables et à jour. Vous pouvez établir une planification des tests en fonction des exigences de coût et de fiabilité de votre organisation.

Vous pouvez tester plusieurs serveurs de restauration simultanément et vérifier leur interaction. Dans le réseau de test, les serveurs communiquent en utilisant leurs adresses IP de production, mais ils ne peuvent pas initier de connexions TCP ou UDP vers les ressources de votre réseau local.

Réseau de test de restauration

Pour garantir qu'un basculement test n'interfère pas avec les opérations de production, configurez un réseau virtuel isolé (VNet) dans Azure à des fins de test. Confirmez que le VNet de test n'a pas de connexions de routage ou de mise en réseau avec le VNet de production. Testez la connectivité d'un ordinateur virtuel dans le VNet de test pour vous assurer qu'il ne peut pas accéder aux ressources de production.

Processus de basculement test

Le processus de basculement test se compose des phases suivantes.

Initialisation

© Acronis International GmbH, 2003-2026

Au cours de cette phase, vous sélectionnez un point de restauration et lancez le basculement test.

Déploiement d'un worker temporaire

Au cours de cette phase, un worker utilisé pour l'opération de basculement test est déployé automatiquement. Le déploiement initial du worker pour un basculement test ou de production peut prendre plusieurs minutes. Le démarrage des workers pour les basculements suivants devrait être plus rapide.

Restauration de données

Au cours de cette phase, les données sont copiées depuis le stockage des sauvegardes vers un conteneur temporaire de stockage Azure Blob. Le temps nécessaire pour copier ou restaurer les données dépend de la taille de la ressource. Une fois les données copiées, le contenu du stockage Azure Blob est converti en disque géré, qui est ensuite utilisé pour démarrer la machine virtuelle temporaire.

Création de machine virtuelle de restauration

La machine virtuelle de restauration est connectée au réseau virtuel Azure isolé préconfiguré ainsi qu'au sous-réseau. Par défaut, la machine virtuelle se voit affecter une adresse IP dont le dernier octet correspond à celui de l'ordinateur d'origine. Vous pouvez modifier l'adresse IP avant le basculement test dans les paramètres du serveur de restauration. Pendant le basculement test, vous pouvez le faire directement dans le portail Azure.

Assurez-vous que le VNet est isolé du réseau de production pour éviter les interactions non intentionnelles.

Vérification

Après la création de la machine virtuelle, le fait de cliquer sur le bouton **Connexion** vous redirigera vers la machine virtuelle spécifique dans le portail Azure.

Effectuez tous les tests nécessaires pour vérifier le comportement de l'application, la connectivité et les objectifs de restauration dans l'environnement isolé.

Le basculement test ne remplace pas les points de restauration existants, garantissant ainsi que vos sauvegardes restent intactes.

Arrêt du basculement test

L'arrêt du basculement test supprime la machine virtuelle temporaire, les ressources associées ainsi que l'agent. Si un mot de passe de chiffrement a été utilisé, il est automatiquement supprimé du magasin d'identifiants lors de l'arrêt ou de l'achèvement du basculement test.

Vous pouvez arrêter le basculement test à tout moment depuis le portail Azure.

Exécution d'un basculement test dans Microsoft Azure

Bien que le basculement test soit facultatif, nous vous recommandons d'en exécuter régulièrement, à une fréquence adéquate pour vous en matière de coût et de fiabilité.

© Acronis International GmbH, 2003-2026

Important
Vous ne pouvez effectuer un basculement que depuis des points de restauration créés après la création du serveur de restauration du terminal.

Vous devez créer au moins un point de restauration avant de basculer vers un serveur de restauration. Le nombre maximal de points de restauration pris en charge est de 100.

Prérequis

- Le serveur de restauration est configuré dans un emplacement Azure et a au moins un point de restauration créé après la création du serveur de restauration.
- Un VNet Azure isolé et un sous-réseau pour le basculement test afin d'assurer qu'il n'y a pas d'interférence avec les environnements de production.
- Les règles du groupe de sécurité réseau (NSG) sont configurées pour répondre à vos exigences.

Pour effectuer un basculement test dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs de restauration**.
2. Cliquez sur le serveur sur lequel vous souhaitez effectuer un basculement, puis cliquez sur **Basculement**.
3. Dans la fenêtre **Basculement du serveur**, sélectionnez **Basculement test**, puis sélectionnez le point de restauration (sauvegarde) à partir duquel le serveur cloud sera démarré.
4. Cliquez sur **Démarrer**.
5. Si la sauvegarde sélectionnée est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur :
   a. Saisissez le mot de passe de chiffrement pour l'ensemble de sauvegardes.

      Remarque
      Le mot de passe ne sera enregistré que temporairement et utilisé uniquement pour le basculement test en cours. Le mot de passe est supprimé automatiquement du magasin des identifiants si le basculement test est arrêté ou une fois que le basculement test est terminé.

   b. [Facultatif] Pour enregistrer le mot de passe de l'ensemble de sauvegardes et l'utiliser dans les opérations de basculement ultérieures, cochez la case **Stocker le mot de passe dans un magasin d'identifiants sécurisé** et saisissez un nom pour les identifiants dans le champ **Nom des identifiants**.

      Important
      Le mot de passe sera stocké dans un magasin d'identifiants sécurisé et sera appliqué automatiquement dans les opérations de basculement ultérieures. Toutefois, l'enregistrement des mots de passe peut entrer en conflit avec vos obligations de conformité.

   c. Cliquez sur **Terminé**.

   Quand le serveur de restauration démarre, son état est modifié en **Test de basculement**.

© Acronis International GmbH, 2003-2026

6. Testez le serveur de restauration à l'aide de l'une des méthodes suivantes :
   - Dans **Disaster Recovery** > **Serveurs de restauration**, sélectionnez le serveur de restauration, puis cliquez sur **Connexion**.
   - Connectez-vous au serveur de restauration via RDP ou SSH, à l'aide de l'adresse IP de test que vous avez indiquée lors de la création du serveur de restauration. Testez la connexion depuis l'intérieur et l'extérieur du réseau de production (comme décrit dans « Connexion de point à site »).
   - Exécutez un script au sein du serveur de restauration.

     Le script peut vérifier l'écran de connexion, le démarrage des applications, la connexion Internet, et la capacité d'autres machines à se connecter au serveur de restauration.
7. Une fois le test terminé, cliquez sur **Arrêter le test**.

   Le serveur de restauration est arrêté. Les modifications apportées au serveur de restauration lors du basculement test ne sont pas enregistrées.

Basculement test automatisé dans Microsoft Azure

Le basculement test automatisé dans Microsoft Azure valide l'intégrité de la sauvegarde en démarrant une machine virtuelle de serveur de restauration à partir de la dernière sauvegarde et en capturant une capture d'écran pour confirmer que le système d'exploitation a démarré avec succès.

Avec le basculement test automatisé, le serveur de restauration est testé automatiquement une fois par mois, sans aucune interaction manuelle.

Le processus de basculement test automatisé se compose des étapes suivantes :

1. Création d'une machine virtuelle dans Microsoft Azure à partir du dernier point de restauration.
2. Capture d'écran de la machine virtuelle.
3. Analyse pour déterminer si le système d'exploitation de la machine virtuelle démarre correctement.
4. Envoi d'une notification pour vous informer du statut du basculement test.

Remarque
Le basculement test automatisé consomme des heures de calcul de machine virtuelle Azure.

Vous pouvez configurer le basculement test automatisé dans les paramètres du serveur de restauration. Pour plus d'informations, voir "Configuration du basculement test automatisé dans Microsoft Azure" (p. 1137).

Si le basculement test automatisé est ignoré, quelle qu'en soit la raison, une alerte est générée.

© Acronis International GmbH, 2003-2026

Remarque
Le basculement test automatisé échoue si les sauvegardes de l'ordinateur original sont chiffrées à l'aide du chiffrement comme propriété de l'ordinateur, et que le mot de passe de chiffrement n'est pas spécifié lors de la création du serveur de restauration. Pour plus d'informations sur la spécification du mot de passe de chiffrement, voir "Création de serveurs de restauration dans Microsoft Azure" (p. 1127).

Configuration du basculement test automatisé dans Microsoft Azure

En configurant le basculement test automatisé, vous pouvez tester votre serveur de restauration tous les mois, sans aucune intervention manuelle.

Pour configurer le basculement test automatisé d'un serveur de restauration dans Microsoft Azure

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Tableau de bord**.
2. Dans le widget **Basculement test automatisé**, cliquez sur **Configurer**.
3. Dans la boîte de dialogue **Configuration du basculement test automatisé**, sélectionnez un ou plusieurs serveurs de restauration pour lesquels vous souhaitez configurer le basculement test automatisé, puis cliquez sur **Suivant**.
4. Activez l'interrupteur **Basculement test automatisé**.
5. Dans le champ **Planification**, sélectionnez **Mensuel**.
6. [Facultatif] Dans **Délai de démarrage de la machine virtuelle / Minutes**, modifiez la valeur par défaut de la période maximale pendant laquelle le système tente de démarrer la machine virtuelle dans Azure, puis prenez une capture d'écran pour vérifier si le système d'exploitation a été chargé avec succès.

   Remarque
   - Ce délai d'attente ne comprend pas le temps nécessaire pour restaurer des données à partir d'une archive de sauvegarde à froid. Le chronomètre démarre lorsque la machine virtuelle commence à démarrer.
   - Lors de la restauration de données froides, Azure crée temporairement un stockage Blob standard, qui est ensuite converti en disque géré pour la machine virtuelle.
   - Les heures de calcul de la machine virtuelle Azure ne sont pas comptabilisées pendant le processus de restauration des données.

7. [Facultatif] Pour enregistrer la valeur **Délai de démarrage de la machine virtuelle / Minutes** comme valeur par défaut et qu'elle soit renseignée automatiquement lorsque vous activez le basculement test automatisé pour les autres serveurs de restauration, sélectionnez **Définir comme délai d'attente par défaut**.
8. Cliquez sur **Configurer**.

© Acronis International GmbH, 2003-2026

Dans l'onglet **Serveurs de restauration**, vous pouvez voir que le basculement test automatisé a commencé. Une fois terminé, la machine virtuelle sera supprimée et vous pourrez trouver le lien vers la capture d'écran du système d'exploitation validé dans les détails du serveur de restauration.

Affichage du statut du basculement test automatisé

Vous pouvez afficher les détails d'un basculement test automatisé effectué sur un serveur de restauration dans Microsoft Azure, tels que le statut, l'heure de début, l'heure de fin, la durée et la capture d'écran de la machine virtuelle.

Remarque
L'instantané de la machine virtuelle est conservée jusqu'à ce que le basculement test automatisé soit réexécuté et génère un nouvel instantané.

Pour voir le statut du basculement test automatisé d'un serveur de restauration dans Microsoft Azure

1. Dans la console, accédez à **Disaster Recovery** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Dans la section **Basculement test automatisé**, vérifiez les détails du dernier basculement test automatisé.
3. [Facultatif] Pour afficher l'instantané de la machine virtuelle, cliquez sur **Afficher l'instantané**.

Désactivation du basculement test automatisé

Vous pouvez désactiver le basculement test automatisé si vous souhaitez économiser des ressources ou si vous n'avez pas besoin d'effectuer un basculement test automatisé pour un serveur de restauration donné dans Microsoft Azure.

Pour désactiver le basculement test automatisé pour un serveur de restauration dans Microsoft Azure

1. Dans la console, accédez à **Disaster Recovery** > **Serveurs de restauration**, puis sélectionnez le serveur de restauration.
2. Cliquez sur **Modifier**.
3. Dans l'assistant, cliquez sur l'onglet **Basculement test automatisé**.
4. Désactivez l'interrupteur **Basculement test automatisé**.
5. Cliquez sur **Enregistrer**.

Exigences et limitations pour le basculement de machines virtuelles Linux vers Microsoft Azure

Cette section décrit les exigences et les limitations clés pour le basculement de ressources Linux vers Microsoft Azure, en particulier dans les environnements sans accès Internet.

© Acronis International GmbH, 2003-2026

Configuration requise

Installation de l'agent de machine virtuelle Azure avec accès Internet

L'agent de machine virtuelle Azure est installé automatiquement lors du basculement test et de production.

Les outils Linux requis (par exemple, **cloud-init**, pilotes de mise en réseau) sont récupérés à partir de référentiels publics (par exemple, `archive.ubuntu.com` ou `mirror.centos.org`).

Pour des raisons de sécurité, vous pouvez autoriser les https sortants uniquement vers des référentiels spécifiques.

Installation de l'agent de machine virtuelle Azure sans accès Internet

Vous devez installer manuellement l'agent de machine virtuelle Azure sur la machine Linux source avant le basculement.

Sans l'agent, le basculement peut échouer ou entraîner une fonctionnalité limitée de la machine virtuelle.

Limites

Dépendance Internet

L'absence d'accès Internet sur la machine virtuelle Azure cible nécessitera qu'un agent Azure soit préinstallé sur la ressource d'origine, ce qui ajoute une surcharge de configuration.

L'absence d'accès à Internet peut empêcher la mise à jour après le basculement (par exemple, des outils de mise en réseau ou de sauvegarde).

Recommandations

- Autoriser l'accès Internet pour le VNet de production et de test avant un basculement. Il s'agit d'une configuration par défaut.
- Restreindre l'accès sortant à des référentiels Linux spécifiques si vous les connaissez avant un basculement.
- Restreindre l'accès à des services de production spécifiques lors des basculements test.
- Vous pouvez utiliser des miroirs internes ou un VPN pour minimiser la dépendance à Internet.
- Exécutez régulièrement des basculements test pour garantir la préparation de l'environnement.

Restauration automatique dans Microsoft Azure

Une restauration automatique est un processus consistant à déplacer la ressource du cloud vers une machine physique ou une machine virtuelle sur votre site local. Vous pouvez exécuter une restauration automatique sur un serveur de restauration dont l'état est **Basculement**, puis continuer à utiliser le serveur sur votre site local.

© Acronis International GmbH, 2003-2026

Vous pouvez exécuter un basculement automatique vers une machine cible virtuelle ou physique sur votre site local. Lors du processus de restauration automatique, vous pouvez transférer les données de sauvegarde vers votre site local tandis que la machine virtuelle dans le cloud continue à s'exécuter. Cette technologie vous permet de bénéficier d'une période d'interruption d'activité très courte, estimée et affichée dans la console Cyber Protect. Vous pouvez consulter cette information pour planifier vos activités et, si nécessaire, avertir vos clients d'une période d'interruption à venir. Si vous effectuez une restauration automatique avec agent à l'aide d'un support de démarrage, la période d'interruption est encore plus courte, car seules les données modifiées sont transférées vers le site local.

Pour effectuer une restauration automatique sur une machine physique cible, vous pouvez utiliser la restauration automatique avec agent via un support de démarrage. Pour plus d'informations, voir "Restauration automatique avec agent via un support de démarrage à partir de Microsoft Azure" (p. 1140).

Pour effectuer une restauration automatique sur une machine virtuelle cible, vous pouvez utiliser la restauration automatique avec agent via un support de démarrage ou la restauration automatique sans agent via l'agent d'hyperviseur. Pour plus d'informations, voir "Restauration automatique avec agent via un support de démarrage à partir de Microsoft Azure" (p. 1142) et "Restauration automatique sans agent via un agent d'hyperviseur à partir de Microsoft Azure" (p. 1146).

Dans les cas où vous ne pouvez pas utiliser la procédure de restauration automatique automatisée, vous pouvez effectuer une restauration automatique manuelle. Pour plus d'informations, voir "Restauration automatique manuelle à partir de Microsoft Azure" (p. 1150).

Remarque
Les opérations de runbook prennent en charge la restauration automatique en mode manuel uniquement. Cela signifie que si vous démarrez le processus de restauration automatique en exécutant un runbook qui inclut une étape **Serveur de restauration automatique**, la procédure nécessitera une interaction manuelle : vous devez restaurer l'ordinateur manuellement, et confirmer ou annuler le processus de restauration automatique à partir de l'onglet **Disaster Recovery** > **Serveurs**

Restauration automatique avec agent via un support de démarrage à partir de Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Le processus de restauration automatique avec agent via un support de démarrage est optimisé pour effectuer une restauration automatique vers la machine physique ou virtuelle d'origine. Pendant ce processus, seules les données modifiées sont transférées vers le site local.

Le processus de restauration automatique avec agent via un support de démarrage vers une machine virtuelle ou physique cible comprend les phases suivantes :

© Acronis International GmbH, 2003-2026

1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.
2. **Transfert de données**. Lors de cette phase, l'exécution de la machine virtuelle dans le Cloud est maintenue pendant que les données sont transférées du site dans le Cloud vers le site local. Vous pouvez démarrer la phase suivante, le basculement, à tout moment durant la phase de transfert de données, mais vous devriez tenir compte des relations suivantes.

   Plus vous restez longtemps dans la phase Transfert de données,
   - plus longtemps la machine virtuelle dans le cloud continue à s'exécuter ;
   - plus la quantité de données qui sera transférée à votre site local sera importante ;
   - plus cela vous coûtera cher (vous dépensez plus de points de calcul) ;
   - plus la période d'interruption d'activité lors de la phase de basculement sera courte.

   Si vous souhaitez réduire l'interruption d'activité au minimum, démarrez la phase de basculement une fois que 90 % au moins des données ont été transférés sur le site local.

   Si vous pouvez vous permettre une période d'interruption d'activité plus longue et que vous ne souhaitez pas dépenser plus de points de calcul pour l'exécution de la machine virtuelle dans le Cloud, vous pouvez démarrer la phase de basculement plus tôt.

   Remarque

   Le processus de transfert de données utilise une technologie de flashback. Cette technologie compare les données disponibles sur la machine cible aux données de la machine virtuelle dans le cloud. Si une partie des données est déjà disponible sur la machine cible, elles ne sont pas retransférées. Cette technologie accélère la phase de transfert de données.

   C'est la raison pour laquelle nous vous recommandons de restaurer le serveur sur la machine d'origine sur votre site local.
3. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données restantes, y compris le dernier incrément de sauvegarde, sont transférées sur le site local. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.
4. **Validation**. Lors de cette phase, l'ordinateur sur le site local est prêt et vous pouvez le redémarrer à l'aide d'un support de démarrage Linux. Vous pouvez vérifier que la machine virtuelle fonctionne correctement et :
   - Si tout fonctionne comme prévu, vous pouvez confirmer la restauration automatique. Après la confirmation de la restauration automatique, la machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**. Le processus de restauration automatique est alors terminé.
   - En cas d'anomalie, vous pouvez annuler le basculement et revenir à la phase de planification.

© Acronis International GmbH, 2003-2026

Remarque
Une fois que le support de démarrage a été redémarré, vous ne pourrez plus le réutiliser. Si vous détectez une anomalie au cours de la phase de validation, vous devez enregistrer un nouveau support de démarrage et redémarrer le processus de restauration automatique.
Toutefois, étant donné qu'une technologie de flashback est utilisée, les données figurant déjà sur le site local ne seront pas retransférées et le processus de restauration automatique sera accéléré.

Restauration automatique avec agent via un support de démarrage à partir de Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez effectuer une restauration automatique avec agent via un support de démarrage à partir de Microsoft Azure vers une machine cible physique ou une machine virtuelle sur votre site local.

Remarque
Le processus de transfert de données utilise une technologie de flashback. Cette technologie compare les données disponibles sur la machine cible aux données de la machine virtuelle dans le cloud. Si une partie des données est déjà disponible sur la machine cible, elles ne sont pas retransférées. Cette technologie accélère la phase de transfert de données.

C'est la raison pour laquelle nous vous recommandons de restaurer le serveur sur la machine d'origine sur votre site local.

Prérequis

- L'agent que vous allez utiliser pour exécuter une restauration automatique est en ligne et n'est pas actuellement utilisé pour une autre opération de restauration automatique.
- Votre connexion Internet est stable.
- Un support de démarrage enregistré est disponible.
  Pour plus d'informations, voir "Création d'un support de démarrage afin de restaurer des systèmes d'exploitation" (p. 989).
- La machine physique cible est la machine d'origine sur votre site local ou une machine dont le firmware est identique à celui de la machine d'origine.
- Il existe au moins une sauvegarde complète de la machine virtuelle dans le cloud.

Pour effectuer une restauration automatique vers une machine physique

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.

© Acronis International GmbH, 2003-2026

3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans le champ **Type de restauration automatique**, sélectionnez **Avec agent via un support de démarrage**.
5. Dans le champ **Support de démarrage cible**, cliquez sur **Spécifier**, sélectionnez le support de démarrage, puis cliquez sur **Terminé**.

Remarque
Nous vous recommandons d'utiliser un support de démarrage prêt à l'emploi, car il est déjà configuré. Pour plus d'informations, voir "Création d'un support de démarrage afin de restaurer des systèmes d'exploitation" (p. 989).

6. [Facultatif] Pour modifier le mappage de disque par défaut, cliquez dans le champ **Mappage de disque** sur **Spécifier**, mappez les disques de la sauvegarde vers les disques de la machine cible, puis cliquez sur **Terminé**.
7. Cliquez sur **Démarrer le transfert de données**, puis sur **Démarrer** dans la fenêtre de confirmation.

Remarque
S'il n'y a pas de sauvegarde de la machine virtuelle dans le cloud, le système effectuera une sauvegarde automatiquement avant la phase de transfert des données.

La phase transfert de données démarre. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre affiche la quantité de données déjà transférées vers le site local, ainsi que la quantité totale de données à transférer. La quantité totale de données comprend les données de la dernière sauvegarde avant le démarrage de la phase de transfert de données, ainsi que les sauvegardes des données nouvellement générées (incréments de sauvegarde), car la machine virtuelle continue à s'exécuter lors de la phase de transfert de données. C'est la raison pour laquelle les valeurs **Progression** augmentent au fil du temps. Étant donné que le système utilise une technologie de flashback pendant le transfert de données et ne transfère pas les données déjà disponibles sur la machine cible, la progression peut être plus rapide que dans le calcul initial effectué par la console.
Estimation de l'interruption d'activité	Ce paramètre indique la durée d'indisponibilité de la machine virtuelle dans le cloud si vous démarrez la phase de basculement maintenant. La valeur est calculée en fonction des valeurs du paramètre **Progression** et diminue au fil du temps. Étant donné que le système utilise une technologie de flashback pendant le transfert de données et ne transfère pas les données déjà disponibles sur la machine cible, l'interruption d'activité peut être plus courte que la valeur affichée initialement dans la console.

© Acronis International GmbH, 2003-2026

8. Cliquez sur **Basculement**, puis cliquez une nouvelle fois sur **Basculement** dans la fenêtre de confirmation.

   La phase de basculement commence. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre montre la progression de la restauration de la machine sur le site local.
Temps restant estimé	Ce paramètre indique l'heure approximative à laquelle la phase de basculement sera terminée et où vous pourrez démarrer la machine virtuelle sur le site local.

   Remarque
   Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

9. Une fois la phase de **basculement** terminée, redémarrez le support de démarrage, puis vérifiez que la machine physique sur votre site local fonctionne comme prévu.

   Pour plus d'informations, voir "Restauration de disques via un support de démarrage" (p. 704).

10. Cliquez sur **Confirmer la restauration automatique**, puis sur **Confirmer** dans la fenêtre de confirmation pour finaliser le processus.

    La machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

    Remarque
    Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

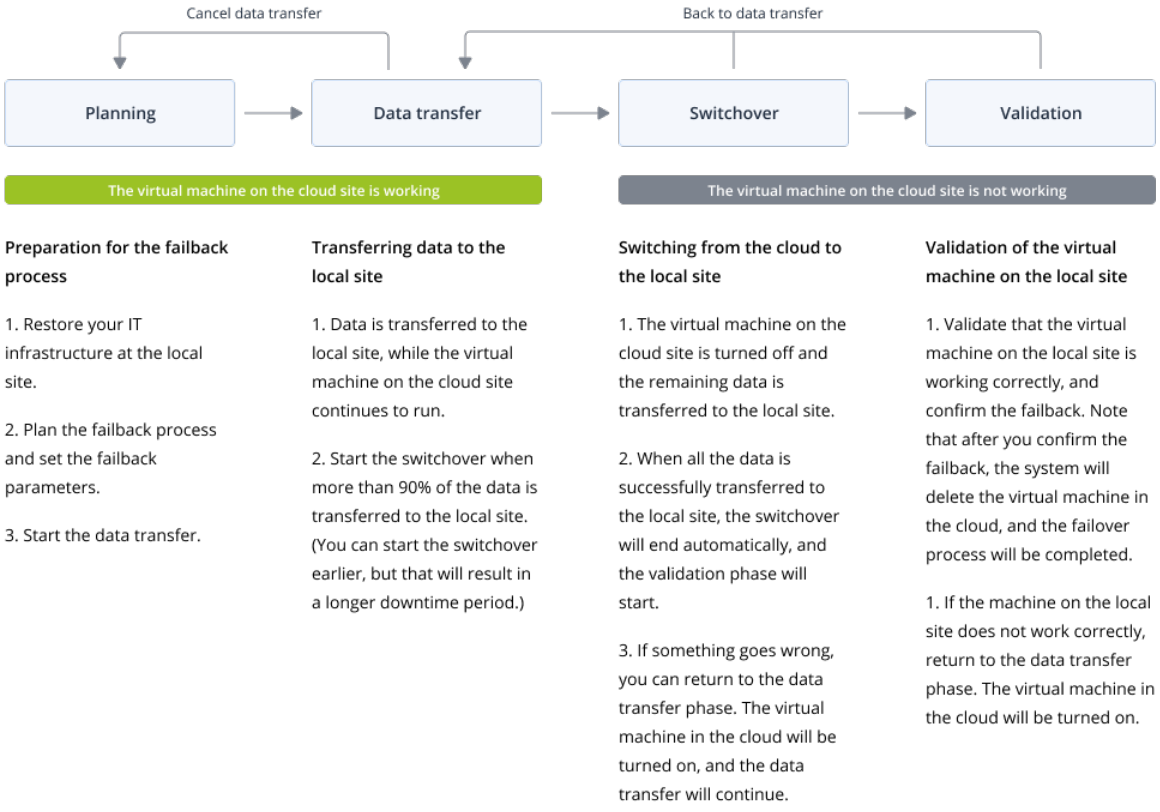
Restauration automatique sans agent via un agent d'hyperviseur à partir de Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La restauration automatique sans agent via un processus d'agent d'hyperviseur est optimisée pour effectuer une restauration automatique à partir de Microsoft Azure vers une nouvelle machine virtuelle. Si vous souhaitez effectuer une restauration automatique vers la machine virtuelle d'origine, suivez la procédure de restauration automatique avec agent via un support de démarrage.

La restauration automatique sans agent via un agent d'hyperviseur se déroule en quatre phases.

© Acronis International GmbH, 2003-2026



1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.

   Remarque
   Pour diminuer la durée totale du processus de restauration automatique, nous vous recommandons de démarrer la phase de transfert de données immédiatement après avoir configuré vos serveurs locaux, puis de poursuivre avec la configuration du réseau et le reste de l'infrastructure locale lors de la phase de transfert de données.

2. **Transfert de données**. Lors de cette phase, l'exécution de la machine virtuelle dans le Cloud est maintenue pendant que les données sont transférées du site dans le Cloud vers le site local. Vous pouvez démarrer la phase suivante, le basculement, à tout moment durant la phase de transfert de données, mais vous devriez tenir compte des relations suivantes.
   Plus vous restez longtemps dans la phase Transfert de données,
   - plus longtemps la machine virtuelle dans le cloud continue à s'exécuter ;
   - plus la quantité de données qui sera transférée à votre site local sera importante ;
   - plus cela vous coûtera cher (vous dépensez plus de points de calcul) ;
   - plus la période d'interruption d'activité lors de la phase de basculement sera courte.

© Acronis International GmbH, 2003-2026

Si vous souhaitez réduire l'interruption d'activité au minimum, démarrez la phase de basculement une fois que 90 % au moins des données ont été transférés sur le site local.

Si vous pouvez vous permettre une période d'interruption d'activité plus longue et que vous ne souhaitez pas dépenser plus de points de calcul pour l'exécution de la machine virtuelle dans le Cloud, vous pouvez démarrer la phase de basculement plus tôt.

Si vous annulez le processus de restauration automatique lors de la phase Transfert de données, les données transférées ne seront pas supprimées du site local. Pour éviter d'éventuels problèmes, supprimez manuellement les données transférées avant de lancer un nouveau processus de restauration automatique. Le processus de transfert de données suivant reprendra au début.

3. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données restantes, y compris le dernier incrément de sauvegarde, sont transférées sur le site local. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

   Vous pouvez consulter le temps estimé pour finir cette phase (période d'interruption d'activité) dans la console Cyber Protect. Lorsque toutes les données sont transférées sur le site local (il n'y a aucune perte de données et la machine virtuelle située sur le site local est une copie parfaite de la machine virtuelle dans le cloud), la phase de basculement est terminée. La machine virtuelle sur le site local est restaurée et la phase de validation démarre automatiquement.
4. **Validation**. Pendant cette phase, la machine virtuelle sur le site local est prête et démarre automatiquement. Vous pouvez vérifier si elle fonctionne correctement et :
   - Si tout fonctionne comme prévu, vous pouvez confirmer la restauration automatique. Après la confirmation de la restauration automatique, la machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**. Le processus de restauration automatique est alors terminé.
   - En cas d'anomalie, vous pouvez annuler le basculement et revenir à la phase de transfert de données.

Restauration automatique sans agent via un agent d'hyperviseur à partir de Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez effectuer une restauration automatique sans agent à partir de Microsoft Azure vers une machine virtuelle cible sur votre site local via un agent d'hyperviseur.

Prérequis

- L'agent que vous allez utiliser pour exécuter une restauration automatique est en ligne et n'est pas actuellement utilisé pour une autre opération de restauration automatique.
- Votre connexion Internet est stable.
- Il existe au moins une sauvegarde complète de la machine virtuelle dans le cloud.

© Acronis International GmbH, 2003-2026

Pour effectuer une restauration automatique sans agent vers une machine virtuelle via un agent d'hyperviseur

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans la section **Paramètres de restauration automatique**, sélectionnez dans le champ **Type de restauration automatique** l'option **Sans agent via l'agent d'hyperviseur**, puis configurez les autres paramètres.

   Certains **Paramètres de restauration** sont remplis automatiquement avec des valeurs suggérées, mais vous pouvez les modifier.

   Le tableau suivant fournit plus de détails sur les **paramètres de restauration automatique**.

Paramètre	Description
Taille de la sauvegarde	Quantité de données qui sera transférée à votre site local lors du processus de restauration automatique. Une fois que vous aurez lancé le processus de restauration automatique vers une machine virtuelle cible, la **Taille de la sauvegarde** augmentera lors de la phase de transfert de données, car la machine virtuelle dans le cloud continuera à s'exécuter et à générer de nouvelles données. Pour calculer l'interruption d'activité estimée qui surviendra lors du processus de restauration automatique vers une machine virtuelle cible, partez de 10 % de la **Taille de la sauvegarde** (puisque nous vous recommandons de démarrer la phase de basculement quand 90 % des données ont été transférés vers votre site local) et divisez cette valeur par celle de la vitesse de votre connexion Internet. **Remarque** La valeur de la vitesse de votre connexion Internet diminuera quand vous exécuterez simultanément plusieurs processus de restauration automatique.
Emplacement de machine cible	Emplacement de restauration automatique : hôte VMware ESXi ou Microsoft Hyper-V. Vous pouvez faire votre choix parmi tous les hôtes qui possèdent un agent enregistré avec le service de cyberprotection.
Agent	Agent qui exécutera l'opération de restauration automatique. Vous pouvez utiliser un agent pour effectuer une opération de restauration automatique à la fois. Vous pouvez sélectionner un agent qui est en ligne et qui n'est pas actuellement utilisé pour un autre processus de restauration automatique, qui possède une version compatible avec la fonctionnalité de restauration automatique, et qui dispose des droits

© Acronis International GmbH, 2003-2026

Paramètre	Description
	d'accès à la sauvegarde. Vous pouvez installer plusieurs agents sur des hôtes VMware ESXi, et lancer un processus de restauration automatique distinct avec chacun d'eux. Ces processus de restauration automatique peuvent s'exécuter simultanément.
Paramètres de machine cible	Paramètres de machine virtuelle : • **Processeurs virtuels**. Sélectionnez le nombre de processeurs virtuels. • **Mémoire**. Sélectionnez la quantité de mémoire dont disposera la machine virtuelle. • **Unités**. Sélectionnez les unités pour la mémoire. • [Facultatif] **Adaptateurs réseau**. Pour ajouter un adaptateur réseau, cliquez sur **Ajouter**, puis sélectionnez un réseau dans le champ **Réseau**. Quand les changements vous conviennent, cliquez sur **Terminé**.
Chemin d'accès	(Pour les hôtes Microsoft Hyper-V) Dossier sur l'hôte où votre machine sera stockée. Assurez-vous que l'espace disponible sur l'hôte est suffisant pour la machine.
Magasin de données	(Pour les hôtes VMware ESXi) Magasin de données sur l'hôte où votre ordinateur sera stocké. Assurez-vous que l'espace disponible sur l'hôte est suffisant pour la machine.
Mode de provisionnement	Méthode d'allocation du disque virtuel. Pour les hôtes Microsoft Hyper-V : • **En expansion dynamique** (Valeur par défaut). • **Taille fixe**. Pour les hôtes Microsoft Hyper-V : • **Dynamique** (Valeur par défaut). • **Statique**.
Nom de machine cible	Le nom de la machine cible. Par défaut, le nom de la machine cible est le même que celui du serveur de restauration. Le nom de la machine cible doit être spécifique à l'**emplacement de la machine cible** sélectionné.

5. Cliquez sur **Démarrer le transfert de données** et, dans la fenêtre de confirmation, cliquez sur **Démarrer**.

© Acronis International GmbH, 2003-2026

Remarque
S'il n'y a pas de sauvegarde de la machine virtuelle dans le cloud, le système effectuera une sauvegarde automatiquement avant la phase de transfert des données.

La phase **Transfert de données** démarre. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre affiche la quantité de données déjà transférées vers le site local, ainsi que la quantité totale de données à transférer. La quantité totale de données comprend les données de la dernière sauvegarde avant le démarrage de la phase de transfert de données, ainsi que les sauvegardes des données nouvellement générées (incréments de sauvegarde), car la machine virtuelle continue à s'exécuter lors de la phase de transfert de données. Pour cette raison, les deux valeurs du paramètre **Progression** augmentent au fil du temps.
Estimation de l'interruption d'activité	Ce paramètre indique la durée d'indisponibilité de la machine virtuelle dans le cloud si vous démarrez la phase de basculement maintenant. La valeur est calculée en fonction des valeurs du paramètre **Progression** et diminue au fil du temps.

6. Cliquez sur **Basculement**, puis cliquez une nouvelle fois sur **Basculement** dans la fenêtre de confirmation.
   La phase de basculement commence. La console affiche les informations suivantes :

Champs	Description
Progression	Ce paramètre montre la progression de la restauration de la machine sur le site local.
Temps restant estimé	Ce paramètre indique l'heure approximative à laquelle la phase de basculement sera terminée et où vous pourrez démarrer la machine virtuelle sur le site local.

Remarque
Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

7. Une fois que la phase de **basculement** est terminée et que la machine virtuelle de votre site local est démarrée automatiquement, vérifiez qu'elle fonctionne comme prévu.
8. Cliquez sur **Confirmer la restauration automatique** et, dans la fenêtre de confirmation, cliquez sur **Confirmer** pour finaliser le processus.
   La machine virtuelle dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

© Acronis International GmbH, 2003-2026

Remarque
Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

Restauration automatique manuelle à partir de Microsoft Azure

Remarque
Nous vous recommandons d'utiliser le processus de restauration automatique en mode manuel uniquement lorsque l'équipe de support vous l'indique.

Vous pouvez également démarrer un processus de restauration automatique en mode manuel. Dans ce cas, le transfert de données depuis la sauvegarde dans le cloud vers le site local n'est pas effectué automatiquement. Il doit être effectué manuellement après l'arrêt de la machine virtuelle dans le cloud. Le processus de restauration automatique en mode manuel est beaucoup plus lent et vous devez vous attendre à une interruption d'activité plus longue.

Le processus de restauration automatique en mode manuel se compose des phases suivantes :

1. **Planification**. Lors de cette phase, vous restaurez l'infrastructure informatique sur votre site local (configuration des hôtes et du réseau), configurez les paramètres de restauration automatique et planifiez le moment où démarrer le transfert de données.
2. **Basculement**. Lors de cette phrase, la machine virtuelle dans le cloud est arrêtée et les données générées récemment sont sauvegardées. Si aucun plan de sauvegarde n'est appliqué au serveur de restauration, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus. Lorsque la sauvegarde est terminée, restaurez manuellement la machine sur le site local. Vous pouvez restaurer le disque à l'aide d'un support de démarrage, ou restaurer la machine tout entière à partir du stockage de sauvegarde dans le Cloud.
3. **Validation**. Lors de cette phase, vous vérifiez que la machine physique ou virtuelle sur le site local fonctionne correctement, et confirmez la restauration automatique. Après la confirmation, la machine virtuelle sur le site dans le Cloud est supprimée, et le serveur de restauration revient à l'état **En attente**.

Exécution d'une restauration automatique manuelle à partir de Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Vous pouvez effectuer une restauration automatique manuelle à partir de Microsoft Azure vers une machine cible physique ou une machine virtuelle sur votre site local.

© Acronis International GmbH, 2003-2026

Pour effectuer une restauration automatique en mode manuel

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Serveurs**.
2. Sélectionnez le serveur de restauration en état de **basculement**.
3. Cliquez sur l'onglet **Restauration automatique**.
4. Dans le champ **Cible**, sélectionnez **Machine physique**.
5. Cliquez sur l'icône en forme d'engrenage, puis activer le paramètre **Utiliser le mode manuel**.
6. [Facultatif] Calculez le temps d'arrêt estimé qui surviendra lors du processus de restauration automatique en divisant la valeur **Taille de la sauvegarde** par la vitesse de votre connexion Internet.

   Remarque
   La valeur de la vitesse de votre connexion Internet diminuera quand vous exécuterez simultanément plusieurs processus de restauration automatique.

7. Cliquez sur **Basculement** et, dans la fenêtre de confirmation, cliquez une nouvelle fois sur **Basculement**.
   La machine virtuelle sur le site dans le Cloud est désactivée.

   Remarque
   Si aucun plan de sauvegarde n'est appliqué à la machine virtuelle dans le cloud, une sauvegarde sera effectuée automatiquement pendant la phase de basculement, ce qui ralentit le processus.

8. Restaurez le serveur depuis la sauvegarde dans le cloud vers la machine physique ou virtuelle sur votre site local.
   Pour plus d'informations, voir "Restauration de machines virtuelles" (p. 689) et "Restauration de machines physiques" (p. 674).

   Remarque
   Si vous effectuez une restauration automatique d'une machine virtuelle Microsoft Azure vers la machine virtuelle Azure d'origine, utilisez les options de restauration décrites dans "Restauration automatique à partir de Microsoft Azure vers une machine virtuelle Azure" (p. 1152).

9. Assurez-vous que la restauration est terminée et que la machine restaurée fonctionne correctement, puis cliquez sur **La machine a été restaurée**.
10. Si tout fonctionne comme prévu, cliquez sur **Confirmer la restauration automatique** et, dans la fenêtre de confirmation, cliquez une nouvelle fois sur **Confirmer**.
    Le serveur de restauration et le point de restauration sont disponibles pour le prochain basculement. Pour créer de nouveaux points de restauration, appliquez un plan de protection au nouveau serveur local.

© Acronis International GmbH, 2003-2026

Remarque
Appliquer un plan de protection sur le serveur restauré ne fait pas partie du processus de restauration automatique. Une fois le processus de restauration automatique terminé, appliquez un plan de protection sur le serveur restauré pour vous assurer qu'il est de nouveau protégé. Vous pouvez appliquer le même plan de protection que celui appliqué sur le serveur d'origine ou un nouveau plan de protection pour lequel le module **Reprise d'activité après sinistre** est activé.

Restauration automatique à partir de Microsoft Azure vers une machine virtuelle Azure

Vous pouvez effectuer une restauration automatique d'une machine virtuelle Microsoft Azure vers la machine virtuelle Azure d'origine en suivant la procédure pour "Exécution d'une restauration automatique manuelle à partir de Microsoft Azure" (p. 1150) et en utilisant l'une des options de restauration suivantes à l'étape 8 :

Options de restauration

- Restauration sans agent

  Prend en charge la restauration uniquement vers une nouvelle machine virtuelle Azure qui est créée automatiquement.

  Processus : Configurez la connexion Azure dans la console Cyber Protect (**Terminaux** > **Ajouter** > **Machine virtuelle Microsoft Azure**).

  Une machine virtuelle d'appliance de sauvegarde est déployée dans l'abonnement Azure pour gérer la restauration.

  Flux de restauration :

  Dans l'écran **Stockage de sauvegarde**, sélectionnez une sauvegarde. Restaurez-la en tant que machine virtuelle Azure.

  Vous pouvez utiliser le même flux pour les sauvegardes physiques, virtuelles ou avec agent.

  Considération des coûts : la machine virtuelle de l'appliance, lorsqu'elle est utilisée uniquement pour la restauration, peut être mise sous tension uniquement pendant la restauration, puis éteinte manuellement.
- Restauration avec agent

  Prend en charge la restauration vers la même machine virtuelle Azure (si la machine virtuelle d'origine avec l'agent est disponible) ou une nouvelle machine virtuelle Azure qui a un nouvel agent installé.

  Processus : Créez manuellement une machine virtuelle Windows/Linux vierge dans Azure. Installez l'agent de protection. Utilisez l'agent pour parcourir et restaurer des sauvegardes à partir du stockage dans le cloud Acronis.

  Pour plus d'informations, voir Restaurer des ordinateurs Microsoft Azure et Amazon EC2.

© Acronis International GmbH, 2003-2026

Runbooks dans Microsoft Azure

Un runbook est un ensemble d'instructions décrivant comment lancer l'environnement de production dans le cloud.

Les runbooks vous permettent d'effectuer les opérations suivantes :

- Automatisez le basculement d'un ou de plusieurs serveurs.
- Vérifiez automatiquement le résultat du basculement en envoyant une commande ping à l'adresse IP du serveur et en vérifiant la connexion au port que vous spécifiez.
- Définissez la séquence d'opérations pour les serveurs exécutant des applications distribuées.
- Incluez des opérations manuelles dans votre workflow.
- Vérifier l'intégrité de votre solution de reprise d'activité après sinistre en exécutant des runbooks en mode test

Runbooks pour automatiser l'opération de basculement et garantir que vos systèmes sont restaurés dans le bon ordre pour répondre aux dépendances entre les applications.

Les runbooks vous permettent d'automatiser le basculement d'un ou plusieurs serveurs. Vous pouvez définir la bonne séquence d'opérations de basculement pour les serveurs exécutant des applications distribuées. Vous pouvez exécuter des runbooks en mode test ou production, afin de vérifier l'intégrité de votre solution de reprise d'activité après sinistre.

Création d'un runbook dans Microsoft Azure

Un runbook se compose d'étapes exécutées consécutivement. Une étape se compose d'actions qui commencent simultanément.

Pour créer un runbook dans Microsoft Azure

1. Dans la console Cyber Protection, accédez à **Disaster Recovery** > **Runbooks**.
2. Cliquez sur **Créer un runbook**.
3. Cliquez sur **Ajouter une étape**.
4. Cliquez sur **Ajouter une action**, puis sélectionnez l'action que vous souhaitez ajouter à l'étape.

Action	Description
Basculer le serveur	Effectue le basculement d'un serveur de restauration. Pour définir cette action, vous devez sélectionner un serveur de restauration et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres de runbook dans Microsoft Azure" (p. 1155).

© Acronis International GmbH, 2003-2026

Action	Description
	Remarque Si la sauvegarde du serveur que vous sélectionnez est chiffrée à l'aide du chiffrement comme propriété de l'ordinateur, l'action de **Basculer le serveur** est mise en pause et passe automatiquement à **Interaction requise**. Pour poursuivre l'exécution du runbook, vous devez fournir le mot de passe de la sauvegarde chiffrée.
Restaurer le serveur automatiquement	Effectue la restauration automatique d'un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres de runbook dans Microsoft Azure" (p. 1155). **Remarque** Les opérations de runbook prennent en charge la restauration automatique en mode manuel uniquement. Cela signifie que si vous démarrez le processus de restauration automatique en exécutant un runbook qui inclut une étape **Restaurer le serveur automatiquement**, la procédure nécessitera une interaction manuelle : vous devez restaurer l'ordinateur manuellement, et confirmer ou annuler le processus de restauration automatique à partir de l'onglet **Disaster Recovery** > **Serveurs**.
Démarrer le serveur	Démarre un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres de runbook dans Microsoft Azure" (p. 1155). **Remarque** L'action **Démarrer le serveur** ne s'applique qu'aux opérations de basculement test dans les runbooks. Si vous essayez d'exécuter une telle action, elle échoue et affiche le message d'erreur suivant : Échec : l'action ne s'applique pas à l'état actuel du serveur.
Arrêter le serveur	Arrête un serveur cloud. Pour définir cette action, vous devez sélectionner un serveur cloud et configurer les paramètres du runbook disponibles pour cette action. Pour plus d'informations sur ces paramètres, voir "Paramètres de runbook dans Microsoft Azure" (p. 1155). **Remarque** L'action **Arrêter le serveur** ne s'applique pas aux opérations de basculement test dans les runbooks. Si vous essayez d'exécuter une telle action, elle échoue et affiche le message d'erreur suivant : Échec : l'action ne s'applique pas à l'état actuel du serveur.
Opération manuelle	Une opération manuelle nécessite une interaction de la part de l'utilisateur. Pour définir cette action, vous devez entrer une description. Lorsqu'une séquence de runbook atteint une opération manuelle, le runbook

© Acronis International GmbH, 2003-2026

Action	Description
	est mis en pause et ne reprend que lorsqu'un utilisateur effectue l'opération manuelle requise, par exemple, clique sur le bouton de confirmation.
Exécuter le runbook	Exécute un autre runbook. Pour définir cette action, vous devez choisir un runbook. Un runbook ne peut contenir qu'une seule exécution d'un runbook donné. Par exemple, si vous avez ajouté l'action « Exécuter le runbook A », vous pouvez ajouter l'action « Exécuter le runbook B », mais vous ne pouvez pas ajouter une autre action « Exécuter le runbook A ».

5. Définissez les paramètres de runbook de l'action. Pour plus d'informations sur ces paramètres, voir "Paramètres du runbook" (p. 1107).
6. [Facultatif] Pour ajouter une description de l'étape :
   a. Cliquez sur l'icône représentant des points de suspension, puis cliquez sur **Description**.
   b. Entrez une description de l'étape.
   c. Cliquez sur **Terminé**.
7. Répétez les étapes 3 à 6 jusqu'à ce que vous ayez créé la séquence d'étapes et d'actions souhaitée.
8. [Facultatif] Pour changer le nom par défaut du runbook :
   a. Cliquez sur l'icône représentant des points de suspension.
   b. Entrez le nom du runbook.
   c. Entrez une description du runbook.
   d. Cliquez sur **Terminé**.
9. Cliquez sur **Enregistrer**.
10. Cliquez sur **Fermer**.

Paramètres de runbook dans Microsoft Azure

Les paramètres de runbook sont des paramètres spécifiques que vous devez configurer pour définir une action de runbook. Ils définissent le comportement du runbook en fonction de l'état ou du résultat initial de l'action.

Le tableau suivant décrit les paramètres de runbook configurables pour chaque action.

Paramètre de runbook	Disponible pour l'action	Description
Continuer si l'action a déjà été effectuée	• **Basculer le serveur** • **Démarrer le serveur** • **Arrêter le serveur** • **Restaurer le serveur automatiquement**	Ce paramètre définit le comportement du runbook lorsque l'action requise est déjà effectuée (par exemple, lorsqu'un basculement a déjà été effectué ou qu'un serveur est déjà en fonctionnement). Lorsqu'il est activé, le runbook émet un avertissement et

© Acronis International GmbH, 2003-2026

Paramètre de runbook	Disponible pour l'action	Description
		continue le processus. Lorsqu'il est désactivé, l'action échoue et le runbook échoue également. Par défaut, ce paramètre est activé.
Continuer si l'action a échoué	• **Basculer le serveur** • **Démarrer le serveur** • **Arrêter le serveur** • **Restaurer le serveur automatiquement**	Ce paramètre définit le comportement du runbook lorsque l'action requise échoue. Lorsqu'il est activé, le runbook affiche un avertissement, puis continue. Lorsqu'il est désactivé, l'action et le runbook échouent. Par défaut, ce paramètre est désactivé.

Opérations avec des runbooks dans Microsoft Azure

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Lorsque le runbook n'est pas en cours d'exécution, les opérations suivantes sont disponibles : exécuter, modifier, cloner, afficher les détails et supprimer.

Exécuter

À chaque fois que vous cliquez sur **Exécuter**, vous êtes invité à saisir les paramètres d'exécution. Ces paramètres s'appliquent à toutes les opérations de basculement et de restauration automatique incluses dans le runbook. Les runbooks spécifiés dans les opérations **Exécuter le runbook** hériteront de ces paramètres du runbook principal.

Pour exécuter un runbook

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Runbooks**.
2. Cliquez sur le runbook que vous souhaitez exécuter, puis cliquez sur **Exécuter**.

© Acronis International GmbH, 2003-2026

3. Dans la fenêtre **Paramètres d'exécution**, configurez les paramètres.

Paramètre	Description
Mode basculement et restauration automatique	Choisissez si vous souhaitez effectuer un basculement test (par défaut) ou un basculement réel (production). Le mode de restauration automatique correspondra au mode de basculement sélectionné.
Point de restauration en mode basculement	Sélectionnez le point de restauration le plus récent (par défaut) ou sélectionnez un moment donné dans le passé. Si vous sélectionnez un moment donné dans le passé, les points de restauration les plus proches avant la date et l'heure spécifiées seront sélectionnés pour chaque serveur.

4. Cliquez sur **Démarrer**.

   L'exécution du runbook commence. Vous pouvez arrêter l'exécution du runbook. Le logiciel complétera toutes les actions déjà commencées, sauf celles qui nécessitent une intervention de l'utilisateur.

   Modifier

   Pour modifier un runbook

   1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Runbooks**.
   2. Cliquez sur le runbook que vous souhaitez modifier, puis cliquez sur **Modifier**.
   3. Modifiez le runbook.
   4. Cliquez sur **Enregistrer**.

   Cloner

   Lorsque vous clonez un runbook, l'historique du runbook d'origine n'est pas cloné.

   Cloner un runbook

   1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Runbooks**.
   2. Cliquez sur le runbook que vous souhaitez cloner, puis cliquez sur **Cloner**.
   3. [Facultatif] Dans la fenêtre de clonage, modifiez le nom par défaut et entrez une description.
   4. Cliquez sur **Cloner**.

   Afficher les détails

   Pour afficher les détails d'un runbook

   1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Runbooks**.
   2. Cliquez sur le runbook dont vous souhaitez afficher les détails.
      Les détails du runbook et l'historique d'exécution sont affichés.

© Acronis International GmbH, 2003-2026

3. [Facultatif] Pour afficher le journal d'exécution d'une exécution spécifique, cliquez sur la ligne qui lui correspond.

Supprimer

Pour supprimer un runbook

1. Dans la console Cyber Protect, accédez à **Disaster Recovery** > **Runbooks**.
2. Cliquez sur le runbook que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Ressources Azure créées lors de la configuration du site DR et du basculement

Lorsque vous ajoutez une connexion à votre abonnement Azure, le système crée un groupe de ressources avec le préfixe `cyber-protect-rg*` dans la région Azure que vous avez sélectionnée lors de la configuration de la connexion Azure. Ce groupe de ressources a la balise suivante : **Application:CyberProtect**. Pour plus d'informations, voir Sécurité et audit de la connexion Microsoft Azure (72684).

Lorsque la configuration du site (DR) est terminée, un groupe de ressources avec le préfixe `dr-rg*` est créé pour agréger les ressources pour le basculement. Ce groupe de ressources a la balise suivante : **Application:DisasterRecovery**.

Lors des opérations de reprise d'activité après sinistre, des workers temporaires sont déployés pour orchestrer les opérations de basculement, de restauration automatique et de sauvegarde après basculement. Il s'agit de machines virtuelles Azure temporaires exécutées dans le groupe de ressources `cyber-protect-rg*`. Toutes les ressources Azure nécessaires à un basculement de reprise d'activité après sinistre, comme les comptes de stockage et les machines virtuelles ayant fait l'objet d'un basculement, sont créées dans le groupe de ressources `dr-rg*`. Vous pouvez gérer la région Azure du groupe de ressources de connexion, du groupe de ressources DR et de leurs ressources associées lors de la configuration du site DR.

Suppression douce des tenants disposant d'un site de reprise d'activité après sinistre dans Microsoft Azure

La fonctionnalité de suppression douce d'un tenant (Corbeille) est prise en charge pour la configuration du site DR Microsoft Azure.

Pour garantir la continuité des activités pendant la suppression douce et la suppression définitive, les machines virtuelles Azure en basculement ne seront ni arrêtées ni supprimées.

Cas particulier

Si vous désactivez l'élément d'offre **DR et sauvegarde directe sur Azure** (soit intentionnellement, soit accidentellement), une suppression douce de la configuration DR Azure est déclenchée. Cela signifie que la configuration est supprimée mais reste dans la Corbeille pendant 30 jours. Si pendant

© Acronis International GmbH, 2003-2026

cette période vous configurez un nouveau site DR dans un autre emplacement (pas Microsoft Azure), pour restaurer la configuration DR initiale vers Microsoft Azure, vous devez activer l'élément d'offre **DR et sauvegarde directe vers Azure**, supprimer la nouvelle configuration, puis restaurer la configuration initiale.

Agents dans Microsoft Azure

Les agents temporaires à la demande sont exécutés dans votre abonnement Azure, dans le groupe de ressources système (avec le préfixe : « cyber-protect-rg* »), lors des opérations de reprise d'activité après sinistre telles que le basculement, la sauvegarde après basculement et la restauration automatique. Un agent est déployé pour chaque opération, puis supprimé à la fin de celle-ci. Ce modèle à la demande permet de réduire les coûts en déployant automatiquement les agents uniquement pendant les opérations DR actives, puis en les supprimant ensuite.

Le déploiement initial de l'agent pour un basculement test ou de production peut prendre plusieurs minutes. Le démarrage des workers pour les basculements suivants devrait être plus rapide.

Pour surveiller l'état des workers actifs, accédez à **Clouds publics**, cliquez sur la connexion à votre abonnement Microsoft Azure, puis cliquez sur l'onglet **Workers**.

Si une opération de reprise d'activité après sinistre échoue en raison d'une erreur avec l'agent, vous pouvez générer un rapport et afficher plus d'informations sur l'erreur. Pour ce faire, accédez à l'onglet **Workers**, activez l'interrupteur **Dépannage**, cliquez sur le lien **Instructions**, puis suivez les instructions.

Tableau de bord Reprise d'activité après sinistre

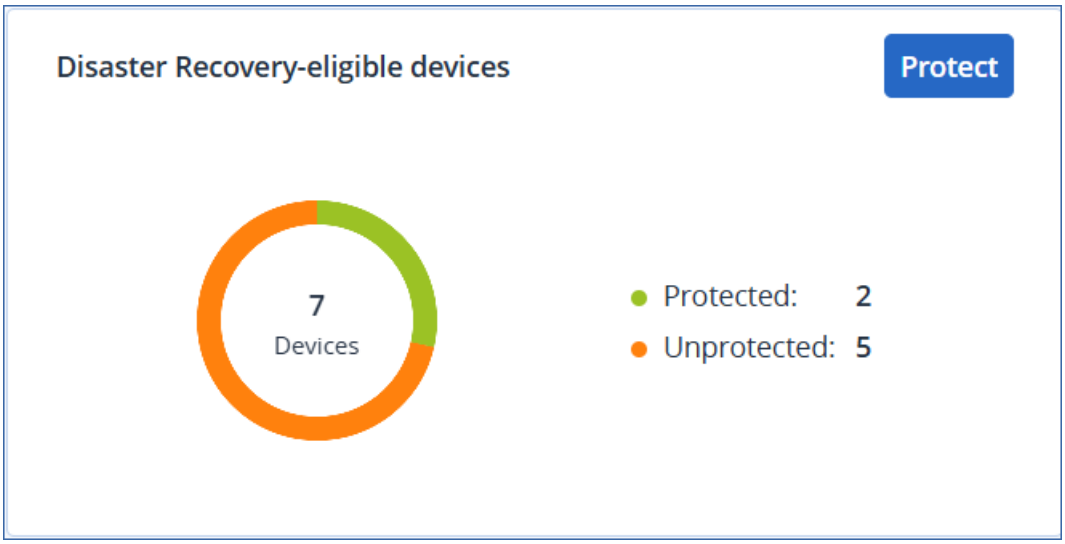
La page **Tableau de bord** de la reprise d'activité après sinistre contient des widgets qui fournissent une vue d'ensemble en temps réel et des informations exploitables concernant votre site de reprise d'activité après sinistre tout au long de son cycle de vie. Cela vous aide à :

- Détectez et résolvez rapidement les problèmes en surveillant l'état des serveurs de restauration et principaux.
- Évitez l'utilisation excessive de points de calcul en surveillant le nombre de serveurs qui les consomment.

Terminaux éligibles à la reprise d'activité après sinistre

Le widget affiche le nombre total de terminaux protégés par la reprise d'activité après sinistre (ayant un serveur de restauration) et le nombre total de terminaux éligibles à la protection par la reprise d'activité après sinistre.

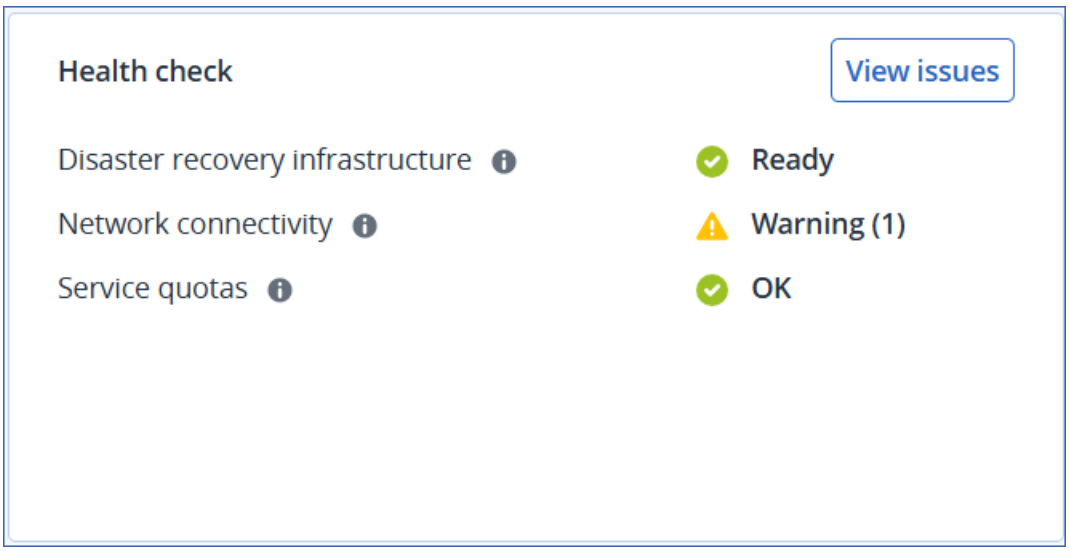
© Acronis International GmbH, 2003-2026



Pour accéder à la page **Tous les terminaux** où vous pouvez configurer la reprise d'activité après sinistre pour les terminaux éligibles, cliquez sur **Protéger**.

Vérification de l'intégrité

Le widget affiche des informations sur l'intégrité de votre infrastructure de reprise d'activité après sinistre. Vous pouvez vérifier l'état de la configuration du site, la disponibilité du réseau (disponible uniquement pour Disaster Recovery vers Cyber Protect Cloud), ainsi que l'existence de quotas de service manquants.

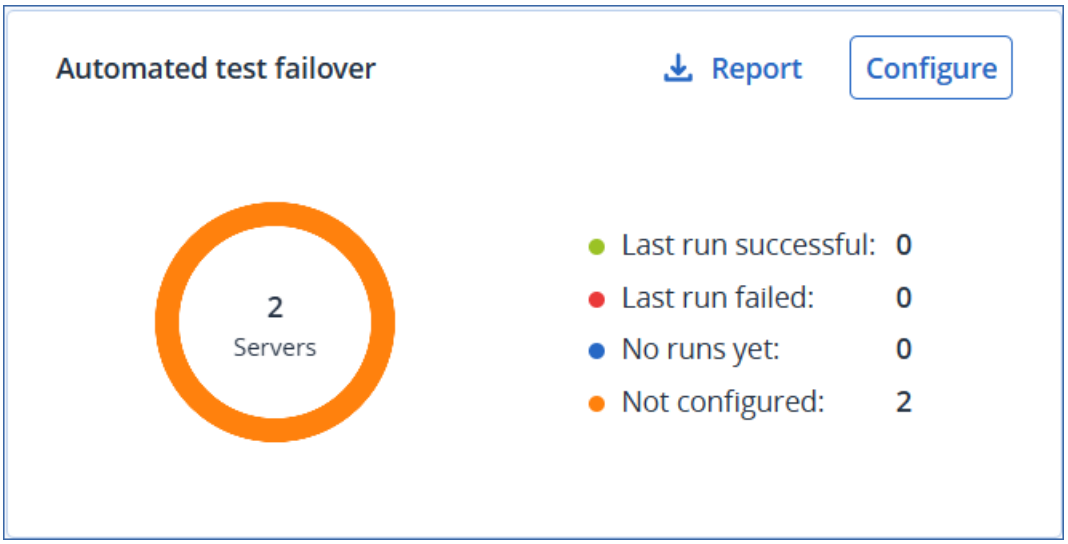


Pour afficher plus d'informations sur les problèmes détectés (avertissements ou erreurs), cliquez sur **Afficher les problèmes**.

Basculement test automatisé

Le widget affiche des informations sur les opérations de basculement test automatisé de vos serveurs de restauration.

© Acronis International GmbH, 2003-2026



Pour commencer à configurer le basculement test automatisé de vos serveurs, cliquez sur **Configurer**.

Pour télécharger les données du widget, cliquez sur **Rapport**, puis choisissez le format – **PDF** ou **CSV**.

Serveurs de restauration en basculement

Le widget affiche le nombre et l'état des serveurs de restauration qui sont en production ou en basculement de test.

S'il n'y a actuellement aucun serveur de restauration en cours d'exécution dans le cloud, vous verrez un zéro. S'il y a un problème avec un serveur, vous verrez un avertissement ou un statut d'erreur.

L'utilisation des points de calcul affichée par heure est une image instantanée en temps réel, pas une valeur historique. Cela signifie que si, par exemple, vous avez deux serveurs de restauration et que chacun d'eux utilise huit points, vous verrez un total de 16 points affichés dans le widget.

Vous pouvez utiliser ces informations pour estimer le coût d'exécution de ces serveurs, et également comme rappel pour arrêter un basculement d'un serveur dont vous n'avez plus besoin.

Serveurs primaires

Le widget est disponible uniquement pour Disaster Recovery vers Cyber Protect Cloud. Il affiche le nombre et l'état des serveurs principaux dans votre environnement, ainsi que leur utilisation des points de calcul par heure. Vous pouvez utiliser ces informations pour repérer et résoudre rapidement tout problème.

L'utilisation des points de calcul affichée par heure est une image instantanée en temps réel, pas une valeur historique. Cela signifie que si, par exemple, vous avez deux serveurs de restauration et que chacun d'eux utilise huit points, vous verrez un total de 16 points affichés dans le widget.

Vous pouvez utiliser ces informations pour estimer le coût d'exécution de ces serveurs, et également comme rappel pour arrêter un basculement d'un serveur dont vous n'avez plus besoin.

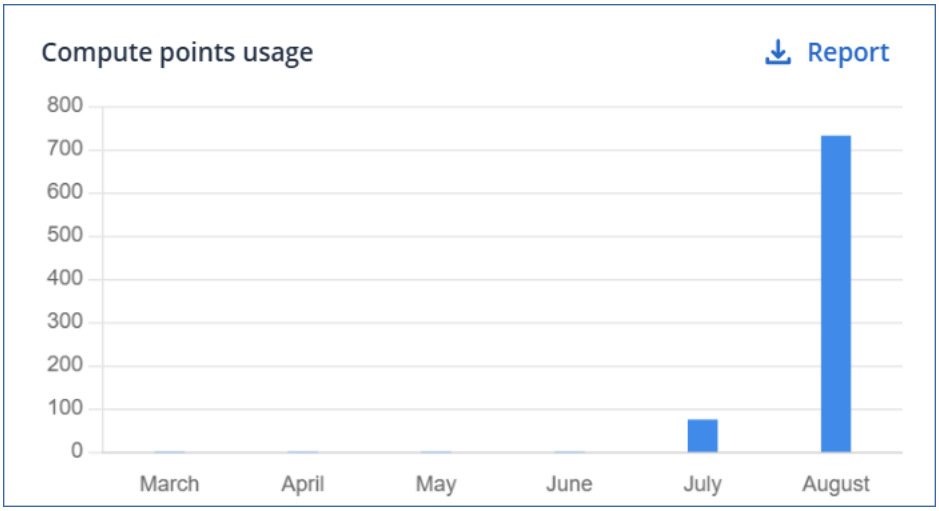
© Acronis International GmbH, 2003-2026

Alertes du serveur dans le cloud

Le widget affiche les dernières alertes par gravité, afin que vous puissiez voir les alertes critiques d'un coup d'œil. Les valeurs **Type d'alerte** et **Serveur de restauration** dans le widget sont des liens qui ouvrent les détails de l'alerte et les détails du serveur de restauration, respectivement.

Utilisation des points de calcul

Ce widget affiche le nombre de points de calcul qui ont été utilisés dans votre environnement au cours des 6 derniers mois - le mois en cours et chacun des cinq mois précédents.



Vous pouvez télécharger un rapport détaillé sous forme de fichier CSV ou PDF. Le fichier contient, pour chaque mois, les informations suivantes concernant les serveurs ayant consommé des points de calcul : nom du serveur, type de serveur, état, initiateur, heure de démarrage, heure d'arrêt, nombre d'heures d'utilisation dans le mois, consommation de calcul par heure et consommation totale de points de calcul sur le mois.

Pour télécharger les données du widget, cliquez sur **Rapport**, puis sélectionnez le format de fichier de votre choix.

Compatibilité de Disaster Recovery avec le logiciel de chiffrement

La reprise d'activité après sinistre est compatible avec les logiciels de chiffrement de disque suivants :

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

© Acronis International GmbH, 2003-2026

Remarque

- Pour les ressources avec chiffrement au niveau du disque, nous vous recommandons d'installer l'agent de protection dans le système d'exploitation invité de la ressource, et d'effectuer des sauvegardes avec agent.
- Le basculement et la restauration automatique ne sont pas pris en charge pour les sauvegardes sans agent de ressources chiffrées.

Pour plus d'informations sur la compatibilité de Cyber Protection avec le logiciel de chiffrement, voir "Compatibilité avec le logiciel de chiffrage" (p. 545).

© Acronis International GmbH, 2003-2026

Configuration de la protection antivirus et antimalware

Remarque
Sur les ordinateurs Windows, les fonctionnalités de protection antimalware et de filtrage d'URL nécessitent l'installation de l'agent de protection antimalware et de filtrage d'URL. Cet agent est installé automatiquement pour les ressources protégées si les options **Protection antivirus et antimalware** ou **Filtrage d'URL** sont activées dans leurs plans de protection.

La protection antimalware dans Cyber Protection vous offre les avantages suivants :

- Protection optimale à toutes les étapes : proactive, active et réactive.
- Quatre technologies antimalware intégrées pour vous offrir une protection de premier ordre à plusieurs niveaux.
- Gestion du service Microsoft Security Essentials et de l'antivirus Microsoft Defender.

  Remarque
  La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Important
Le fichier test EICAR est détecté uniquement lorsque l'option **Protection antimalware Advanced** est activée dans le plan de protection. Cependant, les fonctionnalités antimalware de Cyber Protection ne sont pas affectées si le fichier test EICAR n'est pas détecté.

Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware

Remarque
Cette fonctionnalité n'est prise en charge que sur les processeurs suivants, qui prennent en charge le jeu d'instructions SSE4.2 :

- Processeurs Intel publiés après 2011
- Processeurs AMD publiés après 2012

Les fonctionnalités de protection active antivirus et antimalware sont prises en charge sur les plates-formes suivantes.

Système d'exploitation	Version/Distribution
Windows	• Windows 7 Service Pack 1 et versions ultérieures • Windows Server 2008 R2 Service Pack 1 et versions ultérieures

© Acronis International GmbH, 2003-2026

Système d'exploitation	Version/Distribution
	Remarque Pour Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft avant d'installer l'agent de protection : • Mises à jour de sécurité étendues (ESU) pour Windows 7 • KB4474419 • KB4490628 Pour plus d'informations sur les mises à jour requises, voir cet article de la base de connaissances.
Linux	• Red Hat Linux 7.x, 8.x, 9.x • CloudLinux 6.10, 7.x, 8.x • CentOS 6.5 et dernières versions 6.x, 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 • Debian 8.x, 9.x, 10,x, 11.x • Oracle Linux 7.x, 8.x, 9.x • SUSE Enterprise Linux 15.x • openSUSE Leap 15.x **Remarque** Le moteur d'analyse comportementale prend en charge les versions Linux suivantes : • CentOS 7.x • Debian 10.x, 11.x • CloudLinux 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04, et 22.04
macOS	• macOS 10.13.x et versions ultérieures

Fonctionnalités prises en charge par plate-forme

Remarque
La protection antimalware pour Linux et macOS est disponible uniquement avec le pack antimalware Advanced Security.

Protection contre les virus et les malwares

Fonctionnalité	Windows	Linux	macOS
Fonctionnalité Active Protection totalement intégrée	Oui	Non	Non
Protection antimalware en temps réel	Oui	Oui	Oui

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Fonctionnalité avancée de protection antimalware en temps réel avec détection basée sur la signature locale	Oui	Oui	Oui
Analyse statique pour les fichiers exécutables portables	Oui	Non	Oui[1]
Analyse antimalware à la demande	Oui	Oui[2]	Oui
Protection du dossier réseau	Oui	Non[3]	Non
Protection côté serveur	Oui	Non	Non
Analyse des fichiers d'archive	Oui	Non	Oui
Analyse des lecteurs amovibles	Oui	Non	Oui
Analyse des fichiers nouveaux et modifiés uniquement	Oui	Non	Oui
Exclusions de fichier/dossier	Oui	Oui	Oui[4]
Exclusions des processus	Oui	Non	Oui
Moteur d'analyse du comportement	Oui	Oui[5]	Oui
Prévention des failles	Oui	Non	Non
Quarantaine	Oui	Oui	Oui
Nettoyage automatique de la zone de quarantaine	Oui	Oui	Oui
Filtrage d'URL (http/https)	Oui	Non	Non
Liste blanche à l'échelle de l'entreprise	Oui	Non	Oui
Gestion du pare-feu[6]	Oui	Non	Non
Gestion de Microsoft Defender Antivirus[7]	Oui	Non	Non
Gestion de Microsoft Security Essentials	Oui	Non	Non
Inscription et gestion de la protection contre les virus et les malwares via le centre de sécurité Windows	Oui	Non	Non

[1] L'analyse statique pour les fichiers exécutables portables est prise en charge uniquement pour les analyses planifiées sur macOS.

[2] Les conditions de démarrage ne sont pas prises en charge pour l'analyse à la demande sous Linux.

[3] Les dossiers réseau dans Linux sont traités comme des dossiers locaux, c'est pourquoi Active Protection protégera automatiquement les dossiers réseau dans le système d'exploitation Linux, comme s'il s'agissait de dossiers locaux.

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
[4] Les exclusions de fichier/dossier sont prises en charge uniquement lorsque vous spécifiez les fichiers et les dossiers qui ne seront pas analysés par la protection en temps réel ni par les analyses planifiées sur macOS. [5] Le moteur d'analyse comportementale prend en charge les versions Linux suivantes : • CentOS 7.x • Debian 10.x, 11.x • CloudLinux 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04, et 22.04 [6] La gestion du pare-feu est prise en charge sur Windows 8 et versions ultérieures. Windows Server n'est pas pris en charge. [7] La gestion de l'Antivirus Microsoft Defender est prise en charge sur Windows 8.1 et versions ultérieures. Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).			

Active Protection

Fonctionnalité	Windows	Linux	macOS
Détection d'un processus d'injection	Oui	Non	Non
Restauration automatique de fichiers affectés depuis le cache local	Oui	Oui	Oui
Auto-défense pour les fichiers de sauvegarde Acronis	Oui	Non	Non
Auto-défense pour le logiciel Acronis	Oui	Non	Oui (Uniquement les composants Active Protection et Antimalware)
Gestion des processus fiables/bloqués	Oui	Non	Oui
Exclusions des processus/dossiers	Oui	Oui	Oui
Détection des ransomware basée sur un comportement de processus (basé sur l'IA)	Oui	Oui	Oui
Détection du cryptominage basée sur un comportement de processus	Oui	Non	Non
Protection des lecteurs externes (HDD, lecteurs flash, cartes SD)	Oui	Non	Oui

© Acronis International GmbH, 2003-2026

Fonctionnalité	Windows	Linux	macOS
Protection du dossier réseau	Oui	Non*	Oui
Protection côté serveur	Oui	Non	Non
Protection Zoom, Cisco Webex, Citrix Workspace et Microsoft Teams	Oui	Non	Non

*Les dossiers réseau sous Linux sont traités comme des dossiers locaux ; ainsi, Active Protection protégera automatiquement les dossiers réseau dans le système d'exploitation Linux, comme s'il s'agissait de dossiers locaux.

Pour plus d'informations sur les systèmes d'exploitation et leurs versions pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Protection contre les virus et les malwares

Remarque
Certaines fonctionnalités peuvent nécessiter une licence supplémentaire, en fonction du modèle de gestion de licences appliqué.

Le module **Protection contre les virus et les malwares** protège vos ordinateurs Windows, Linux et macOS contre toutes les menaces de malwares récentes. Vous trouverez la liste complète des fonctionnalités antimalware prises en charge dans "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

La protection contre les virus et les malwares est prise en charge et enregistrée dans le centre de sécurité Windows.

Fonctionnalités antimalware

- Détection des malwares dans les fichiers en mode temps réel et à la demande
- Détection des comportements malveillants dans les processus (Windows)
- Blocage de l'accès aux URL malveillantes (Windows)
- Placement des fichiers dangereux en quarantaine
- Ajout des applications d'entreprise de confiance à la liste d'autorisation

Types d'analyses

Vous pouvez configurer la protection contre les virus et les malwares pour qu'elle s'exécute en permanence en arrière-plan ou à la demande.

© Acronis International GmbH, 2003-2026

Protection en temps réel

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La protection en temps réel vérifie tous les fichiers ouverts ou en cours d'exécution sur un ordinateur afin de prévenir les menaces liées à des malwares.

Pour éviter les éventuels problèmes de compatibilité et de performances, la protection en temps réel ne peut fonctionner en même temps que d'autres solutions antivirus qui proposent également des fonctionnalités de protection en temps réel. L'état des autres solutions antivirus installées est déterminé via le centre de sécurité Windows. Si la machine Windows est déjà protégée par une autre solution antivirus, la protection en temps réel est automatiquement désactivée.

Pour activer la protection en temps réel, désactivez ou désinstallez l'autre solution antivirus. La protection en temps réel peut remplacer automatiquement la protection en temps réel de Microsoft Defender.

Remarque
Sur les machines fonctionnant sous Windows Server, Microsoft Defender ne sera pas désactivé automatiquement lors de l'activation de la protection en temps réel. Un administrateur doit désactiver manuellement Microsoft Defender pour éviter les problèmes de compatibilité potentiels.

Vous pouvez choisir l'un des modes d'analyse suivants :

- La détection **Mode sur accès intelligent** signifie que le programme antimalware s'exécute en arrière-plan et analyse le système de votre ordinateur de manière active et constante, à la recherche de virus et d'autres menaces malveillantes, pendant tout le temps où votre système est sous tension. Les malware seront détectés dans les deux cas lorsqu'un fichier est en cours d'exécution et lors de diverses opérations impliquant le fichier, comme son ouverture en vue de sa lecture ou de sa modification.
- La détection **Lors de l'exécution** signifie que seuls les fichiers exécutables seront analysés lors de leur exécution, afin de garantir qu'ils sont inoffensifs et qu'ils n'endommageront pas votre machine ni vos données. La copie d'un fichier infecté ne sera pas détectée.

Analyse planifiée

L'analyse antimalware est réalisée de façon planifiée.

Vous pouvez choisir l'un des modes d'analyse suivants.

- Mode **Analyse rapide** – Vérifie uniquement les fichiers système de la ressource.
- Mode **Analyse complète** – Vérifie tous les fichiers de votre ressource.
- Mode **Analyse personnalisée** – Vérifie les fichiers/dossiers ajoutés par l'administrateur au plan de protection.

© Acronis International GmbH, 2003-2026

Une fois les analyses antimalware effectuées, vous pouvez consulter les informations relatives aux ressources affectées par des menaces dans le widget **Surveillance** > **Vue d'ensemble** > Affectés récemment.

Paramètres de protection contre les virus et les malwares

Cette section décrit les fonctionnalités que vous pouvez configurer dans le module **Protection antivirus et antimalware** d'un plan de protection. Pour savoir comment créer un plan de protection, voir "Création d'un plan de protection" (p. 244).

Remarque
Tous les systèmes d'exploitation ne prennent pas en charge les fonctions de protection Antivirus & Antimalware. Pour plus d'informations sur les fonctionnalités et systèmes d'exploitation pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164). Certaines fonctionnalités nécessitent une certaine licence pour être disponibles dans votre plan de protection.

Vous pouvez configurer les fonctionnalités suivantes dans le module Protection antivirus et antimalware pour un plan de protection :

Active Protection

Active Protection protège votre système contre le ransomware. Le ransomware est un type de logiciel malveillant qui bloque l'accès à vos fichiers, systèmes ou réseaux en les chiffrant, puis exige un paiement (rançon) pour restaurer l'accès. Une attaque de ransomware peut causer une perturbation opérationnelle sérieuse, une perte de données et des dommages à la réputation de votre organisation.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Paramètre par défaut : **Activé**.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Remarque
Un agent de protection doit être installé sur la machine protégée. Pour plus d'informations sur les fonctionnalités et systèmes d'exploitation pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Pour configurer Active Protection

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Active Protection**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Action lors de la détection**, sélectionnez l'une des options disponibles :
   - **Notifier uniquement** : le logiciel génère une alerte sur le processus suspecté d'activité de ransomware.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus suspecté d'activité de ransomware.
   - **Revenir à l'utilisation du cache** : le logiciel génère une alerte, arrête le processus et annule les modifications apportées aux fichiers, à l'aide du cache de service.

   Paramètre par défaut : Revenir à l'utilisation du cache
4. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Protection antimalware Advanced

Ce moteur utilise une base de données améliorée de signatures de virus afin d'améliorer l'efficacité de la détection des malwares, aussi bien lors des analyses rapides que lors des analyses complètes.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour configurer la protection antimalware Advanced

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Dans la section **Protection antimalware Advanced**, utilisez le bouton-bascule pour activer le moteur basé sur les signatures locales.

Remarque
La protection contre les virus et les malwares pour macOS et Linux nécessitent également le moteur basé sur la signature locale. Pour Windows, la protection contre les virus et les malwares est disponible avec ou sans ce moteur.

Protection du dossier réseau

La fonctionnalité **Protection du dossier réseau** définit si la protection antivirus et antimalware protège les dossiers réseau mappés en tant que lecteurs locaux. La protection s'applique aux dossiers partagés via les protocoles SMB ou NFS.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Pour configurer la protection du dossier réseau

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection du dossier réseau**.
3. Ajoutez les fichiers à l'endroit où vous souhaitez sauvegarder les dossiers réseau :

© Acronis International GmbH, 2003-2026

- Par exemple, si votre ressource est une ressource Windows, saisissez dans le champ **Windows** le chemin d'accès au fichier Windows dans lequel vous souhaitez sauvegarder les dossiers réseau. Valeur par défaut : C:\ProgramData\Acronis\Restored Network Files.
- Par exemple, si votre ressource est une ressource macOS, saisissez dans le champ **macOS** le chemin d'accès aux fichiers macOS dans lequel vous souhaitez sauvegarder les dossiers réseau. Valeur par défaut : /Library/Application Support/Acronis/Restored Network Files/.

Remarque
Saisissez le chemin d'un dossier local. Les dossiers réseau, y compris les dossiers sur les lecteurs mappés, ne sont pas pris en charge en tant que destinations de sauvegarde des dossiers réseau.

4. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Protection côté serveur

Cette fonctionnalité définit si Active Protection protège les dossiers réseau que vous partagez des connexions extérieures entrantes provenant d'autres serveurs du réseau et qui pourraient apporter des menaces.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Paramètre par défaut : **Désactivé**.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Remarque
La protection côté serveur n'est pas prise en charge sous Linux.

Pour configurer des connexions fiables

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.
3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Fiable**.
5. Dans le champ **Connexions fiables**, cliquez sur **Ajouter** pour définir les connexions qui seront autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.

© Acronis International GmbH, 2003-2026

8. Cliquez sur la coche à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Terminé**.

Pour configurer les connexions bloquées

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.
3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Bloqué**.
5. Dans le champ **Connexions bloquées**, cliquez sur **Ajouter** pour définir les connexions qui ne seront pas autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cochez la case à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Terminé**.

Autoprotection

L'autoprotection empêche les modifications non autorisées des propres processus du logiciel, de ses enregistrements du registre et de ses fichiers exécutables et de configuration, ainsi que des sauvegardes contenues dans vos dossiers locaux.

Les administrateurs peuvent activer l'**Autoprotection** sans activer **Active Protection**.

Paramètre par défaut : **Activé**.

Remarque
L'autoprotection n'est pas prise en charge sous Linux.

Pour activer l'autoprotection

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Autoprotection**.
3. Utilisez le bouton-bascule **Autoprotection** pour l'activer.

Protection contre la désinstallation de l'agent

L'option **Protection contre la désinstallation de l'agent** empêche les utilisateurs ou les logiciels de désinstaller l'agent pour Windows, ou de modifier ses composants en dehors de la fenêtre de maintenance configurée.

Paramètre par défaut : **Activé**

© Acronis International GmbH, 2003-2026

Pour désactiver la protection contre la désinstallation de l'agent

Avertissement !
La désactivation de la **Protection contre la désinstallation de l'agent** expose les ressources protégées à des risques de sécurité.

1. Lorsque la fonctionnalité **Autoprotection** est activée, décochez la case **Protection contre la désinstallation de l'agent**.
2. Cliquez sur **Terminé**.

Remarque
Cette option n'empêche pas les mises à jour automatiques de l'agent Cyber Protection.

Chaque tentative de désinstallation ou de modification de l'agent de protection en dehors de la fenêtre de maintenance déclenche une alerte.

Un utilisateur administrateur peut examiner l'alerte et décider d'autoriser les modifications de l'agent pour 1 heure, ou configurer une fenêtre de maintenance d'une durée comprise entre 1 heure et 7 jours. Voir "Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée" (p. 208).

Autoriser les processus à modifier des sauvegardes

Le paramètre **Autoriser des processus particuliers à modifier des sauvegardes** est disponible uniquement lorsque l'option **Autoprotection** est activée.

Elle s'applique aux fichiers dans les dossiers locaux avec les extensions suivantes :

- .tibx
- .tib
- .tia

Le paramètre **Autoriser des processus particuliers à modifier des sauvegardes** vous permet de spécifier les processus autorisés à modifier les fichiers de sauvegarde, même si ces fichiers sont protégés par l'autoprotection. Cela est utile, par exemple, si vous supprimez des fichiers de sauvegarde ou les déplacez vers un autre emplacement à l'aide d'un script.

Si ce paramètre est désactivé, les fichiers de sauvegarde ne peuvent être modifiés que par les processus signés par le fournisseur du logiciel de sauvegarde. Cela permet au logiciel d'appliquer des règles de rétention et de supprimer des sauvegardes lorsqu'un utilisateur le demande depuis l'interface Web. Les autres processus, qu'ils soient suspects ou non, ne peuvent pas modifier les sauvegardes.

Si ce paramètre est activé, vous pouvez autoriser d'autres processus à modifier les sauvegardes.

Paramètre par défaut : **Désactivé**.

Pour activer Autoriser des processus particuliers à modifier des sauvegardes

© Acronis International GmbH, 2003-2026

1. Lorsque la fonctionnalité d'**autoprotection** est activée, sélectionnez la case à cocher **Autoriser des processus particuliers à modifier des sauvegardes**.
2. Dans le champ **Processus de modification des sauvegardes**, cliquez sur **Ajouter**.
3. Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre de lecteur.
4. Cliquez sur la coche à droite pour enregistrer le processus.

Détection d'un processus de cryptominage

Un malware de cryptominage réduit les performances des applications utiles, accroît la facture d'électricité, peut causer des plantages système et même endommager le matériel à cause d'un usage abusif. La fonctionnalité **Détection d'un processus de cryptominage** protège vos terminaux des malwares de cryptominage et évite toute utilisation non autorisée de ressources informatiques.

Les administrateurs peuvent activer la **Détection d'un processus de cryptominage** sans activer **Active Protection**. Paramètre par défaut : **Activé**.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Remarque
La détection de processus de cryptominage n'est pas prise en charge sous Linux.

Pour configurer la détection des processus de cryptominage

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Détection d'un processus de cryptominage**.
3. Utilisez le bouton-bascule **Détecter des processus de cryptominage** pour activer ou désactiver la fonctionnalité.
4. Sélectionnez l'opération à effectuer sur les processus suspectés d'activités de cryptominage :

   Paramètre par défaut : **Arrêter le processus**

   - **Notifier uniquement** : le logiciel génère une alerte.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus.
5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Paramètres de quarantaine

La quarantaine est un dossier utilisé pour isoler les fichiers suspects (probablement infectés) ou potentiellement dangereux.

Pour configurer la quarantaine

© Acronis International GmbH, 2003-2026

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Quarantaine**.
3. Dans le champ **Supprimer les fichiers mis en quarantaine après**, vous pouvez définir la période (en jours) après laquelle les fichiers en quarantaine seront supprimés.
   Paramètre par défaut : **30 jours**
4. Cliquez sur **Terminé**.

Pour plus d'informations sur cette fonctionnalité, consultez la section Quarantaine.

Moteur de comportement

La fonctionnalité **Moteur de comportement** protège un système des malwares en adoptant une approche comportementale heuristique pour repérer les processus malveillants.

Paramètre par défaut : **Activé**.

Pour configurer la protection du dossier réseau

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Moteur de comportement**.
3. Utilisez le bouton-bascule **Moteur de comportement** pour activer ou désactiver la fonctionnalité.
4. Dans la section **Action lors de la détection**, sélectionnez l'action que le logiciel exécutera lors de la détection d'une activité de malware :
   Paramètre par défaut : **Quarantaine**
   - **Notifier uniquement** : le logiciel génère une alerte au sujet du processus suspecté d'activité de malware.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus suspecté d'activité de malware.
   - **Quarantaine** : le logiciel génère une alerte, arrête le processus et place le fichier exécutable dans le dossier de quarantaine.
5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Prévention des failles

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La prévention des exploits détecte les processus infectés et les empêche de se diffuser et d'exploiter les vulnérabilités logicielles sur les systèmes. Lorsqu'une faille est détectée, le logiciel peut générer une alerte et arrêter le processus suspecté d'être à l'origine de la faille.

© Acronis International GmbH, 2003-2026

L'option Prévention des failles est disponible uniquement à partir des versions 12.5.23130 de l'agent (21.08, publiée en août 2020) ou versions ultérieures.

Paramètre par défaut : **Activé** pour les plans de protection nouvellement créés, et **Désactivé** pour les plans de protection existants, créés avec des versions antérieures de l'agent.

Remarque
La prévention des failles n'est pas prise en charge sous Linux.

Vous pouvez sélectionner l'action que le programme doit exécuter lors de la détection d'une faille et les méthodes de prévention des failles appliquées par le programme.

Pour configurer la prévention des exploits

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Prévention des failles**.
3. Dans la section **Action lors de la détection**, sélectionnez l'une des options disponibles :

   Paramètre par défaut : **Arrêter le processus**

   - **Notifier uniquement**
     Le logiciel générera une alerte au sujet du processus suspecté d'activités d'exploit.
   - **Arrêter le processus**
     Le logiciel générera une alerte et arrêtera le processus suspecté d'activités d'exploit.
4. Dans la section **Techniques de prévention des failles activées**, sélectionnez les options disponibles que vous souhaitez appliquer :
   Paramètre par défaut : **Toutes les méthodes sont activées**

   - **Protection de la mémoire**
     Détecte et stoppe les modifications suspectes des droits d'exécution des pages de mémoire. Des processus malveillants apportent de telles modifications aux propriétés de page pour activer l'exécution de shellcodes depuis des zones de mémoire non exécutables telles que les piles et segments.
   - **Protection contre la programmation orientée retour (ROP)**
     Détecte et stoppe les tentatives d'utilisation de la technique d'exploit ROP.
   - **Protection contre la réaffectation de privilèges**
     Détecte et stoppe les tentatives de réaffectation de privilèges effectuées par un code ou une application non autorisés. La réaffectation de privilèges est utilisée par un code malveillant pour obtenir entièrement l'accès à la machine attaquée puis exécuter des tâches essentielles et sensibles. Un code non autorisé n'a pas le droit d'accéder à des ressources critiques du système ni de modifier les paramètres système.
   - **Protection contre l'injection de code**

© Acronis International GmbH, 2003-2026

Détecte et stoppe l'injection de code malveillant dans des processus distants. L'injection de code est utilisée pour masquer l'intention malveillante d'une application derrière des processus propres ou bénins, en vue d'éviter la détection par des solutions antimalware.

5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Remarque
Les processus identifiés comme fiables dans la liste d'exclusion ne seront pas analysés à la recherche de failles.

Protection en temps réel

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La **protection en temps réel** recherche en permanence des virus et d'autres menaces malveillantes dans votre système informatique pendant toute la durée d'activité du système, à moins qu'elle ne soit mise en pause par l'utilisateur de l'ordinateur.

Paramètre par défaut : **Activé**.

Pour configurer la protection en temps réel

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection en temps réel**.
3. Dans la liste déroulante **Action lors de la détection**, sélectionnez l'une des options disponibles :
   Paramètre par défaut : **Quarantaine**
   - **Notifier uniquement**

     Le logiciel génère une alerte concernant le processus suspecté d'activité de ransomware.
   - **Bloquer et notifier**

     Le logiciel bloque le processus et génère une alerte au sujet du processus suspecté d'activité de malware.
   - **Quarantaine**

     Le logiciel génère une alerte, arrête le processus et place le fichier exécutable dans le dossier de quarantaine.
4. Dans la section **Mode d'analyse**, sélectionnez l'action que le logiciel exécutera lors de la détection d'un virus ou d'une autre menace malveillante :
   Paramètre par défaut : **Mode sur accès intelligent**
   - **Mode sur accès intelligent** : surveille toutes les activités du système et analyse automatiquement les fichiers lorsque quelqu'un y accède en lecture ou en écriture, ou à

© Acronis International GmbH, 2003-2026

chaque lancement d'un programme.

- **Lors de l'exécution** : n'analyse automatiquement que les fichiers exécutables lors de leur lancement, afin de vérifier qu'ils sont inoffensifs et qu'ils n'endommageront pas votre ordinateur ni vos données.

5. Cliquez sur **Terminé**.

Planifier l'analyse

L'analyse à la demande recherche des virus dans votre système informatique, en fonction du calendrier précisé. Une analyse complète vérifie tous les fichiers de votre machine, alors qu'une analyse rapide vérifie uniquement les fichiers système de la machine.

Pour configurer une analyse planifiée

Paramètres par défaut :

- L'**Analyse personnalisée** est désactivée.
- Des analyses **Rapides** et **Complètes** sont planifiées.

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Planifier l'analyse**.
3. Utilisez le bouton-bascule pour activer le type d'analyse que vous souhaitez appliquer à votre ordinateur.

Types d'analyse disponibles :

- **Complète** : elle est plus longue que l'analyse rapide, car chaque fichier est vérifié.
- **Rapide** : analyse uniquement les emplacements courants où se trouvent habituellement les malwares sur l'ordinateur.
- **Personnalisée** : analyse les fichiers/dossiers sélectionnés par l'administrateur du plan Protection.

Remarque
Vous pouvez planifier les trois analyses (**Rapide**, **Complète** et **Personnalisée**) dans un même plan de protection.

Pour configurer une analyse personnalisée

- Utilisez le bouton-bascule **Analyse personnalisée** pour activer ou désactiver ce type d'analyse.
- Dans la liste déroulante **Action lors de la détection**, sélectionnez l'une des options disponibles :

Paramètre par défaut : **Quarantaine**

Quarantaine

Le logiciel génère une alerte et place le fichier exécutable dans le dossier de quarantaine.

© Acronis International GmbH, 2003-2026

Notifier uniquement

Le logiciel génère une alerte au sujet du processus suspecté d'être un malware.

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements suivants	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon**

© Acronis International GmbH, 2003-2026

Champs	Description
	l'horaire dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte utilisateur dont la connexion au système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après

© Acronis International GmbH, 2003-2026

Champs	Description
	laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

- Cochez la case **Analyser uniquement les fichiers nouveaux ou modifiés** si vous souhaitez analyser uniquement les fichiers nouveaux ou modifiés.

Paramètre par défaut : **Activé**

- Deux options supplémentaires sont affichées pour l'**Analyse personnalisée** et l'**analyse complète** uniquement :

1. **Analyser les fichiers d'archive**

   Paramètre par défaut : **Activé**.

   Profondeur de réapparition maximum

   Paramètre par défaut : **16**

   Le nombre de niveaux d'archive incorporées qui peuvent être analysés. Par exemple, Document MIME > archive ZIP > archive Office > contenu du document.

   Taille maximale

   Paramètre par défaut : **100**

   Taille maximale d'un fichier d'archive à analyser.

2. **Analyser les lecteurs amovibles**

Paramètre par défaut : **Désactivé**

- **Lecteurs réseau mappés (à distance)**
- **Périphériques de stockage USB** (Par exemple, une clé USB ou des disques durs externes)
- **CD/DVD**

Remarque
L'analyse des lecteurs amovibles n'est pas prise en charge sous Linux.

Exclusions de protection

Les exclusions de protection vous permettent d'éliminer les faux positifs lorsqu'un programme fiable est considéré comme étant un ransomware ou un malware. Vous pouvez définir des éléments fiables et bloqués en les ajoutant à la liste des exclusions de la protection.

© Acronis International GmbH, 2003-2026

Dans la liste des éléments de confiance, vous pouvez ajouter des fichiers, des processus et des dossiers afin qu'ils soient considérés comme sûrs par le système, ce qui empêchera toute détection future les concernant.

Dans la liste des éléments bloqués, vous pouvez ajouter des processus et des hachages. Cette option garantit que ces processus seront bloqués et que votre ressource sera sécurisée.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Élément exclu de la protection	Bloqué	Fiable
Hachage	Lorsqu'un hachage est ajouté à la liste des éléments bloqués, le système arrête le processus en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est bloqué.	Lorsqu'un hachage est ajouté à la liste des éléments fiables, le système connaît les processus que la surveillance doit ignorer en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est considéré comme fiable et est exclu de la surveillance.
Processus	Lorsqu'un processus est ajouté à la liste des éléments bloqués, le système sait que ces processus doivent être surveillés et ces derniers sont toujours bloqués. Par exemple, si vous ajoutez ce chemin **C:\Users\user1\application\nppInstaller.exe** à la liste des éléments bloqués, ce processus spécifique sera bloqué, et lorsque vous essaierez de l'ouvrir, il ne sera pas autorisé à démarrer.	Lorsqu'un processus est ajouté à la liste des éléments fiables, le système exclut ce processus de la surveillance. Par exemple, si vous ajoutez ce chemin : `C:\Users\user1\application\nppInstaller.exe`, ce processus spécifique sera exclu de la surveillance, et l'antivirus n'interférera pas avec ce processus. Si vous ajoutez cette expression : `C:\Users\user1\application\*.exe`, tous les processus dans le dossier `application` seront exclus. **Remarque** Les processus signés par Microsoft sont toujours fiables.
Fichier/dossier		Lorsqu'un fichier ou un dossier est ajouté à la liste des éléments fiables, le système sait que ces fichiers ou dossiers doivent toujours être

© Acronis International GmbH, 2003-2026

Élément exclu de la protection	Bloqué	Fiable
		considérés comme étant fiables, et qu'ils n'ont pas besoin d'être analysés/surveillés.

Pour indiquer les éléments toujours fiables

1. Ouvrez le plan de protection pour le modifier.
   Par exemple, cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions**.
   La fenêtre **Exclusions de protection** s'affiche.
4. Dans la section **Éléments de confiance**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour définir des fichiers, dossiers ou processus comme étant fiables, sélectionnez l'option **Fichier/dossier/processus**. La fenêtre **Ajouter un fichier/dossier/processus** s'ouvre.
     - Dans le champ **Fichier/dossier/processus**, saisissez le chemin d'accès de chaque processus, dossier ou fichier sur une nouvelle ligne.
     - Cochez la case **Ajouter en tant que fichier/dossier** pour définir le fichier/dossier comme étant fiable.
       Exemples de description de dossier : `D:\folder\`, `/home/Folder/folder2`, `F:\`
     - Cochez la case **Ajouter en tant que processus** pour définir un processus comme étant fiable. Les processus sélectionnés seront exclus de la surveillance.

       Vous pouvez spécifier le chemin d'accès complet à un processus ou utiliser un caractère générique. Par exemple, pour exclure tous les processus dans le dossier `Temp`, vous pouvez entrer `C:\Windows\Temp\*.exe`.

       Les chemins d'accès du réseau local sont pris en charge. Par exemple, `\\localhost\folderpath\file.exe`
   - Pour ajouter des hachages MD5 à la liste des éléments de confiance, sélectionnez l'option **Hachage**. La fenêtre **Ajoutez le hachage** s'ouvre.
     - Vous pouvez insérer ici des hachages MD5 sur des lignes séparées afin qu'ils soient inclus comme éléments fiables dans la liste Exclusions de protection. Sur la base de ces hachages, Cyber Protection exclura de la surveillance les processus qu'ils décrivent.
5. [Facultatif] Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre modification dans la liste des éléments de confiance. Par exemple, raisons et objectifs de l'exclusion, horodatages, etc.

© Acronis International GmbH, 2003-2026

Remarque
Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

6. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Pour indiquer les éléments toujours bloqués

1. Ouvrez le plan de protection.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions de protection**.
   La fenêtre **Exclusions de protection** s'affiche.
4. Dans la section **Éléments bloqués**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour bloquer des processus, sélectionnez l'option **Processus**. La fenêtre **Ajouter un processus** s'ouvre.
     - Dans le champ **Processus**, saisissez le chemin d'accès de chaque processus sur une nouvelle ligne.

     Remarque
     Ces processus ne pourront pas démarrer tant qu'Active Protection sera activé sur la machine.

   - Pour bloquer des hachages, sélectionnez l'option **Hachage**. La fenêtre **Ajoutez le hachage** s'ouvre.
     - Dans le champ **Hachage**, saisissez le hachage de chaque processus sur une nouvelle ligne.
5. [Facultatif]
   Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre changement dans la liste des éléments bloqués. Par exemple, raisons et objectifs de l'exclusion, horodatages, etc.

   Remarque
   Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

6. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Utilisation de caractères génériques pour définir des exclusions

Pour définir des exclusions, vous pouvez utiliser les caractères génériques * et ?. L'astérisque (*) remplace zéro ou plusieurs caractères. Le point d'interrogation (?) remplace exactement un caractère. Les variables d'environnement, telles que `%AppData%`, ne peuvent pas être utilisées.

Vous pouvez utiliser un caractère générique (*) pour ajouter des éléments aux listes d'exclusion.

- Les caractères génériques peuvent être utilisés au milieu ou à la fin d'une description.

© Acronis International GmbH, 2003-2026

Exemple des caractères génériques acceptés dans des descriptions :

C:*.pdf

D:\dossiers\fichier.*

C:\Users*\AppData\Roaming

- Les caractères génériques ne peuvent pas être utilisés au début d'une description.

Exemple des caractères génériques non acceptés dans des descriptions :

*.docx

*:\dossier\

Utilisation de variables pour définir des exclusions

Vous pouvez utiliser des variables pour ajouter des éléments à la liste Exclusions de protection, avec les restrictions suivantes :

- Pour Windows, seules les variables SYSTEM sont prises en charge. Les variables propres à l'utilisateur, par exemple %USERNAME% ou %APPDATA% ne sont pas prises en charge. Les variables avec {username} ne sont pas prises en charge. Pour plus d'informations, voir https://ss64.com/nt/syntax-variables.html.
- Pour macOS, les variables d'environnement ne sont pas prises en charge.
- Pour Linux, les variables d'environnement ne sont pas prises en charge.

Exemples de formats pris en charge :

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Paramètres personnalisés

Dans certains cas, l'équipe de support peut vous aider à résoudre des problèmes en vous demandant de modifier les paramètres du plan de protection.

Avertissement !
Utilisez les **Paramètres personnalisés** uniquement selon les instructions de l'équipe de support. L'ajout d'un paramètre personnalisé incorrect peut avoir un impact négatif sur votre ressource, et le fournisseur de services ne pourra pas être tenu responsable.

Pour configurer les paramètres personnalisés

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Paramètres personnalisés**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Paramètres personnalisés**, cliquez sur **Ajouter**.
4. Dans le champ de valeur, entrez le paramètre personnalisé fourni par l'équipe de support.
5. Configurez le bouton **Vrai/Faux** comme indiqué par l'équipe de support.
6. Cliquez sur la coche à droite pour enregistrer le paramètre personnalisé.
7. Dans la boîte de dialogue **Ajouter un paramètre personnalisé**, cliquez sur **Ajouter**.
8. Cliquez sur **Terminé**.

Le paramètre personnalisé est maintenant appliqué au plan de protection.

Application potentiellement indésirable

Les applications indésirables sont des applications que vous auriez pu installer sur vos ressources de manière involontaire. Vous pouvez configurer les actions que le système exécutera lorsqu'il détectera des applications potentiellement indésirables. De cette manière, vous pouvez protéger vos ressources contre des logiciels qui peuvent réduire leurs performances, empêcher l'affichage de publicités non désirées et de pister l'utilisation d'internet dans le but de vendre des données à des tiers.

Paramètre par défaut : **Activé**.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

- Dans la licence basée sur la solution, la fonctionnalité est disponible uniquement avec l'élément d'offre Postes de travail sous la licence Protection Ultime.
- Dans la licence basée sur le service, la fonctionnalité est disponible avec l'élément d'offre Terminaux sous le service Detection and Response.

Pour configurer des actions contre les applications potentiellement indésirables

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Application potentiellement indésirable**.
3. Dans la liste déroulante **Action sur la détection**, sélectionnez l'une des options suivantes :

   Paramètre par défaut : **Bloquer et notifier**

   - **Notifier uniquement**
   - **Bloquer et notifier**
   - **Quarantaine**
4. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Active Protection dans l'édition Cyber Backup Standard

Dans Cyber Backup Standard Edition, Active Protection est un module distinct du plan de protection. Par conséquent, il peut être configuré différemment et appliqué à différents terminaux ou groupes de terminaux.

Dans toutes les autres éditions du service de cyberprotection, Active Protection fait partie du module **Antivirus et antimalware** du plan de protection.

Paramètre par défaut : **Activé**.

Remarque
Un agent de protection doit être installé sur la machine protégée. Pour plus d'informations sur les fonctionnalités et systèmes d'exploitation pris en charge, voir "Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware" (p. 1164).

Fonctionnement

Active Protection surveille les processus en cours d'exécution sur la machine protégée. Lorsqu'un processus tiers essaye de chiffrer des fichiers ou de miner de la cryptomonnaie, Active Protection génère une alerte et exécute des actions supplémentaires précisées dans le plan de protection.

Par ailleurs, Active Protection empêche les modifications non autorisées des propres processus du logiciel de sauvegarde, de ses enregistrements du registre, et de ses fichiers exécutables et de configuration, ainsi que des sauvegardes contenues dans les dossiers locaux.

Pour identifier les processus malveillants, Active Protection utilise des heuristiques comportementales. Active Protection compare la chaîne d'actions réalisées par un processus avec la chaîne d'événements enregistrée dans la base de données des schémas de comportement malveillants. Cette approche permet à Active Protection de détecter de nouveaux malware grâce à leur comportement typique.

Paramètres d'Active Protection dans Cyber Backup Standard

Dans l'édition Cyber Backup Standard, vous pouvez configurer les foncitonnalités Active Protection suivantes :

- Action lors de la détection
- Autoprotection
- Protection du dossier réseau
- Protection côté serveur
- Détection d'un processus de cryptominage
- Exclusions

© Acronis International GmbH, 2003-2026

Remarque
La fonctionnalité Active Protection pour Linux prend en charge les paramètres suivants : Action lors de la détection, Protection du dossier réseau et Exclusions. Le paramètre Protection du dossier réseau est toujours actif et n'est pas configurable.

Action lors de la détection

Dans la section **Action lors de la détection**, sélectionnez l'une des options disponibles :

- **Notifier uniquement**
  Le logiciel générera une alerte au sujet du processus suspecté d'activité de ransomware.
- **Arrêter le processus**
  Le logiciel générera une alerte et arrêtera le processus suspecté d'activité de ransomware.
- **Revenir à l'utilisation du cache**
  Le logiciel générera une alerte, arrêtera le processus et annulera les modifications apportées aux fichiers, à l'aide du cache de service.

Paramètre par défaut : **Revenir à l'utilisation du cache**.

Autoprotection

L'autoprotection empêche les modifications non autorisées des propres processus du logiciel, de ses enregistrements du registre et de ses fichiers exécutables et de configuration, ainsi que des sauvegardes contenues dans vos dossiers locaux.

Les administrateurs peuvent activer l'**Autoprotection** sans activer **Active Protection**.

Paramètre par défaut : **Activé**.

Remarque
L'autoprotection n'est pas prise en charge sous Linux.

Pour activer l'autoprotection

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Autoprotection**.
3. Utilisez le bouton-bascule **Autoprotection** pour l'activer.

Protection contre la désinstallation de l'agent

L'option **Protection contre la désinstallation de l'agent** empêche les utilisateurs ou les logiciels de désinstaller l'agent pour Windows, ou de modifier ses composants en dehors de la fenêtre de maintenance configurée.

Paramètre par défaut : **Activé**

Pour désactiver la protection contre la désinstallation de l'agent

© Acronis International GmbH, 2003-2026

Avertissement !
La désactivation de la **Protection contre la désinstallation de l'agent** expose les ressources protégées à des risques de sécurité.

1. Lorsque la fonctionnalité **Autoprotection** est activée, décochez la case **Protection contre la désinstallation de l'agent**.
2. Cliquez sur **Terminé**.

Remarque
Cette option n'empêche pas les mises à jour automatiques de l'agent Cyber Protection.

Chaque tentative de désinstallation ou de modification de l'agent de protection en dehors de la fenêtre de maintenance déclenche une alerte.

Un utilisateur administrateur peut examiner l'alerte et décider d'autoriser les modifications de l'agent pour 1 heure, ou configurer une fenêtre de maintenance d'une durée comprise entre 1 heure et 7 jours. Voir "Pour autoriser la modification d'un agent avec la protection contre la désinstallation activée" (p. 208).

Autoriser les processus à modifier des sauvegardes

Le paramètre **Autoriser des processus particuliers à modifier des sauvegardes** est disponible uniquement lorsque l'option **Autoprotection** est activée.

Elle s'applique aux fichiers dans les dossiers locaux avec les extensions suivantes :

- .tibx
- .tib
- .tia

Le paramètre **Autoriser des processus particuliers à modifier des sauvegardes** vous permet de spécifier les processus autorisés à modifier les fichiers de sauvegarde, même si ces fichiers sont protégés par l'autoprotection. Cela est utile, par exemple, si vous supprimez des fichiers de sauvegarde ou les déplacez vers un autre emplacement à l'aide d'un script.

Si ce paramètre est désactivé, les fichiers de sauvegarde ne peuvent être modifiés que par les processus signés par le fournisseur du logiciel de sauvegarde. Cela permet au logiciel d'appliquer des règles de rétention et de supprimer des sauvegardes lorsqu'un utilisateur le demande depuis l'interface Web. Les autres processus, qu'ils soient suspects ou non, ne peuvent pas modifier les sauvegardes.

Si ce paramètre est activé, vous pouvez autoriser d'autres processus à modifier les sauvegardes.

Paramètre par défaut : **Désactivé**.

Pour activer Autoriser des processus particuliers à modifier des sauvegardes

© Acronis International GmbH, 2003-2026

1. Lorsque la fonctionnalité d'**autoprotection** est activée, sélectionnez la case à cocher **Autoriser des processus particuliers à modifier des sauvegardes**.
2. Dans le champ **Processus de modification des sauvegardes**, cliquez sur **Ajouter**.
3. Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre de lecteur.
4. Cliquez sur la coche à droite pour enregistrer le processus.

Protection du dossier réseau

Le paramètre **Protéger vos dossiers réseau mappés en tant que lecteurs locaux** définit si Active Protection protège les dossiers réseau qui sont mappés en tant que lecteurs locaux contre les processus malveillants locaux.

Ce paramètre s'applique aux fichiers partagés via les protocoles SMB ou NFS.

Si un fichier était situé à l'origine sur un lecteur mappé, il ne peut pas être sauvegardé dans l'emplacement d'origine lorsqu'il est extrait du cache à l'aide de l'action **Revenir à l'utilisation du cache**. Il sera en fait sauvegardé dans le dossier indiqué dans ce paramètre. Le dossier par défaut est `C:\ProgramData\Acronis\Restored Network Files` pour Windows, et `Library/Application Support/Acronis/Restored Network Files/` pour macOS. Si ce dossier n'existe pas, il sera créé. Si vous souhaitez modifier ce chemin, choisissez un dossier local. Les dossiers réseau, y compris les dossiers sur les lecteurs mappés, ne sont pas pris en charge.

Paramètre par défaut : **Activé**.

Protection côté serveur

Cette fonctionnalité définit si Active Protection protège les dossiers réseau que vous partagez des connexions extérieures entrantes provenant d'autres serveurs du réseau et qui pourraient apporter des menaces.

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Paramètre par défaut : **Désactivé**.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Remarque
La protection côté serveur n'est pas prise en charge sous Linux.

Pour configurer des connexions fiables

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.

© Acronis International GmbH, 2003-2026

3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Fiable**.
5. Dans le champ **Connexions fiables**, cliquez sur **Ajouter** pour définir les connexions qui seront autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cliquez sur la coche à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Terminé**.

Pour configurer les connexions bloquées

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Protection côté serveur**.
3. Utilisez le bouton-bascule **Protection côté serveur** pour l'activer.
4. Sélectionnez l'onglet **Bloqué**.
5. Dans le champ **Connexions bloquées**, cliquez sur **Ajouter** pour définir les connexions qui ne seront pas autorisées à modifier les données.
6. Dans le champ **Nom d'ordinateur/Compte**, saisissez le nom de l'ordinateur et le compte de l'ordinateur sur lequel l'agent de protection est installé. Par exemple, `MyComputer\TestUser`.
7. Dans le champ **Nom de l'hôte**, saisissez le nom d'hôte de l'ordinateur autorisé à se connecter à l'ordinateur utilisant l'agent de protection.
8. Cochez la case à droite pour enregistrer la définition de connexion.
9. Cliquez sur **Terminé**.

Détection de cryptominage

Un malware de cryptominage réduit les performances des applications utiles, accroît la facture d'électricité, peut causer des plantages système et même endommager le matériel à cause d'un usage abusif. La fonctionnalité **Détection d'un processus de cryptominage** protège vos terminaux des malwares de cryptominage et évite toute utilisation non autorisée de ressources informatiques.

Les administrateurs peuvent activer la **Détection d'un processus de cryptominage** sans activer **Active Protection**. Paramètre par défaut : **Activé**.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Remarque
La détection de processus de cryptominage n'est pas prise en charge sous Linux.

© Acronis International GmbH, 2003-2026

Pour configurer la détection des processus de cryptominage

1. Dans la fenêtre **Créer un plan de protection**, développez le module **Protection antivirus et antimalware**.
2. Cliquez sur **Détection d'un processus de cryptominage**.
3. Utilisez le bouton-bascule **Détecter des processus de cryptominage** pour activer ou désactiver la fonctionnalité.
4. Sélectionnez l'opération à effectuer sur les processus suspectés d'activités de cryptominage :

   Paramètre par défaut : **Arrêter le processus**

   - **Notifier uniquement** : le logiciel génère une alerte.
   - **Arrêter le processus** : le logiciel génère une alerte et arrête le processus.
5. Cliquez sur **Terminé** pour appliquer les options sélectionnées à votre plan de protection.

Exclusions

Les exclusions de protection vous permettent d'éliminer les faux positifs lorsqu'un programme fiable est considéré comme étant un ransomware ou un malware. Vous pouvez définir des éléments fiables et bloqués en les ajoutant à la liste des exclusions de la protection.

Dans la liste des éléments de confiance, vous pouvez ajouter des fichiers, des processus et des dossiers afin qu'ils soient considérés comme sûrs par le système, ce qui empêchera toute détection future les concernant.

Dans la liste des éléments bloqués, vous pouvez ajouter des processus et des hachages. Cette option garantit que ces processus seront bloqués et que votre ressource sera sécurisée.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Élément exclu de la protection	Bloqué	Fiable
Hachage	Lorsqu'un hachage est ajouté à la liste des éléments bloqués, le système arrête le processus en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est bloqué.	Lorsqu'un hachage est ajouté à la liste des éléments fiables, le système connaît les processus que la surveillance doit ignorer en fonction du hachage fourni. Par exemple, lorsque vous ajoutez ce hachage MD5, 938c2cc0dcc05f2b68c4287040cfcf71, le processus associé à ce hachage est considéré comme fiable et est exclu de la surveillance.
Processus	Lorsqu'un processus est ajouté à la liste des éléments bloqués, le système	Lorsqu'un processus est ajouté à la liste des éléments fiables, le système

© Acronis International GmbH, 2003-2026

Élément exclu de la protection	Bloqué	Fiable
	sait que ces processus doivent être surveillés et ces derniers sont toujours bloqués. Par exemple, si vous ajoutez ce chemin **C:\Users\user1\application\nppInstaller.exe** à la liste des éléments bloqués, ce processus spécifique sera bloqué, et lorsque vous essaierez de l'ouvrir, il ne sera pas autorisé à démarrer.	exclut ce processus de la surveillance. Par exemple, si vous ajoutez ce chemin : `C:\Users\user1\application\nppInstaller.exe`, ce processus spécifique sera exclu de la surveillance, et l'antivirus n'interférera pas avec ce processus. Si vous ajoutez cette expression : `C:\Users\user1\application\*.exe`, tous les processus dans le dossier `application` seront exclus. **Remarque** Les processus signés par Microsoft sont toujours fiables.
Fichier/dossier		Lorsqu'un fichier ou un dossier est ajouté à la liste des éléments fiables, le système sait que ces fichiers ou dossiers doivent toujours être considérés comme étant fiables, et qu'ils n'ont pas besoin d'être analysés/surveillés.

Pour indiquer les éléments toujours fiables

1. Ouvrez le plan de protection pour le modifier.
   Par exemple, cliquez sur l'icône en forme de points de suspension (...) située à côté du nom du plan de protection, puis sélectionnez **Modifier**.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions**.
   La fenêtre **Exclusions de protection** s'affiche.
4. Dans la section **Éléments de confiance**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour définir des fichiers, dossiers ou processus comme étant fiables, sélectionnez l'option **Fichier/dossier/processus**. La fenêtre **Ajouter un fichier/dossier/processus** s'ouvre.
     - Dans le champ **Fichier/dossier/processus**, saisissez le chemin d'accès de chaque processus, dossier ou fichier sur une nouvelle ligne.
     - Cochez la case **Ajouter en tant que fichier/dossier** pour définir le fichier/dossier comme étant fiable.
       Exemples de description de dossier : `D:\folder\`, `/home/Folder/folder2`, `F:\`

© Acronis International GmbH, 2003-2026

- Cochez la case **Ajouter en tant que processus** pour définir un processus comme étant fiable. Les processus sélectionnés seront exclus de la surveillance.

  Vous pouvez spécifier le chemin d'accès complet à un processus ou utiliser un caractère générique. Par exemple, pour exclure tous les processus dans le dossier `Temp`, vous pouvez entrer `C:\Windows\Temp\*.exe`.

  Les chemins d'accès du réseau local sont pris en charge. Par exemple, `\\localhost\folderpath\file.exe`

- Pour ajouter des hachages MD5 à la liste des éléments de confiance, sélectionnez l'option **Hachage**. La fenêtre **Ajoutez le hachage** s'ouvre.
  - Vous pouvez insérer ici des hachages MD5 sur des lignes séparées afin qu'ils soient inclus comme éléments fiables dans la liste Exclusions de protection. Sur la base de ces hachages, Cyber Protection exclura de la surveillance les processus qu'ils décrivent.

5. [Facultatif] Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre modification dans la liste des éléments de confiance. Par exemple, raisons et objectifs de l'exclusion, horodatages, etc.

   Remarque
   Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

6. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Pour indiquer les éléments toujours bloqués

1. Ouvrez le plan de protection.
2. Développez le module **Protection contre les virus et les malwares**.
3. Sélectionnez l'option **Exclusions de protection**.
   La fenêtre **Exclusions de protection** s'affiche.
4. Dans la section **Éléments bloqués**, cliquez sur **Ajouter** pour sélectionner l'une des options disponibles :
   - Pour bloquer des processus, sélectionnez l'option **Processus**. La fenêtre **Ajouter un processus** s'ouvre.
     - Dans le champ **Processus**, saisissez le chemin d'accès de chaque processus sur une nouvelle ligne.

     Remarque
     Ces processus ne pourront pas démarrer tant qu'Active Protection sera activé sur la machine.

   - Pour bloquer des hachages, sélectionnez l'option **Hachage**. La fenêtre **Ajoutez le hachage** s'ouvre.
     - Dans le champ **Hachage**, saisissez le hachage de chaque processus sur une nouvelle ligne.
5. [Facultatif]
   Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre changement dans la liste des éléments bloqués. Par exemple, raisons et objectifs de

© Acronis International GmbH, 2003-2026

l'exclusion, horodatages, etc.

Remarque
Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

6. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Utilisation de caractères génériques pour définir des exclusions

Pour définir des exclusions, vous pouvez utiliser les caractères génériques * et ?. L'astérisque (*) remplace zéro ou plusieurs caractères. Le point d'interrogation (?) remplace exactement un caractère. Les variables d'environnement, telles que `%AppData%`, ne peuvent pas être utilisées.

Vous pouvez utiliser un caractère générique (*) pour ajouter des éléments aux listes d'exclusion.

- Les caractères génériques peuvent être utilisés au milieu ou à la fin d'une description.

Exemple des caractères génériques acceptés dans des descriptions :

C:*.pdf

D:\dossiers\fichier.*

C:\Users*\AppData\Roaming

- Les caractères génériques ne peuvent pas être utilisés au début d'une description.

Exemple des caractères génériques non acceptés dans des descriptions :

*.docx

*:\dossier\

Utilisation de variables pour définir des exclusions

Vous pouvez utiliser des variables pour ajouter des éléments à la liste Exclusions de protection, avec les restrictions suivantes :

- Pour Windows, seules les variables SYSTEM sont prises en charge. Les variables propres à l'utilisateur, par exemple %USERNAME% ou %APPDATA% ne sont pas prises en charge. Les variables avec {username} ne sont pas prises en charge. Pour plus d'informations, voir https://ss64.com/nt/syntax-variables.html.
- Pour macOS, les variables d'environnement ne sont pas prises en charge.
- Pour Linux, les variables d'environnement ne sont pas prises en charge.

Exemples de formats pris en charge :

- %WINDIR%\Media
- %public%

© Acronis International GmbH, 2003-2026

- %CommonProgramFiles%\Acronis\

Filtrage d'URL

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Les malwares sont souvent distribués par des sites malveillants ou infectés et utilisent la méthode d'infection dite Drive-by download.

La fonctionnalité de filtrage d'URL vous permet de protéger les ordinateurs des menaces comme les malwares ou le phishing, en provenance d'Internet. Vous pouvez protéger votre organisation en bloquant l'accès de l'utilisateur aux sites Web pouvant avoir un contenu malveillant.

La fonctionnalité de filtrage d'URL vous permet aussi de contrôler l'utilisation d'Internet afin de respecter les réglementations externes et les stratégies internes de l'entreprise. Vous pouvez configurer l'accès aux sites Web en fonction de la catégorie à laquelle ils appartiennent. Le filtrage d'URL prend actuellement en charge 44 catégories de sites Web et permet de gérer leur accès.

Actuellement, l'agent de protection vérifie les connexions HTTP/HTTPS sur les ordinateurs Windows.

La fonctionnalité de filtrage des URL nécessite une connexion Internet.

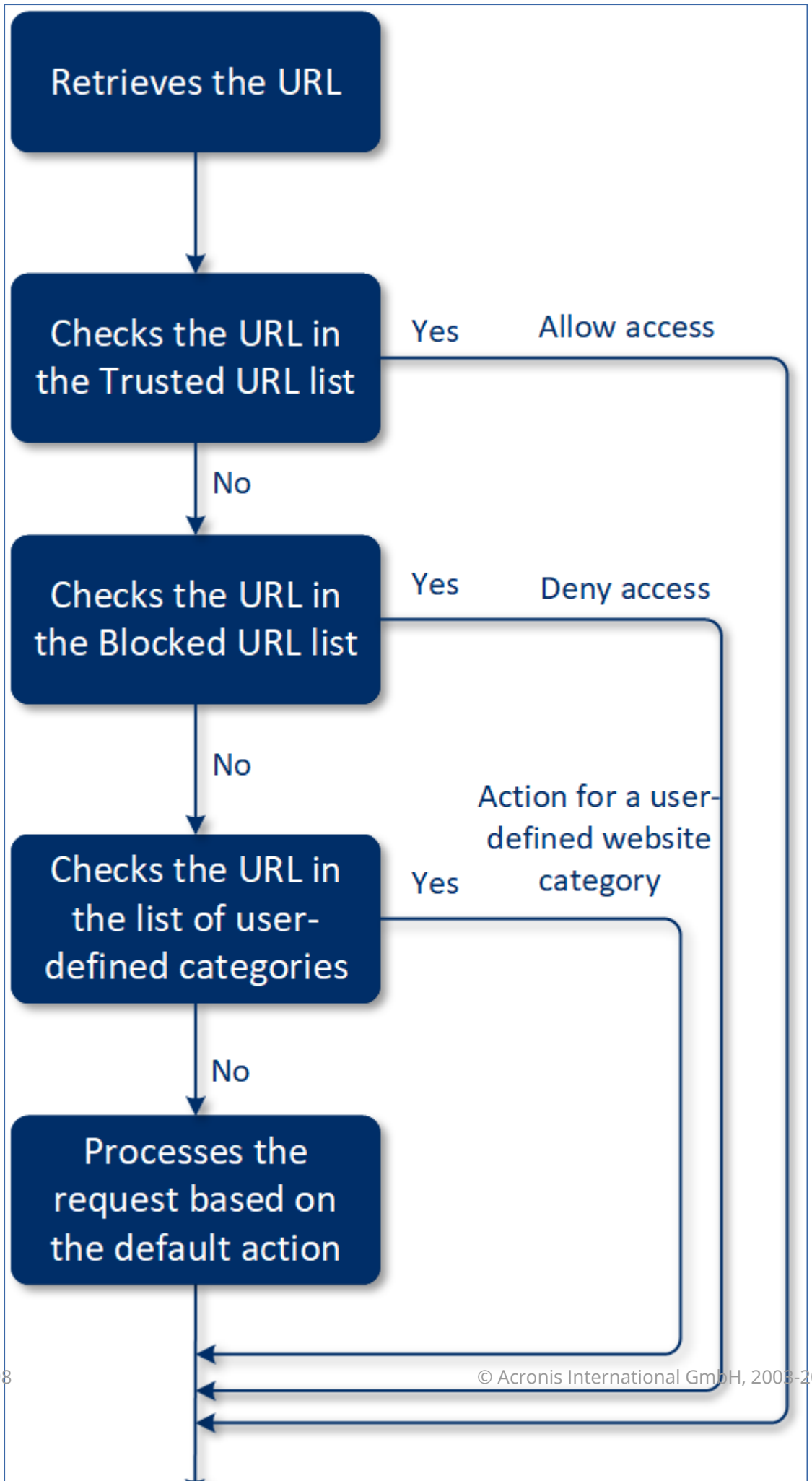
Remarque
Afin d'éviter d'éventuels soucis de compatibilité avec les versions 15.0.26692 et précédentes de l'agent de protection (version C21.03 HF1), la fonctionnalité de filtrage d'URL sera automatiquement désactivée si une autre solution antivirus est détectée, ou si le service de Centre de sécurité Windows n'est pas présent dans le système.
Dans les agents de protection ultérieurs, les problèmes de compatibilité sont résolus de sorte que le filtrage d'URL est toujours activé selon la stratégie.

Comment fonctionne le filtrage d'URL

Lorsque le filtrage d'URL est activé, il filtre tout le trafic réseau entrant sur la machine, y compris l'activité du navigateur et toute autre activité réseau se produisant en arrière-plan.

Par exemple, lorsqu'un utilisateur saisit une URL dans un navigateur, l'Intercepteur récupère le lien et l'envoie à l'agent de protection. L'agent reçoit l'URL, l'analyse, puis vérifie le verdict. L'Intercepteur redirige ensuite l'utilisateur vers la page affichant un message avec les actions disponibles pour poursuivre manuellement vers la page demandée.

© Acronis International GmbH, 2003-2026



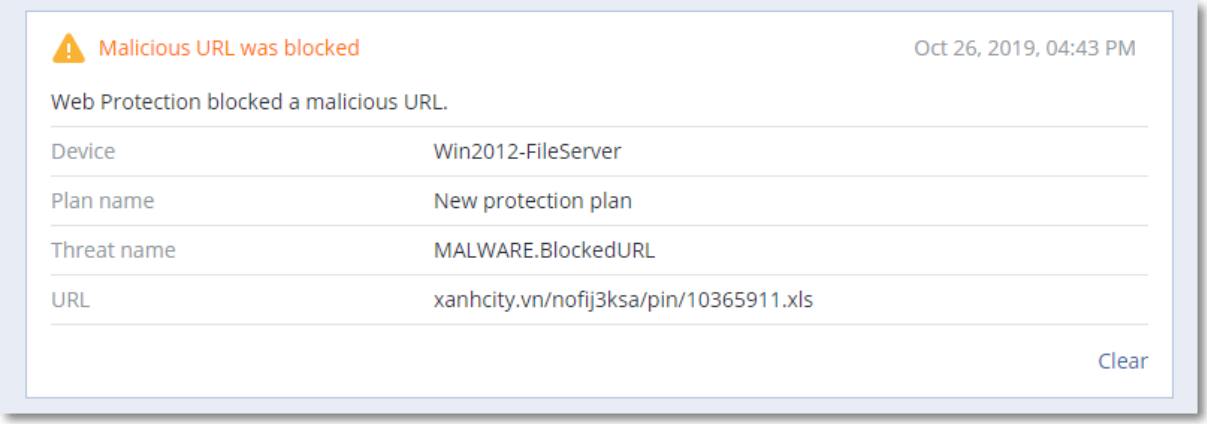
© Acronis International GmbH, 2003-2026

Configurer le filtrage d'URL

En général, la configuration du filtrage d'URL se compose des étapes suivantes :

1. Vous créez un plan de protection avec le module de **filtrage d'URL** activé.
2. Spécifiez les paramètres de filtrage d'URL.
3. Appliquez le plan de protection aux machines.

Pour consulter les URL qui ont été bloquées, accédez à **Surveillance** > **Alertes**.



Paramètres du filtrage d'URL

Définir les paramètres de filtrage d'URL vous permet de bloquer les sites Web nuisibles, de restreindre l'accès à des catégories indésirables et de n'autoriser que les domaines de confiance. Cela garantit une navigation plus sûre et la conformité avec les stratégies de l'entreprise.

Accès à un site Web malveillant

Spécifiez l'action à exécuter lorsqu'un utilisateur ouvre un site Web malveillant :

- **Notifier uniquement** : le logiciel génère une alerte sur le processus suspecté d'activité de ransomware.
- **Bloquer** : bloque l'accès au site Web malveillant. L'utilisateur ne peut pas accéder au site Web et une alerte d'avertissement est générée.
- **Toujours demander à l'utilisateur** : demande à l'utilisateur s'il souhaite quand même accéder au site Web ou revenir en arrière.

Catégories à filtrer

Il existe 44 catégories de sites Web pour lesquelles vous pouvez configurer l'accès :

- **Autoriser** – autoriser l'accès aux sites Web appartenant à la catégorie sélectionnée.
- **Refuser** – refuser l'accès aux sites Web appartenant à la catégorie sélectionnée.

Par défaut, toutes les catégories sont autorisées.

© Acronis International GmbH, 2003-2026

Afficher les notifications des URL bloquées sur la ressource protégée – si cette option est activée, les notifications relatives aux URL bloquées par catégorie s'affichent dans la zone de notification. Si un site Web comporte plusieurs sous-domaines, le système génère également des notifications pour chacun d'eux, ce qui peut entraîner un nombre élevé de notifications dans la zone de notification.

Remarque
Certaines catégories bloquées peuvent générer plusieurs notifications.

Vous pouvez trouver les descriptions des catégories dans le tableau ci-dessous :

	Catégorie de site Web	Description
1	**Publicités**	Cette catégorie couvre les domaines dont le but principal est de proposer des publicités.
2	**Forums**	Cette catégorie couvre les forums et les sites Web de type question–réponse. Elle ne couvre pas les sections particulières des sites Web des entreprises, dans lesquelles les clients posent des questions.
3	**Sites Web personnels**	Cette catégorie couvre les sites Web personnels et tous les types de blog : individuels, collectifs et même ceux des entreprises. Un blog est un journal intime publié sur Internet. Il se compose d'entrées (« publications ») généralement affichées en ordre chronologique inversé, de façon à ce que la publication la plus récente apparaisse en premier.
4	**Sites Web professionnels/d'entreprise**	C'est une vaste catégorie qui couvre les sites Web professionnels qui n'appartiennent habituellement à aucune autre catégorie.
5	**Logiciel d'ordinateur**	Cette catégorie couvre les sites Web qui proposent des logiciels d'ordinateur, généralement soit des logiciels open source, soit des gratuiciels, soit des partagiciels. Elle peut également couvrir certaines boutiques en ligne.
6	**Médicaments**	Cette catégorie couvre les sites Web liés aux médicaments, à l'alcool ou aux cigares, qui contiennent des discussions sur l'utilisation ou la vente de médicaments ou d'équipement médical légaux, d'alcool ou de produits à base de tabac. Veuillez noter que les drogues illicites sont couvertes dans la catégorie Drogues.
7	**Enseignement**	Cette catégorie couvre les sites Web appartenant aux institutions pédagogiques officielles, dont ceux en dehors des domaines .edu. Elle comprend également des sites Web éducatifs, tels qu'une encyclopédie.
8	**Divertissement**	Cette catégorie couvre les sites Web qui apportent des

© Acronis International GmbH, 2003-2026

		informations liées aux activités artistiques et aux musées, ainsi que les sites qui évaluent ou notent du contenu tel que des films, de la musique ou de l'art.
9	**Partage de fichiers**	Cette catégorie couvre les sites Web de partage de fichiers, où un utilisateur peut transférer des fichiers et les partager avec d'autres. Elle couvre également les sites Web de partage BitTorrent et les traqueurs BitTorrent.
10	**Finance**	Cette catégorie couvre les sites Web appartenant à toutes les banques du monde qui proposent un accès en ligne. Certaines coopératives de crédit et autres institutions financières sont également prises en compte. Toutefois, certaines banques locales peuvent ne pas être prises en compte.
11	**Jeux d'argent**	Cette catégorie couvre les sites Web de jeux d'argent. Il s'agit des sites Web de type « casino en ligne » ou « loterie en ligne », qui nécessitent généralement un paiement avant qu'un utilisateur puisse parier de l'argent dans des jeux de roulette, poker, black jack ou similaires en ligne. Certains sont légitimes, ce qui signifie qu'il existe une chance de gagner ; d'autres sont frauduleux, ce qui signifie qu'il n'existe aucune chance de gagner. Les sites Web d'astuces et solutions pour les paris, qui décrivent les façons dont gagner de l'argent en pariant et sur les sites Web de loterie en ligne, sont également détectés.
12	**Jeux**	Cette catégorie couvre les sites Web qui proposent des jeux en ligne, généralement basés sur des applets Adobe Flash ou Java. La détection ne couvre pas le fait que le jeu soit gratuit ou nécessite un abonnement ; les sites Web de style casino sont toutefois détectés sous la catégorie Jeux d'argent. Cette catégorie ne prend pas en compte : • Les sites Web officiels des sociétés qui développent des jeux vidéos (à moins qu'ils ne produisent des jeux en ligne) • Les sites Web de discussion sur les jeux • Les sites Web sur lesquels vous pouvez télécharger des jeux qui ne sont pas des jeux en ligne (certains sont couverts dans la catégorie Activités illégales) • Les jeux qui nécessitent qu'un utilisateur télécharge et exécute un fichier exécutable, comme World of Warcraft ; ceux-ci peuvent être évités par divers moyens, comme un pare-feu
13	**Gouvernement**	Cette catégorie couvre les sites Web gouvernementaux, dont les sites des institutions et services gouvernementaux et des ambassades.
14	**Piratage**	Cette catégorie couvre les sites Web qui contiennent des outils

© Acronis International GmbH, 2003-2026

		de piratage, des articles sur le sujet, et des plates-formes de discussion pour pirates. Elle couvre également les exploitations d'offres de sites Web pour des plates-formes courantes, qui facilitent le piratage de compte Facebook ou Gmail.
15	**Activités illégales**	Il s'agit d'une vaste catégorie liée au contenu haineux, violent ou raciste, qui a pour but de bloquer les catégories suivantes des sites Web : • Sites Web appartenant à des organisations terroristes • Sites Web au contenu raciste ou xénophobe • Sites Web traitant de sports agressifs, et/ou faisant la promotion de la violence
16	**Santé et forme physique**	Cette catégorie couvre les sites Web associés aux institutions médicales, ceux liés à la prévention et au traitement des maladies, et ceux qui apportent des informations sur la perte de poids, les régimes, les stéroïdes, les anabolisants ou les HCH, ainsi que les sites Web fournissant des informations concernant la chirurgie esthétique.
17	**Loisirs**	Cette catégorie couvre les sites Web qui présentent des ressources liées aux activités généralement réalisées pendant le temps libre d'un individu, comme les collections, les travaux manuels et le vélo.
18	**Hébergement Web**	Cette catégorie couvre les services gratuits et commerciaux d'hébergement de sites Web, qui permettent à des particuliers et à des organisations de créer et publier des pages Web.
19	**Téléchargements illégaux**	Cette catégorie couvre les sites Web liés au piratage de logiciels, y compris : • Les sites Web traqueurs pair à pair (BitTorrent, emule, DC++) connus pour aider à distribuer du contenu protégé sans le consentement du détenteur des droits d'auteur • Les sites Web et forums de discussion de warez (logiciel commercial piraté) • Les sites Web qui fournissent aux utilisateurs des cracks, des générateurs de clés et des numéros de série destinés à faciliterl'utilisation illégale d'un logiciel Il se peut également que certains de ces sites Websoient détectés dans la catégorie pornographie ou alcool/cigares, étant donné qu'ils utilisent souvent des publicités pornographiques ou pour l'alcool pour gagner de l'argent.
20	**Messagerie instantanée**	Cette catégorie couvre les sites Web de messagerie et de chat qui permettent aux utilisateurs de discuter en temps réel. Elle détectera également yahoo.com et gmail.com, étant donné que

© Acronis International GmbH, 2003-2026

		les deux comprennent un service de messagerie intégré.
21	**Emplois**	Cette catégorie couvre les sites Web qui présentent des tableaux d'offres d'emploi, des petites annonces d'emploi et des opportunités de carrière, ainsi que des agrégateurs de tels services. Elle ne couvre pas les agences de recrutement ou les pages d'offres d'emploi sur les sites Web habituels des entreprises.
22	**Contenu adulte**	Cette catégorie couvre le contenu étiqueté par un créateur de site Web comme destiné à un public adulte. Elle couvre une grande variété de sites Web, du Kama Sutra aux sites Web d'éducation sexuelle, en passant par la pornographie « dure ».
23	**Drogues**	Cette catégorie couvre les sites Web qui partagent des informations sur les drogues à usage récréatif et illégales. Elle couvre également les sites Web traitant des drogues en développement ou dont l'utilisation se répand.
24	**Actualités**	Cette catégorie couvre les sites Web d'actualités contenant du texte et des vidéos. Elle s'efforce de couvrir les sites Web d'actualités aussi bien mondiales que locales ; toutefois, il se peut que certains petits sites Web d'actualités locales ne soient pas couverts.
25	**Rencontres en ligne**	Cette catégorie couvre les sites Web de rencontres en ligne (gratuits et payants) où les utilisateurs peuvent rechercher des personnes à l'aide de certains critères. Ils peuvent également publier leur profil pour que d'autres puissent les trouver. Cette catégorie comprend les sites Web de rencontres en ligne aussi bien gratuits que payants. La plupart des réseaux sociaux populaires pouvant également être utilisés comme des sites Web de rencontres en ligne, certains sites Web populaires comme Facebook sont également détectés dans cette catégorie. Nous vous recommandons d'utiliser cette catégorie avec la catégorie Réseaux sociaux.
26	**Paiements en ligne**	Cette catégorie couvre les sites Web proposant des paiements ou des transferts d'argent. Elle détecte les sites Web de paiement populaires tels que PayPal ou Moneybookers. Elle détecte également de façon heuristique les pages Web des sites Web habituels demandant des informations de carte de crédit, ce qui permet de détecter des boutiques en ligne masquées, inconnues ou illégales.
27	**Partage de photos**	Cette catégorie couvre les sites Web de partage de photos dont le but principal est de permettre aux utilisateurs de transférer et partager des photos.

© Acronis International GmbH, 2003-2026

28	**Boutiques en ligne**	Cette catégorie couvre les boutiques en ligne connues. Un site Web est considéré comme étant une boutique en ligne s'il vend des biens ou des services en ligne.
29	**Pornographie**	Cette catégorie couvre les sites Web contenant du contenu érotique et de la pornographie. Elle comprend les sites Web gratuits aussi bien que payants. Elle couvre les sites Web qui fournissent des images, histoires et vidéos, et détecte également le contenu pornographique des sites Web à contenu mixte.
30	**Portails**	Cette catégorie couvre les sites Web qui agrègent les informations de multiples sources et domaines, et qui proposent généralement des fonctionnalités telles que des moteurs de recherche, un courrier électronique, des actualités et des informations de divertissement.
31	**Radio**	Cette catégorie couvre les sites Web qui offrent des services de streaming de musique sur Internet, allant des stations de Web radio aux sites proposant du contenu audio à la demande (gratuit ou payant).
32	**Religion**	Cette catégorie couvre les sites Web qui promeuvent une religion ou une secte. Elle couvre également les forums de discussion associés à une ou plusieurs religion(s).
33	**Moteurs de recherche**	Cette catégorie couvre les sites Web de moteurs de recherche tels que Google, Yahoo et Bing.
34	**Réseaux sociaux**	Cette catégorie couvre les sites Web de réseaux sociaux. Elle comprend MySpace.com, Facebook.com, Bebo.com, etc. Toutefois, les réseaux sociaux spécialisés, comme YouTube.com, seront répertoriés dans la catégorie Vidéo/Photo.
35	**Sport**	Cette catégorie couvre les sites Web qui proposent des informations, actualités et tutoriels liés au sport.
36	**Suicide**	Cette catégorie couvre les sites Web qui promeuvent, proposent ou défendent le suicide. Elle ne couvre pas les cliniques de prévention du suicide.
37	**Journaux à scandale**	Cette catégorie est principalement conçue pour la pornographie « douce » et les sites Web « people ». Il se peut que cette catégorie répertorie des sous-catégories de nombreux sites Web d'actualités de style journaux à scandale. La détection de cette catégorie se base également sur des heuristiques.
38	**Perte de temps**	Cette catégorie couvre les sites Web sur lesquels les individus ont tendance à passer beaucoup de temps. Cela peut comprendre des sites Web d'autres catégories telles que les réseaux sociaux ou le divertissement.

© Acronis International GmbH, 2003-2026

39	**Voyage**	Cette catégorie couvre les sites Web qui proposent des offres de voyage et d'équipement de voyage, ainsi que des critiques et notations de destinations de voyage.
40	**Vidéos**	Cette catégorie couvre les sites Web qui hébergent diverses photos ou vidéos, qu'elles soient transférées par les utilisateurs ou fournies par divers fournisseurs de contenu. Elle comprend des sites Web tels que YouTube, Metacafe, Google Video, et des sites Web de photo tels que Picasa ou Flickr. Elle détectera également des vidéos incorporées dans d'autres sites Web ou blogs.
41	**Dessins animés violents**	Cette catégorie couvre les sites Web qui partagent et proposent des dessins animés ou manga qui peuvent être inadaptés aux mineurs en raison de contenu violent ou sexuel, ou de langage explicite, ou qui permettent d'en discuter. Elle ne couvre pas les sites Web proposant des dessins animés traditionnels tels que « Tom et Jerry ».
42	**Armes**	Cette catégorie couvre les sites Web qui proposent la vente, l'échange, la fabrication ou l'utilisation d'armes. Elle couvre également le matériel de chasse et l'utilisation d'armes à air comprimé et à balles BB, ainsi que les armes de corps-à-corps.
43	**E-mail**	Cette catégorie couvre les sites Web qui fournissent des fonctionnalités d'e-mail en tant qu'application Web.
44	**Proxy Web**	Cette catégorie couvre les sites Web qui fournissent des services proxy. Il s'agit d'un site Web de type « navigateur dans un navigateur », lorsqu'un utilisateur ouvre une page Web, saisit l'URL demandée dans un formulaire, puis clique sur « Envoyer ». Le site de proxy Web télécharge la vraie page et l'affiche dans le navigateur de l'utilisateur. Ce type est détecté (et peut nécessiter d'être bloqué) pour les raisons suivantes : • Pour la navigation anonyme. Étant donné que les requêtes vers le serveur Web de destination transitent par le serveur proxy, seule l'adresse IP de ce dernier est visible. Si les administrateurs du serveur tentent de remonter jusqu'à l'utilisateur, la piste s'arrêtera au niveau du proxy Web, qui peut ou non conserver les journaux nécessaires pour identifier l'utilisateur d'origine. • Pour l'usurpation d'identité liée à l'emplacement. Les adresses IP des utilisateurs sont souvent utilisées pour établir le profil du service par emplacement de la source (certains sites Web gouvernementaux nationaux peuvent n'être accessibles que depuis des adresses IP locales), et l'utilisation

© Acronis International GmbH, 2003-2026

		de ces services peut aider l'utilisateur à usurper son véritable emplacement. • Pour accéder à du contenu interdit. Si un simple filtre d'URL est utilisé, il ne verra que les URL de proxy Web, et pas les véritables serveurs sur lesquels l'utilisateur se rend. • Pour éviter d'être surveillé par l'entreprise. Il se peut qu'une règle d'entreprise implique de surveiller l'utilisation Internet des employés. En accédant à tout via un proxy Web, il se peut qu'un utilisateur échappe à la surveillance, ce qui fournira des informations incorrectes. Étant donné que le SDK analyse la page HTML (si elle est fournie), et pas uniquement les URL, le SDK pourratoujours détecter le contenu de certaines catégories. Il est toutefois impossible d'éviter d'autres motifs simplement en utilisant le SDK.

Exclusions d'URL

Les URL considérées comme fiables peuvent être ajoutées à la liste des domaines de confiance. Les URL représentant une menace peuvent être ajoutées à la liste des domaines bloqués.

Pour spécifier les URL qui seront toujours considérées comme fiables

1. Dans la section de filtrage d'URL d'un plan de protection, cliquez sur **Exclusions**.
   La fenêtre **Exclusions d'URL** s'ouvre.
2. Dans la section **Éléments de confiance**, cliquez sur **Ajouter**, puis sélectionnez l'une des options disponibles.
   - **Domaine** — si vous sélectionnez cette option, la fenêtre **Ajouter un domaine** s'affiche.
     - Dans le champ **Domaine**, saisissez chaque domaine sur une nouvelle ligne.
   - **Processus** — si vous sélectionnez cette option, la fenêtre **Ajouter un processus** s'affiche.
     - Dans le champ **Processus**, saisissez le chemin d'accès de chaque processus sur une nouvelle ligne.
3. [Facultatif] Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre modification dans la liste des éléments de confiance. Par exemple, raisons et objectifs de l'exclusion, horodatages, etc.

   Remarque
   Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

4. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Pour indiquer les URL qui seront toujours bloquées

© Acronis International GmbH, 2003-2026

1. Dans la section de filtrage d'URL d'un plan de protection, cliquez sur **Exclusions**.
   La fenêtre **Exclusions d'URL** s'ouvre.
2. Dans la section **Éléments bloqués**, cliquez sur **Ajouter**, puis cliquez sur **Domaine**.
3. Dans le champ **Domaine**, saisissez chaque domaine sur une nouvelle ligne.

   Remarque
   Les chemins d'accès du réseau local sont pris en charge. Par exemple, `\\localhost\folderpath\file.exe`.

4. [Facultatif] Dans le champ **Description**, entrez une brève description, afin que vous puissiez reconnaître votre changement dans la liste des éléments bloqués. Par exemple, raisons et objectifs de l'exclusion, horodatages, etc.

   Remarque
   Si plusieurs éléments sont ajoutés dans une même entrée, il ne peut y avoir qu'un seul commentaire saisi pour les différents éléments.

5. Cliquez sur **Ajouter**, puis cliquez sur **Terminé**.

Utilisation de caractères génériques pour définir des exclusions

Vous pouvez utiliser le caractère générique astérisque (*) pour ajouter des processus de confiance aux listes d'exclusion. Les astérisques remplacent zéro ou plusieurs caractères et peuvent être utilisés au milieu ou à la fin d'une description. Ils ne peuvent pas être utilisés au début d'une description. Les variables d'environnement, telles que %AppData%, ne peuvent pas être utilisées.

Descriptions valides utilisant des caractères génériques :

- `C:\*.exe`
- `D:\folders\file.*`
- `C:\Users\*\AppData\Roaming\*.exe`

Descriptions invalides :

- `*.exe`
- `*:\folder\process.exe`

Protection du navigateur

Activez la protection du navigateur pour installer l'extension de filtrage d'URL sur votre navigateur.

L'extension de filtrage d'URL améliore le filtrage d'URL en supportant les sites Web HTTPS qui utilisent des protocoles modernes tels que HTTP/2 et QUIC. Elle garantit que le filtrage Web reste précis et fiable même avec des types de trafic Internet plus récents et plus rapides.

L'extension de filtrage d'URL applique les mêmes règles définies dans vos paramètres de filtrage d'URL pour accéder aux sites Web malveillants. Voir "Accès à un site Web malveillant" (p. 1199).

© Acronis International GmbH, 2003-2026

Installez l'extension de filtrage d'URL

Remarque
L'extension de filtrage d'URL est disponible uniquement pour Google Chrome, version 130 ou ultérieure.

1. Activez l'interrupteur **protection du navigateur**.
2. Attendez que l'alerte **Protection du navigateur est presque prête** apparaisse.
3. Redémarrez votre navigateur pour terminer l'installation.
4. [Facultatif] Dans la fenêtre pop-up de l'extension de filtrage d'URL, activez l'interrupteur **collecte de journaux**.
   Cela permettra la collecte de journaux vers le stockage du navigateur.

   Remarque
   La capacité de stockage par défaut du navigateur est de 50 Mo. Lorsque le stockage du navigateur est plein, les journaux les plus anciens seront supprimés

L'extension de filtrage d'URL est installée et vous pouvez collecter des journaux pour surveiller ses performances.

Antivirus Microsoft Defender et Microsoft Security Essentials

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Antivirus Microsoft Defender

L'antivirus Microsoft Defender est un composant antimalware intégré à Microsoft Windows, qui est fourni à partir de Windows 8.

Le module Antivirus Microsoft Defender vous permet de configurer la stratégie de sécurité de l'antivirus Microsoft Defender et de suivre son état via la console Cyber Protect.

Ce module s'applique aux ressources sur lesquelles l'antivirus Microsoft Defender est installé.

© Acronis International GmbH, 2003-2026

Remarque
Si vous activez **Antivirus Microsoft Defender** pour la protection en temps réel, le module **Protection en temps réel** est automatiquement désactivé afin d'éviter les conflits. Les détections de virus/malware et la mise en quarantaine sont gérées par Microsoft Defender Antivirus, et tous les incidents EDR liés aux détections de virus/malware sont créés à partir des informations fournies par Microsoft Defender Antivirus. EDR inclut d'autres moteurs de détection qui peuvent créer d'autres types d'incidents sans l'intervention de Microsoft Defender Antivirus.

De même, si vous activez la **Protection en temps réel**, le module **Antivirus Microsoft Defender** est automatiquement désactivé.

Les paramètres de **protection contre les modifications** dans Windows doivent également être désactivés pour garantir le bon fonctionnement de l'Antivirus Microsoft Defender dans Cyber Protect Cloud. Pour plus d'informations, consultez cet article de la base de connaissances.

En outre, si **Moteur de comportement** ou **Protection antivirus et antimalware** sont désactivés dans le plan de protection lorsque **Endpoint Detection and Response (EDR)** est activé, cette fonctionnalité est également désactivée.

Microsoft Security Essentials

Microsoft Security Essentials est un composant antimalware intégré à Microsoft Windows, qui est fourni avec les versions antérieures à Windows 8.

Le module Microsoft Security Essentials vous permet de configurer la stratégie de sécurité de Microsoft Security Essentials et de suivre son état via la console Cyber Protect.

Ce module s'applique aux ressources sur lesquelles Microsoft Security Essentials est installé.

Les paramètres pour Microsoft Security Essentials sont similaires à ceux pour l'antivirus Microsoft Defender, mais vous ne pouvez pas configurer la protection en temps réel et ne pouvez pas définir d'exclusions via la console Cyber Protect.

Planifier l'analyse

Spécifiez la planification pour l'analyse planifiée.

Mode d'analyse :

- **Complète** : une vérification complète de tous les fichiers et dossiers en plus des éléments analysés lors de l'analyse rapide. Son exécution requiert plus de ressources machine comparativement à l'exécution de l'analyse rapide.
- **Rapide** : une vérification rapide des processus et dossiers en mémoire, dans lesquels se trouvent généralement les malwares. Son exécution requiert moins de ressources machine.

Définissez l'heure et le jour de la semaine pour l'exécution de l'analyse.

Analyse quotidienne rapide : définit l'heure de l'analyse quotidienne rapide.

En fonction de vos besoins, vous pouvez définir les options suivantes :

© Acronis International GmbH, 2003-2026

Démarrer l'analyse planifiée lorsque la machine est allumée, mais pas en cours d'utilisation

Examinez les dernières définitions de virus et de logiciel espion avant d'exécuter une analyse planifiée

Limiter l'utilisation du CPU lors de l'analyse à

Pour en savoir plus sur les paramètres de l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Actions par défaut

Définissez les actions par défaut à exécuter pour les menaces détectées selon leur niveau de gravité :

- **Nettoyer** : nettoyer le malware détecté sur une ressource.
- **Quarantaine** : placer le malware détecté en quarantaine, mais ne pas le supprimer.
- **Supprimer** : supprimer le malware détecté sur une ressource.
- **Autoriser** : ne pas supprimer le malware détecté, ni le mettre en quarantaine.
- **Défini par l'utilisateur** : un utilisateur sera invité à spécifier l'action à effectuer avec le malware détecté.
- **Aucune action** : aucune action ne sera effectuée.
- **Bloquer** : bloquer le malware détecté.

Pour en savoir plus sur les paramètres des actions par défaut pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings.

Protection en temps réel

Activez la **protection en temps réel** pour détecter les malwares et les empêcher de s'installer ou de s'exécuter sur des ressources.

Analyser tous les téléchargements : si cette option est sélectionnée, l'analyse est effectuée sur tous les fichiers téléchargés et sur toutes les pièces jointes.

Activer surveillance des comportements : si cette option est sélectionnée, la surveillance des comportements sera activée.

Analyser les fichiers réseau : si cette option est sélectionnée, les fichiers réseau seront analysés.

Autoriser une analyse complète sur des lecteurs réseau mappés : si cette option est sélectionnée, les lecteurs réseau mappés seront entièrement analysés.

Autoriser l'analyse des e-mails : si l'option est activée, le moteur procèdera à l'analyse syntaxique de la boîte aux lettres et des fichiers de messagerie, en fonction de leur format spécifique, afin d'analyser le corps des e-mails et les pièces jointes.

© Acronis International GmbH, 2003-2026

Pour en savoir plus sur les paramètres de protection en temps réel pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

Advanced

Spécifiez les paramètres d'analyse avancée :

- **Analyser les fichiers d'archive** : inclure les fichiers archivés, comme les fichiers .zip ou .rar, à l'analyse.
- **Analyser les lecteurs amovibles** : analyser les lecteurs amovibles lors d'une analyse complète.
- **Créer un point de restauration système** : dans certains cas, un fichier ou une entrée de registre important peut être supprimé alors qu'il s'agit d'un « faux positif ». Vous pourrez alors le ou la récupérer à partir d'un point de restauration.
- **Supprimer les fichiers mis en quarantaine après** : définir la période après laquelle les fichiers en quarantaine seront supprimés.
- **Envoyer automatiquement les échantillons de fichiers lorsqu'une analyse plus profonde est requise :**
  - **Toujours demander** : vous serez invité à confirmer avant l'envoi du fichier.
  - **Envoyer automatiquement tous les échantillons sécurisés** : la plupart des échantillons seront envoyés automatiquement, sauf les fichiers qui contiennent des informations personnelles. Ces fichiers nécessiteront une confirmation supplémentaire.
  - **Envoyer automatiquement tous les échantillons** : tous les échantillons seront automatiquement envoyés.
- **Désactiver l'interface utilisateur graphique de l'antivirus Windows Defender :** si cette option est sélectionnée, l'utilisateur de l'antivirus Windows Defender ne sera pas accessible à l'utilisateur. Vous pouvez gérer les règles relatives à l'antivirus Windows Defender via la console Cyber Protect.
- **MAPS (Microsoft Active Protection Service)** : communauté en ligne qui vous aide à choisir comment réagir face aux menaces potentielles.
  - **Je ne souhaite pas rejoindre MAPS** : aucune information ne sera envoyée à Microsoft au sujet des logiciels qui ont été détectés.
  - **Adhésion de base** : des informations de base seront envoyées à Microsoft au sujet des logiciels qui ont été détectés.
  - **Adhésion avancée** : des informations plus détaillées seront envoyées à Microsoft au sujet des logiciels qui ont été détectés.

  Pour en savoir plus, reportez-vous à l'article https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/ (en anglais).

Pour en savoir plus sur les paramètres avancés pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

© Acronis International GmbH, 2003-2026

Exclusions

Vous pouvez définir les fichiers et dossiers suivants afin de les exclure de l'analyse :

- **Processus :** n'importe quel fichier que le processus défini lit ou sur lequel il écrit sera exclu de l'analyse. Vous devez définir un chemin d'accès complet au fichier exécutable du processus.
- **Fichiers et dossiers :** les fichiers et dossiers spécifiés seront exclus de l'analyse. Vous devez définir un chemin d'accès complet au dossier ou au fichier, ou définir l'extension du fichier.

Pour en savoir plus sur les paramètres d'exclusion pour l'antivirus Microsoft Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

Gestion du pare-feu

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

La gestion du pare-feu vous permet de configurer facilement les paramètres de pare-feu sur les ressources protégées.

Dans Cyber Protect, cette fonctionnalité est fournie via un composant de pare-feu Microsoft Defender intégré de Microsoft Windows. Le pare-feu Microsoft Defender bloque le trafic réseau non autorisé entrant ou sortant de vos ressources.

La gestion du pare-feu s'applique à toutes les ressources sur lesquelles le pare-feu Microsoft Defender est installé.

Systèmes d'exploitation Windows compatibles

Les systèmes d'exploitation Windows suivants sont compatibles avec la gestion du pare-feu :

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server n'est pas compatible.

Activation et désactivation de la gestion du pare-feu

Vous pouvez activer la gestion du pare-feu lors de la création d'un plan de protection. Vous pouvez modifier un plan de protection existant afin d'activer ou de désactiver la gestion du pare-feu.

Activer ou désactiver la gestion du pare-feu

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Effectuez l'une des actions suivantes pour ouvrir le panneau du plan de protection :
   - Si vous souhaitez créer un plan de protection, sélectionnez un ordinateur à protéger, cliquez sur **Protection**, puis sur **Création d'un plan**.
   - Si vous souhaitez modifier un plan de protection existant, sélectionnez une machine protégée, cliquez sur **Protection**, sur les points de suspension (...) à côté du nom du plan de protection, puis sur **Modifier**.
3. Dans le panneau du plan de protection, accédez à la zone **Gestion du pare-feu**, et activez ou désactivez **Gestion du pare-feu**.
4. Effectuez l'une des actions suivantes pour appliquer vos modifications :
   - Si vous créez un plan de protection, cliquez sur **Créer**.
   - Si vous modifiez un plan de protection, cliquez sur **Enregistrer**.

Le **Statut du pare-feu Microsoft Defender** dans la zone **Gestion du pare-feu** du panneau du plan de protection s'affiche comme **Activé** ou **Désactivé**, selon que vous avez activé ou désactivé la gestion du pare-feu.

Vous pouvez également accéder au panneau du plan de protection depuis l'onglet Gestion. Toutefois, cette fonctionnalité n'est pas disponible dans toutes les éditions du service Cyber Protection.

Quarantaine

Le dossier `Quarantaine` est un dossier isolé stocké sur le disque dur d'un terminal protégé. Si la protection antivirus et antimalware détecte des fichiers suspects, ils sont placés dans ce dossier de quarantaine pour empêcher toute propagation ultérieure des menaces.

Dans l'onglet **Quarantaine** de la console Cyber Protection, vous pouvez examiner les fichiers suspects et potentiellement dangereux de tous les terminaux protégés, et décider de les supprimer ou de les restaurer.

Remarque
Les fichiers en quarantaine sont automatiquement supprimés si le terminal est supprimé de l'environnement.

Comment les fichiers arrivent-ils dans le dossier de quarantaine ?

1. Dans le plan de protection, sélectionnez **Quarantaine** comme action par défaut pour les fichiers infectés ou suspects.
   Pour savoir comment créer un plan de protection, voir "Création d'un plan de protection" (p. 244).
2. Pendant l'analyse, le module Protection antivirus et antimalware détecte les fichiers malveillants et les place dans le dossier `Quarantaine` sécurisé.

© Acronis International GmbH, 2003-2026

3. Le module met à jour la liste de quarantaine pour ajouter des informations sur les fichiers placés dans le dossier Quarantaine.

Remarque
Les fichiers sont supprimés automatiquement du dossier `Quarantaine` après la période définie dans le paramètre **Supprimer les fichiers mis en quarantaine après** du plan de protection. Voir "Paramètres de quarantaine" (p. 1175).

Gestion des fichiers mis en quarantaine

Pour gérer les fichiers placés en quarantaine, accédez à **Protection** > **Quarantaine**. La liste des fichiers placés en quarantaine sur tous les terminaux protégés contient les informations suivantes.

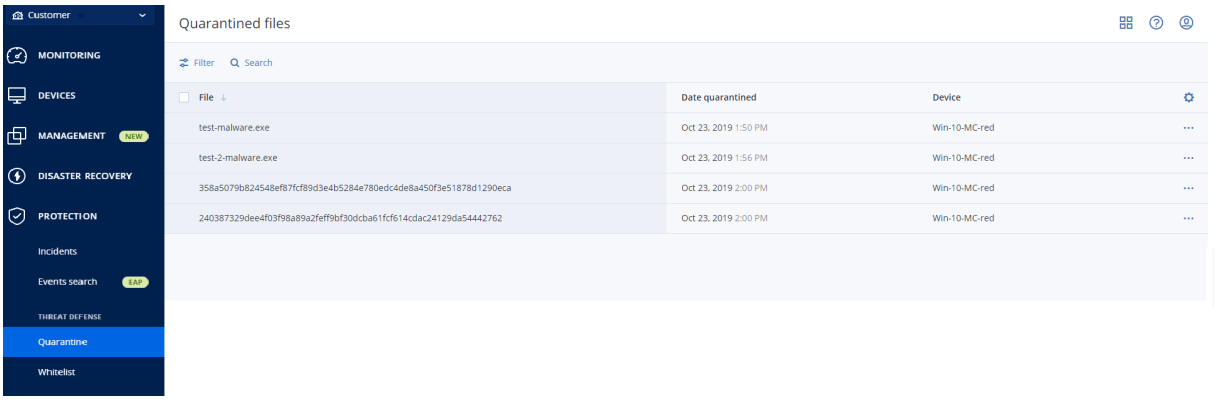
Nom	Description
Fichier	Nom du fichier mis en quarantaine.
Date de début de la mise en quarantaine	Date et heure auxquelles le fichier a été mis en quarantaine.
Terminal	Le terminal sur lequel le fichier infecté a été trouvé.
Nom de la menace	Le nom de la menace.
Plan de protection	Le plan de protection en vertu duquel le fichier suspect a été placé dans le dossier Quarantaine.

Vous pouvez effectuer les actions suivantes sur les fichiers placés en quarantaine :

- **Supprimer** : supprime définitivement un fichier mis en quarantaine de tous les ordinateurs. Vous pouvez supprimer tous les fichiers avec le même hachage de fichier. Vous pouvez restaurer tous les fichiers avec le même hachage de fichier. Regroupez les fichiers par hachage, sélectionnez les fichiers nécessaires, puis supprimez-les.
- **Restaurer** : restaure un fichier mis en quarantaine à son emplacement d'origine, sans aucune modification. Si un fichier de même nom existe dans l'emplacement d'origine, il est écrasé par le fichier restauré.

  Remarque
  Le fichier restauré est ajouté à la liste d'autorisation et ignoré lors des autres analyses antimalware.

© Acronis International GmbH, 2003-2026



Emplacement de quarantaine sur les machines

Voici la liste des emplacements par défaut pour les fichiers mis en quarantaine par système d'exploitation.

- Pour les ordinateurs Windows : `%programdata%\Acronis\NGMP\quarantine`
- Pour les ordinateurs Mac : `/Library/Application Support/Acronis/NGMP/quarantine`
- Pour les ordinateurs Linux : `/var/lib/Acronis/NGMP/quarantine`

L'emplacement de quarantaine est sous l'autoprotection du fournisseur de services.

Dossier personnalisé en libre-service et à la demande

Vous pouvez sélectionner des dossiers personnalisés dans la ressource et les analyser directement depuis le menu contextuel.

Pour accéder à l'analyse avec l'option Cyber Protect dans le menu contextuel

Pour les ressources avec antivirus et antimalware activés dans le plan de protection, cliquez avec le bouton droit sur les fichiers/dossiers que vous voulez analyser.

Remarque
Cette option est disponible uniquement pour les administrateurs de la ressource.

Liste blanche d'entreprise

Une solution antivirus peut identifier des applications spécifiques à l'entreprise comme étant suspectes. Pour éviter ces détections de faux positifs, les applications de confiance doivent être ajoutées manuellement à une liste blanche.

Remarque
La liste blanche d'entreprise n'affecte pas les analyses antimalware des sauvegardes.

Cyber Protection peut automatiser ce processus : les sauvegardes sont analysées par le module de protection antivirus et de protection antimalware, et les données analysées servent à identifier les

© Acronis International GmbH, 2003-2026

applications qui sont ensuite transférées vers la liste blanche, ce qui permet d'éviter les détections de faux positifs. De plus, la liste blanche à l'échelle de l'entreprise améliore les performances des analyses antimalware.

La liste blanche est créée pour chaque client, et se base uniquement sur les données de ce client.

La liste blanche peut être activée et désactivée. Lorsqu'elle est désactivée, les fichiers qui y sont ajoutés sont temporairement masqués.

Remarque
Seuls les comptes ayant le rôle d'administrateur (par exemple, administrateur Cyber Protection, administrateur d'entreprise, administrateur partenaire agissant pour le compte d'un administrateur d'entreprise, administrateur d'unité) peuvent configurer et gérer la liste blanche.

Cette fonctionnalité n'est pas disponible pour un compte administrateur en lecture seule ou un compte utilisateur.

Ajout automatique à la liste blanche

1. Exécutez l'analyse Cloud des sauvegardes sur au moins deux ordinateurs. Pour cela, utilisez les plans d'analyse des sauvegardes.
2. Dans les paramètres de liste blanche, activez le commutateur **Génération automatique d'une liste blanche**.

Ajout manuel à la liste blanche

Même lorsque le commutateur **Génération automatique d'une liste blanche** est désactivé, vous pouvez ajouter des fichiers manuellement.

1. Dans la console Cyber Protect, accédez à **Protection** > **Liste blanche**.
2. Cliquez sur **Ajouter un fichier**.
3. Indiquez le chemin d'accès au fichier, puis cliquez sur **Ajouter**.

Ajout de fichiers mis en quarantaine à la liste blanche

Vous pouvez ajouter des fichiers mis en quarantaine à la liste blanche.

1. Dans la console Cyber Protect, accédez à **Protection** > **Quarantaine**.
2. Sélectionnez un fichier mis en quarantaine, puis cliquez sur **Ajouter à la liste blanche**.

Paramètres de liste blanche

Lorsque vous activez le commutateur **Génération automatique d'une liste blanche**, vous devez indiquer l'un des niveaux de protection heuristique suivants :

- **Faible**
  Les applications d'entreprise seront ajoutées à la liste blanche uniquement après un temps et

© Acronis International GmbH, 2003-2026

des vérifications significatifs. Ces applications sont plus fiables. Cependant, cette approche augmente la possibilité de détections de faux positifs. Les critères pour considérer un fichier comme propre et fiable sont élevés.

- **Défaut**
  Les applications d'entreprise seront ajoutées à la liste blanche selon le niveau de protection recommandé, afin de réduire les détections de faux positifs possibles. Les critères pour considérer un fichier comme propre et fiable sont moyens.
- **Élevé**
  Les applications d'entreprise seront ajoutées à la liste blanche plus rapidement, afin de réduire les détections de faux positifs possibles. Cependant, cela ne garantit pas que le logiciel est propre, et il pourrait être reconnu plus tard comme suspect ou malware. Les critères pour considérer un fichier comme propre et fiable sont faibles.

Afficher les détails à propos des éléments de la liste blanche

Vous pouvez cliquer sur un élément de la liste blanche pour afficher plus d'informations à son sujet et l'analyser en ligne.

Si vous avez des doutes concernant un élément que vous avez ajouté, vous pouvez le vérifier grâce à l'analyseur VirusTotal. Lorsque vous cliquez sur **Examiner sur VirusTotal**, le site analyse les URL et fichiers suspects, afin de détecter certains types de malwares en utilisant le hachage de fichier de l'élément que vous avez ajouté. Vous pouvez afficher le hachage dans la chaîne **Hachage du fichier (MD5)**.

Les valeurs **Machines** font référence au nombre de machines sur lesquelles ce hachage a été détecté lors de l'analyse de sauvegarde. Cette valeur n'est renseignée que si un élément a été retourné de l'analyse de sauvegarde ou de la quarantaine. Ce champ reste vide si le fichier est ajouté manuellement à la liste blanche.

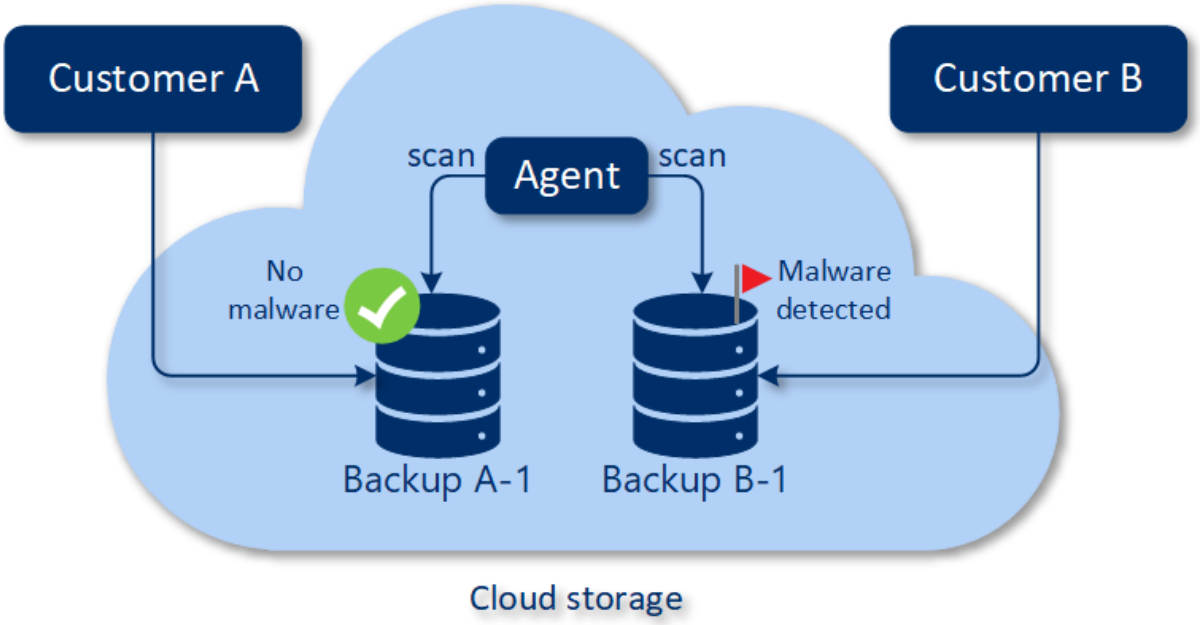
Analyse antimalware des sauvegardes

Remarque
Cette description s'applique à une fonctionnalité qui n'est pas disponible pour les sauvegardes de cloud à cloud. Pour plus d'informations sur une fonctionnalité similaire, l'analyse antimalware des boîtes aux lettres Microsoft 365, voir "Analyse antimalware des boîtes aux lettres" (p. 869).

Grâce à l'analyse antimalware des sauvegardes, vous pouvez empêcher la restauration de fichiers exécutables infectés en vérifiant que vos sauvegardes ne comportent aucun malware. Les analyses antimalware sont effectuées par un agent Cloud qui réside dans le centre de données Cyber Protection et n'utilisent aucune ressource informatique.

Remarque
Seuls les fichiers exécutables (*.exe) sont analysés pour détecter les malwares.

© Acronis International GmbH, 2003-2026



Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Pour effectuer une analyse antimalware, vous devez configurer un plan d'analyse de sauvegarde. Pour plus d'informations, voir "Plan d'analyse des sauvegardes" (p. 272).

Chaque plan d'analyse de sauvegarde crée une tâche d'analyse pour l'agent cloud et ajoute cette tâche à une file d'attente unique par centre de données. Les tâches d'analyse sont traitées selon leur ordre dans la file d'attente.

Le temps d'analyse dépend de la taille de la sauvegarde. C'est la raison pour laquelle il existe un délai entre la création d'un plan d'analyse de sauvegarde et la fin de l'analyse.

Les sauvegardes que vous avez sélectionnées pour l'analyse peuvent avoir l'un des états suivants :

- Non analysé
- Aucun malware
- Malware détecté

Vous pouvez consulter les résultats d'une analyse de la sauvegarde dans le widget **Détails de l'analyse de la sauvegarde (menaces)**. Vous les trouverez dans la console Cyber Protect > **Surveillance** > onglet **Vue d'ensemble**.

Limites

- L'analyse antimalware n'est prise en charge que pour les sauvegardes **Toute la machine** ou **Disques/volumes** des ressources suivantes :

© Acronis International GmbH, 2003-2026

  - Ordinateurs Windows sur lesquels un agent de protection est installé.
  - Machines virtuelles Windows sauvegardées au niveau de l'hyperviseur (sauvegarde sans agent) par l'agent pour Hyper-V et l'agent pour VMware (Windows).

  L'analyse antimalware n'est pas prise en charge pour les sauvegardes créées par des appliances virtuelles telles que l'agent pour VMware (appliance virtuelle), l'agent pour Virtuozzo, l'agent pour Scale Computing HC3, l'agent pour Azure et l'agent pour oVirt.
- Seuls les volumes avec système de fichiers NTFS et partitionnement de table de partitions GUID et du secteur de démarrage principal sont analysés.
- L'analyse antimalware est prise en charge uniquement sur le stockage cloud par défaut. Les stockages locaux, les stockages hébergés par des partenaires et les stockages dans le cloud public ne sont pas pris en charge.
- L'analyse antimalware n'est pas prise en charge pour les tenants en mode de Conformité.
- L'analyse antimalware n'est pas prise en charge pour les types de fichiers suivants :
  - RAR
  - 7z
  - ISO
- Si une tâche d'analyse échoue, elle est retentée le jour suivant.
- Lorsque vous sélectionnez des sauvegardes à analyser, vous pouvez sélectionner des ensembles de sauvegardes incluant une sauvegarde pour la protection continue des données. Toutefois, l'analyse ne concerne que les sauvegardes figurant dans ces ensembles et qui sont d'un autre type que pour la protection continue des données. Pour plus d'informations sur les sauvegardes pour la protection continue des données, voir "Protection continue des données (CDP)" (p. 566).
- Lorsque vous exécutez la restauration sécurisée d'un ordinateur dans son intégralité, vous pouvez sélectionner un ensemble de sauvegardes qui comprend une sauvegarde pour la protection continue des données. Toutefois, cette opération de restauration n'utilise pas les informations de la sauvegarde de protection continue des données. Pour restaurer les données de la protection continue des données, exécutez une autre opération de restauration de **Fichiers/dossiers**.

© Acronis International GmbH, 2003-2026

Configuration de la sécurité de votre intelligence artificielle générative

La sécurité de l'intelligence artificielle générative vous permet de contrôler, surveiller et appliquer une utilisation sécurisée des applications d'intelligence artificielle générative prises en charge à travers les ressources protégées depuis une seule console. Elle inclut la surveillance de l'intelligence artificielle et la prévention des pertes de données pour les applications d'intelligence artificielle, journalise les incidents dans un journal d'événements dédié, et expose des informations de synthèse et de tendance via des rapports et widgets intégrés.

La sécurité de l'intelligence artificielle générative renforce votre posture de conformité et réduit le risque de fuite de données sensibles et réglementées par le biais des applications d'intelligence artificielle.

Important
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Remarque
La sécurité de l'intelligence artificielle générative ne prend en charge que le système d'exploitation Windows. Elle ne prend pas en charge Windows ARM.

Pour activer la sécurité de l'intelligence artificielle générative

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Sélectionnez le plan de protection pertinent dans la liste affichée, puis, dans l'encadré de droite, cliquez sur **Modifier**.
3. Vous pouvez également créer un nouveau plan de protection et passer à l'étape suivante. Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à Plans de protection et modules.
4. Dans l'encadré du plan de protection, activez le module **Sécurité de l'intelligence artificielle générative** en cliquant sur le commutateur à côté du nom du module.

Paramètres de sécurité de l'intelligence artificielle générative

La sécurité de l'intelligence artificielle générative propose des paramètres permettant de configurer la manière dont un plan de protection surveille et protège l'utilisation des applications d'intelligence artificielle générative sur l'ensemble des ressources.

Surveillance de l'utilisation

La surveillance de l'utilisation suit la manière dont votre organisation utilise les applications d'intelligence artificielle générative. Cela fournit des informations précieuses sur l'adoption et les

© Acronis International GmbH, 2003-2026

modèles d'utilisation, vous permettant de prendre des décisions éclairées et de mettre en œuvre des politiques appropriées.

Cette fonctionnalité est disponible au niveau client.

La surveillance de l'utilisation combine les capacités de filtrage d'URL, de protection du navigateur et de EDR. Assurez-vous que ces modules sont activés dans le plan de protection.

Paramètre par défaut : **Activé**

Champ d'application de la protection

Spécifiez le champ d'application de la protection pertinent pour la surveillance de l'utilisation :

- **Navigateur uniquement** - La sécurité de l'intelligence artificielle générative surveille l'activité liée à l'intelligence artificielle dans le navigateur Web.
- **Protection complète** - La sécurité de l'intelligence artificielle générative surveille l'activité liée à l'intelligence artificielle sur l'ensemble du terminal.

Paramètre par défaut : **Navigateur uniquement**

Prévention des pertes de données GenAI

La prévention des pertes de données GenAI détecte et empêche les données sensibles ou confidentielles d'être partagées avec des applications d'intelligence artificielle générative. Le moteur DLP évalue le texte et les types de fichiers courants (par exemple, documents, feuilles de calcul, présentations et archives) par rapport aux définitions des données sensibles.

La prévention des pertes de données GenAI nécessite que :

- La surveillance de l'utilisation est activée.
- Aucun paramètre avancé dans les plans de protection avec Data Loss Prevention n'est appliqué à la même ressource.

La prévention des pertes de données pour l'intelligence artificielle générative utilise la configuration que vous définissez pour l'action à la détection sous Champ d'application de la protection :

- **Navigateur uniquement**
- **Protection complète**

La prévention des pertes de données GenAI présente les limitations suivantes :

- Les fichiers de moins de 100 octets et de plus de 50 Mo ne sont pas vérifiés
- Le texte des images n'est pas pris en charge
- Seul Google Chrome, version 130 ou ultérieure, est pris en charge

Paramètre par défaut : **Activé**

Pour définir l'action à la détection pour la prévention des pertes de données GenAI

© Acronis International GmbH, 2003-2026

1. Dans le module **Sécurité de l'intelligence artificielle générative** d'un plan de protection, cliquez sur **Prévention des pertes de données pour l'intelligence artificielle générative**.
2. Dans la boîte de dialogue, spécifiez l'**Action sur la détection**
   - **Détecter uniquement** - détecte les fuites de données sensibles vers les services d'intelligence artificielle et les enregistre dans le journal des événements d'intelligence artificielle.
   - **Bloquer les fuites de données sensibles vers l'intelligence artificielle** - bloque les tentatives de transférer des fichiers sensibles ou d'entrer des données sensibles dans les services d'intelligence artificielle.
3. Cliquez sur **Terminé**.

Protection contre l'injection de prompt

Utilisez la protection contre l'injection de prompts pour sécuriser les interactions avec les applications d'intelligence artificielle. Une injection de prompts est un type de cyberattaque contre les applications d'intelligence artificielle générative (intelligence artificielle générative), en particulier celles qui utilisent de grands modèles de langage (LLM), tels que ChatGPT. Dans ce type d'attaque, un attaquant insère un prompt nuisible susceptible d'affecter le comportement de l'application d'intelligence artificielle générative, ce qui présente un risque élevé pour les données sensibles et réglementées.

Paramètre par défaut : **Désactivé**

Pour activer la protection contre l'injection de prompt

1. Dans le module de sécurité de l'intelligence artificielle générative d'un plan de protection, cliquez sur **Protection contre l'injection de prompt**.
2. Dans la boîte de dialogue, activez l'interrupteur **Protection contre l'injection de prompt**.
3. Spécifiez l'**Action sur la détection** :
   - **Détecter uniquement** - détecte les attaques d'injection de prompt et les enregistre dans le journal des événements de l'intelligence artificielle
   - **Bloquer les attaques d'injection de prompt** - Les injections de prompt sont bloquées et enregistrées dans le journal des événements de l'intelligence artificielle.
4. Cliquez sur **Terminé**.

© Acronis International GmbH, 2003-2026

Gestion et affectation des workflows d'automatisation

Vous pouvez utiliser des workflows pour automatiser les opérations MSP afin que diverses actions prédéfinies soient déclenchées lorsque des événements spécifiques se produisent dans la plate-forme Cyber Protect Cloud. Cette automatisation assure une utilisation plus efficace des ressources, tout en réduisant simultanément le risque d'erreur humaine dans les opérations guide pas-à-pas. Les techniciens MSP peuvent également accomplir leurs tâches quotidiennes plus facilement et plus rapidement, leur donnant plus de temps pour se consacrer à des problèmes non standard.

Utilisez les workflows pour :

- Réduire le bruit des alertes : Obtenez un meilleur contrôle sur la façon dont les alertes sont déclenchées et livrées, tout en filtrant les notifications inutiles, et en vous concentrant sur celles de plus haute priorité.

  Par exemple, si vous avez une URL qui est bloquée pour l'accès des collaborateurs via le filtrage d'URL, vous pouvez définir un workflow pour gérer toutes les alertes générées lorsque les collaborateurs accèdent à l'URL spécifiée.
- Automatiser les procédures standard : Les workflows définis sont déclenchés par un événement de plate-forme, puis exécutent un ensemble d'actions prédéfinies.

Important
Les utilisateurs partenaires ou tenants avec le rôle d'administrateur d'entreprise, administrateur, ou administrateur cyber, peuvent créer de nouveaux workflows, ainsi que consulter et mettre à jour tous les workflows dans le système. Ces utilisateurs peuvent également consulter l'historique d'exécution, et affecter des workflows aux utilisateurs tenants concernés.

Pour les workflows propagés ou les workflows définis comme modèles, l'administrateur d'entreprise, l'administrateur, ou l'administrateur cyber peut activer ou désactiver les versions de workflow pour les tenants sélectionnés et les enfants tenants, accéder aux détails du workflow en mode en lecture seule, et cloner des workflows, mais pas des versions de workflow. Voir "Création d'un workflow" (p. 1227).

Tous les autres rôles d'utilisateur ont un accès en lecture seule aux workflows qui leur sont affectés.

Pour plus d'informations, voir les rôles d'utilisateur disponibles dans le service de Protection.

Comment créer, configurer et activer un workflow

Vous pouvez créer et configurer un workflow lorsque vous êtes connecté en tant qu'administrateur de l'entreprise, Administrateur ou administrateur Cyber. Une fois le workflow configuré, il peut ensuite être activé pour les tenants clients concernés.

Le tableau ci-dessous inclut les étapes impliquées dans une configuration typique de workflow, avec des liens vers les sections correspondantes pour plus d'informations.

© Acronis International GmbH, 2003-2026

Étape	Description
Accéder et visualiser les workflows	Pour accéder au module **Workflows** dans la Cyber Protectconsole, accédez à **Gestion** > **Workflows**. Dans l'écran principal **Workflows**, vous pouvez afficher et mettre à jour les workflows existants, et créer de nouveaux workflows. En tant qu'administrateur de l'entreprise, administrateur ou administrateur Cyber au niveau le plus élevé de partenaire, vous pouvez afficher tous les workflows dans le système. Leurs tenants enfants peuvent afficher leurs propres workflows, et les workflows qui ont été définis comme un modèle par le partenaire parent. Les utilisateurs clients peuvent afficher leurs propres workflows, et les workflows qui leur ont été affectés ou activés pour eux. Pour plus d'informations, voir "Affichage des workflows actuels" (p. 1226).
Définir les paramètres initiaux pour le workflow	Dans l'écran principal des **Workflows**, cliquez sur **Créer**. Ensuite, définissez un nom et une description pour le workflow. Vous pouvez également enregistrer le workflow comme un modèle qui est propagé au tenant sélectionné et à leurs tenants enfants. **Remarque** Seuls les utilisateurs affectés au rôle d'administrateur de l'entreprise, administrateur ou administrateur Cyber peuvent créer un workflow. Pour plus d'informations, voir

© Acronis International GmbH, 2003-2026

Étape	Description
	"Création d'un workflow" (p. 1227).
Définir les déclencheurs, conditions et actions du workflow	Dans l'écran principal des **Workflows**, ouvrez le workflow concerné, puis : 1. Sélectionnez un événement déclencheur pour initier le workflow, tel que **Sauvegarde échouée**, ou **Menace EDR détectée**. Vous pouvez ajouter des déclencheurs supplémentaires, si nécessaire. 2. Dans la section **Actions**, cliquez sur **Condition** pour ajouter un bloc **Condition**. Ensuite, configurez les chemins **Si** et **Sinon** en conséquence (cliquez sur **+** pour ajouter une condition au chemin, puis sélectionnez une variable de source de données avec l'opérateur et la valeur appropriés, et cliquez sur **Ajouter**). Configurez le chemin **Sinon** (et tout chemin supplémentaire) de la même manière. 3. Cliquez sur **Action** dans le workflow pour définir ce qui se passe après le déclenchement du workflow. Sélectionnez l'action appropriée parmi les options disponibles, telles que **Ignorer l'alerte**, **Envoyer un e-mail**, ou **Ajouter un commentaire**. Les modifications que vous apportez au workflow lors de sa configuration sont enregistrées automatiquement.

© Acronis International GmbH, 2003-2026

Étape	Description
	Pour plus d'informations, voir "Création d'un workflow" (p. 1227).
Activation du workflow	Lorsque le workflow est configuré, accédez à l'onglet **Versions**, puis cliquez le bouton bascule **Désactivé** pour l'activer. Vous pouvez ensuite l'affecter aux tenants clients concernés (dans l'onglet **Clients**, cliquez sur **Gérer les clients** pour sélectionner le ou les tenants concernés, puis sélectionnez la version de workflow requise). Lorsqu'il est activé, le workflow sera exécuté selon les déclencheurs, conditions et actions définis. Pour plus d'informations, voir "Activation d'un workflow" (p. 1234).
Gestion et surveillance du workflow	Lorsqu'il est activé pour les tenants clients concernés, vous pouvez surveiller l'historique d'exécution du workflow, mettre à jour le workflow, et cloner et supprimer le workflow. Pour plus d'informations, voir "Gestion de vos workflows" (p. 1233). Vous pouvez également créer, mettre à jour et gérer les versions du workflow. Pour plus d'informations, voir "Versions de workflow" (p. 1237).

Affichage des workflows actuels

Pour afficher tous les workflows, dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.

Les utilisateurs partenaires ou tenants avec le rôle d'administrateur d'entreprise, Administrateur, ou administrateur Cyber, peuvent visualiser et mettre à jour n'importe quel workflow dans le système.

© Acronis International GmbH, 2003-2026

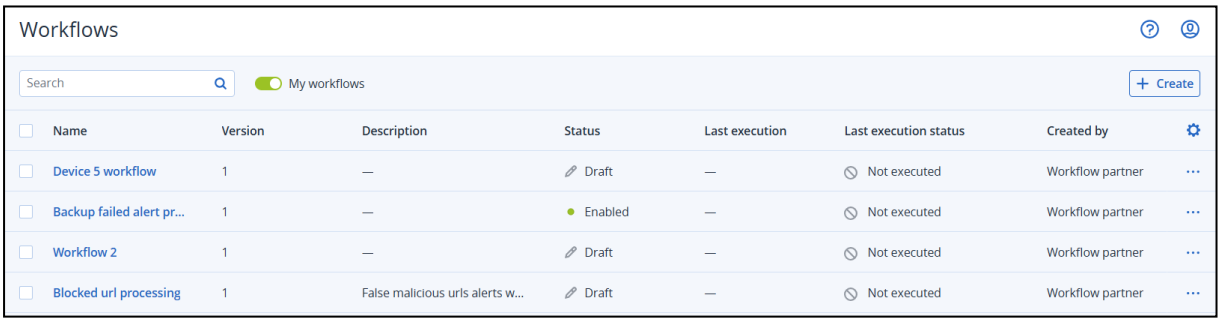
S'il n'existe pas de workflows, vous êtes invité à en créer un. Pour plus d'informations, voir "Création d'un workflow" (p. 1227).

Les informations suivantes sont affichées pour chaque workflow :

- Le nom et la version actuelle activée du workflow.
- Une description définie par l'utilisateur du workflow.
- Le statut actuel du workflow (soit **Activé**, **Désactivé**, ou **Brouillon**).
- La date et l'heure de la dernière exécution du workflow.
- Le statut de la dernière exécution (soit **Réussi**, **Erreur**, ou **Non exécuté**).
- L'utilisateur qui a créé le workflow.

Cliquez sur un workflow pour afficher des détails supplémentaires dans le volet droit. Ces informations incluent un aperçu général, l'accès à l'historique des exécutions, les tenants qui peuvent travailler avec (disponible uniquement pour l'administrateur de l'entreprise, l'administrateur, ou l'administrateur Cyber), et les versions actuellement disponibles.

Vous pouvez également cliquer sur le commutateur **Mes workflows** pour filtrer la liste affichée afin de montrer uniquement les workflows concernés pour votre rôle. Par exemple, si vous êtes un administrateur de l'entreprise, un administrateur, ou un administrateur Cyber, vous verrez uniquement les workflows que vous avez créés. Si vous êtes un utilisateur ou un administrateur en lecture seule, vous verrez les workflows qui vous sont affectés.



Création d'un workflow

En tant qu'administrateur de l'entreprise, Administrateur, ou administrateur Cyber, vous pouvez créer un workflow à partir de zéro, ou utiliser l'un des modèles de workflow prédéfinis, selon vos besoins.

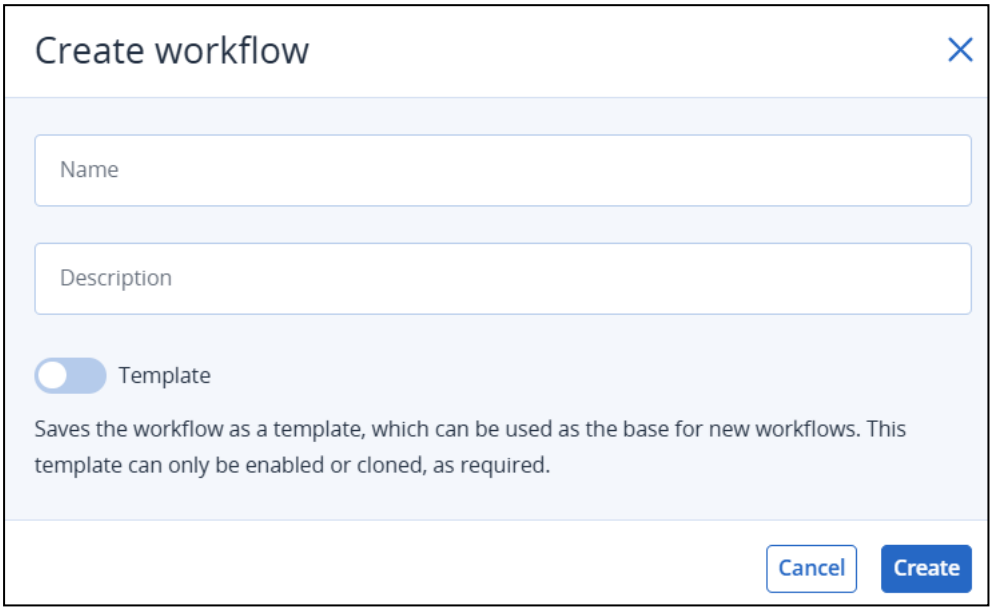
Remarque
Vous pouvez créer des workflows pour un tenant spécifique, ou pour un certain nombre de tenants. Vous pouvez ensuite affecter le workflow aux tenants concernés dans l'onglet **Clients**. Pour plus d'informations, voir "Affectation des workflows" (p. 1235).

Pour créer un workflow

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Cliquez sur **Créer**.

   Si aucun workflow n'existe, cliquez sur **Créer un workflow**.
3. Définissez un nom et une description (facultatif) pour le workflow.



4. [Facultatif] Cliquez sur le bouton bascule **Modèle** pour l'activer. Cela garantit que le workflow est enregistré en tant que modèle, et est automatiquement disponible pour vos partenaires et tenants clients, qui peuvent utiliser le modèle pour créer leurs propres workflows.

   Lorsque **Modèle** est activé, notez ce qui suit :
   - Toutes les versions du workflow seront visibles pour vos tenants clients, et leurs enfants tenants et partenaires.
   - Vos tenants clients et leurs enfants tenants et partenaires peuvent consulter et accéder au workflow propagé, et peuvent activer n'importe quelle version du workflow ou créer leur propre version.
   - Vos tenants clients et leurs enfants tenants et partenaires peuvent désactiver une version de workflow qu'ils ont activée ou que leurs enfants tenants ont activée.
5. Cliquez sur **Créer**.

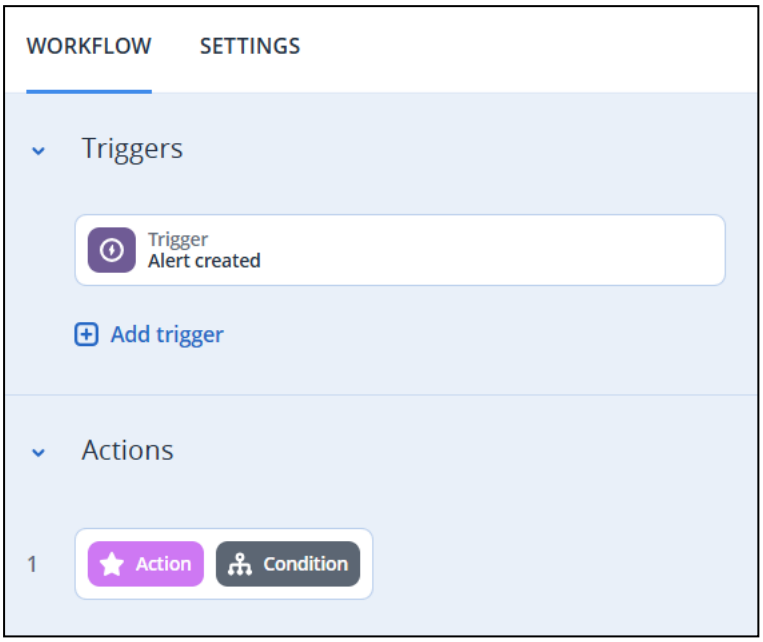
   Le workflow est ajouté à la liste actuelle des workflows disponibles, et accessible depuis l'écran principal **Workflows**. Vous pouvez maintenant ajouter des déclencheurs, des conditions et des actions, selon les besoins.
6. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur **Ouvrir**.

Remarque

Lorsqu'un workflow est initialement créé, il contient deux étapes préliminaires, un déclencheur et un terminal. Le déclencheur doit être sélectionné dans la bibliothèque des déclencheurs disponibles, comme décrit ci-dessous.

© Acronis International GmbH, 2003-2026

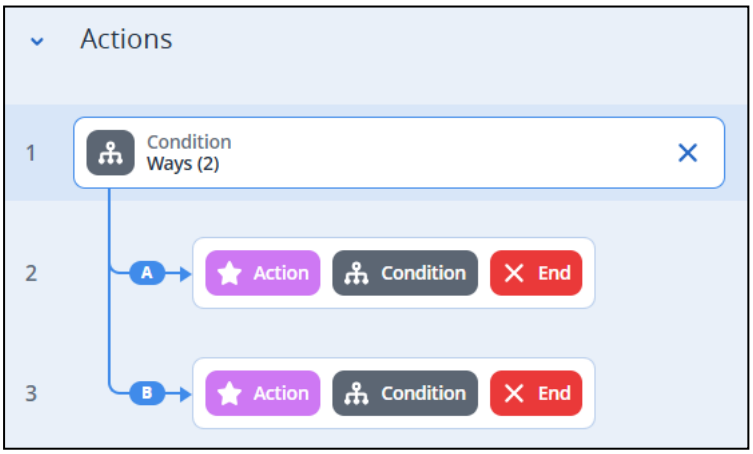
7. Pour définir un déclencheur, cliquez sur le bloc **Déclencheur**, puis sélectionnez le déclencheur concerné, tel que **Sauvegarde échouée**, ou **Alerte créée**. Vous pouvez ajouter des déclencheurs supplémentaires, selon les besoins.



8. Dans la section **Actions**, cliquez sur **Condition** pour ajouter un bloc **Condition**.

   Chaque nouveau bloc contient deux chemins à afficher, qui déterminent la direction et les actions à appliquer au workflow :

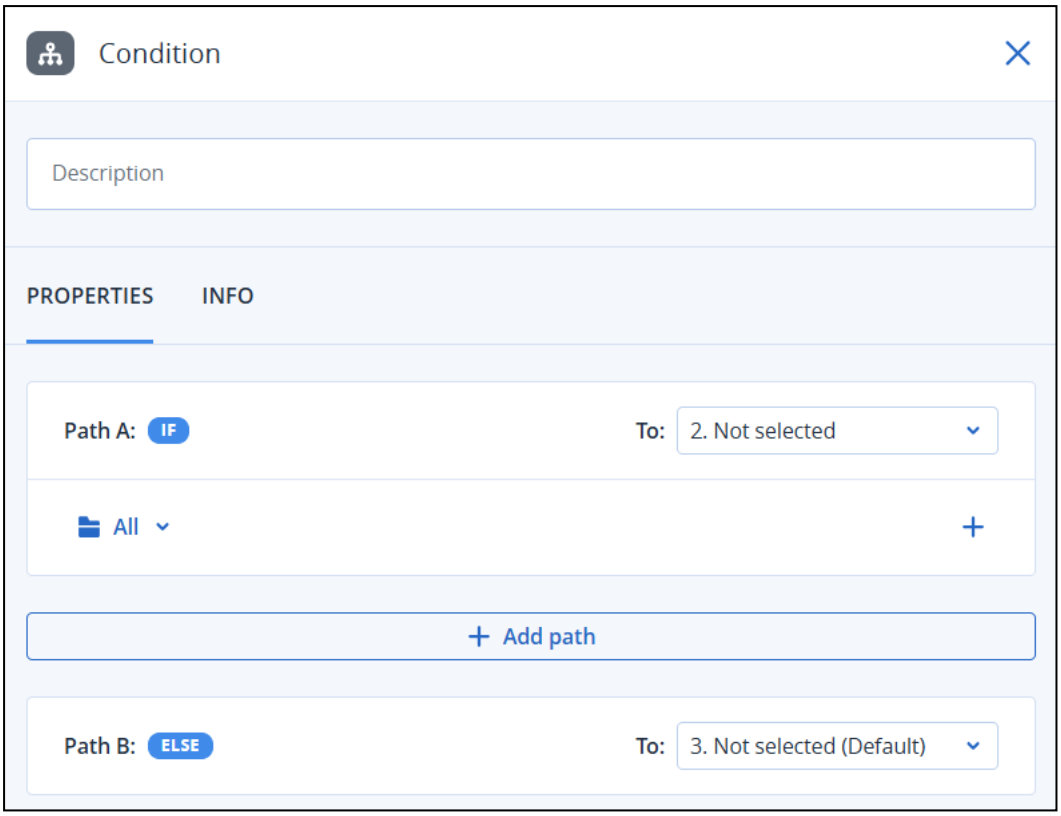
   - Chemin A (**Si**) : Affiche initialement un bloc vide menant à l'étape suivante.
   - Chemin B (**Sinon**) : Définit un résultat Sinon qui mène au terminal du workflow.



   Configurez les chemins **Si** et **Sinon** en conséquence. Cliquez sur **+** pour ajouter une condition au chemin, puis sélectionnez une variable de source de données avec l'opérateur et la valeur appropriés, et cliquez sur **Ajouter**.

   Vous pouvez combiner plusieurs combinaisons `AND` et `OR` de conditions dans un bloc.

© Acronis International GmbH, 2003-2026



Configurez tous les chemins supplémentaires de la même manière. Vous pouvez également supprimer une condition, en cliquant sur l'icône de la poubelle à côté.

Remarque
Le bloc **Condition** définit un ensemble de conditions qui doivent être exécutées dans le cadre du workflow et se compose de deux types de blocs :

- **Tous** : toutes les conditions de ce bloc doivent être remplies pour que vous puissiez passer à l'étape suivante du workflow.
- **Tout** : au moins une des conditions de ce bloc doit être remplie pour que vous puissiez passer à l'étape suivante du workflow.

9. Cliquez sur **Action** dans le workflow pour définir ce qui se passe après le déclenchement du workflow. Sélectionnez l'action appropriée parmi les options disponibles, telles que **Ignorer l'alerte**, **Envoyer un e-mail**, ou **Ajouter un commentaire**.

   Par exemple, cliquez sur l'action **Envoyer un e-mail**, puis modifiez les destinataires, le corps et le sujet de l'e-mail envoyé dans le cadre de ce workflow.

   Les actions disponibles sont filtrées en fonction du déclencheur défini que vous avez sélectionné à l'étape 7. Certaines actions peuvent nécessiter des paramètres d'entrée supplémentaires pour être appliquées au workflow, selon le déclencheur sélectionné.

Les modifications que vous apportez au workflow lors de sa configuration sont enregistrées automatiquement.

© Acronis International GmbH, 2003-2026

Remarque
Après avoir configuré le workflow, vous pouvez activer (et désactiver) un workflow depuis l'écran principal **Workflows** en sélectionnant le workflow concerné, puis en sélectionnant **Activer** ou **Désactiver**. Pour plus d'informations, voir "Activation d'un workflow" (p. 1234).

Composants et modèles de workflow

Ce sujet décrit les composants pris en charge que les tenants partenaires peuvent utiliser pour initier des workflows et définir des actions ou opérations de réponse correspondantes au sein du système. Le tableau à la fin liste les modèles de workflow disponibles que vous pouvez utiliser comme exemples lors de la création de vos propres workflows.

Déclencheurs de workflow

Les déclencheurs suivants peuvent être utilisés pour automatiser l'exécution des workflows.

Catégorie	Nom du déclencheur	Description
EDR	Incident EDR créé	Déclenché automatiquement lorsqu'un nouvel incident est créé dans le système.
	Incident EDR mis à jour	Déclenché chaque fois qu'un incident existant est mis à jour.
Terminaux	Terminal enregistré	Déclenché lorsqu'un nouveau terminal est enregistré avec succès.
Alerte	Alerte créée	Déclenché lorsque tout service surveillé ou composant du système génère une nouvelle alerte.
Tenants	Tenant créé	Déclenché lorsqu'un nouveau tenant est créé.
	Tenant activé	Déclenché lorsqu'un tenant désactivé est réactivé.
Utilisateurs	Utilisateur créé	Déclenché lorsqu'un nouvel utilisateur est créé pour le tenant.
	Utilisateur supprimé	Déclenché lorsqu'un utilisateur est supprimé
	Utilisateur désactivé	Déclenché lorsqu'un utilisateur est désactivé.
	Utilisateur activé	Déclenché lorsqu'un utilisateur désactivé est réactivé.

Actions de workflow

Les composants d'action suivants peuvent être inclus dans les workflows pour automatiser l'exécution de leurs actions correspondantes.

© Acronis International GmbH, 2003-2026

Catégorie	Nom de l'action	Description
EDR	Affecter un incident	Affecte l'incident EDR à un utilisateur spécifié.
	Changer l'état	Met à jour l'état de l'incident EDR.
	Quarantaine	Met en quarantaine le fichier ou l'objet détecté.
	Stopper le processus	Termine un processus spécifié sur la ressource.
	Ajouter un commentaire	Ajoute un commentaire à l'incident EDR.
	Isoler le terminal	Isole la ressource du réseau.
Terminaux	Appliquez un plan de protection	Applique un plan de protection à la ressource. Le plan de protection est pris dans la liste des plans existants.
	Révoquer le plan de protection	Révoque le plan de protection appliqué de la ressource.
	Obtenir le statut de sauvegarde	Récupère le statut actuel de la sauvegarde de la ressource.
	Exécuter la gestion des correctifs	Initie le processus de gestion des correctifs sur le terminal.
	Exécuter le script	Exécute un script sur le terminal. Le script est pris dans la liste des scripts existants.
	Obtenir le statut de sécurité	Récupère le statut actuel de la sécurité de la ressource.
	Exécuter la sauvegarde	Démarre une tâche de sauvegarde sur le terminal sélectionné.
	Obtenir le statut de gestion des correctifs	Récupère le statut de gestion des correctifs du terminal.
	Exécuter l'évaluation des vulnérabilités	Exécute une évaluation des vulnérabilités sur le terminal.
	Exécuter l'analyse des malwares	Exécute une analyse de malware sur le terminal.
Alerte	Obtenir le tenant de l'alerte	Récupère le tenant associé à l'alerte.
	Obtenir la ressource de l'alerte	Récupère la ressource associée à l'alerte.
	Ignorer l'alerte	Ignore l'alerte.
Notifications	Envoyer un e-mail aux administrateurs du tenant	Envoie une notification par e-mail aux administrateurs du tenant.

© Acronis International GmbH, 2003-2026

Catégorie	Nom de l'action	Description
Utilisateurs	Créer utilisateur	Crée un nouvel utilisateur sous le tenant spécifié.
	Configurer les notifications	Configure les paramètres de notification utilisateur.
	Gérer les rôles utilisateur	Affecte ou modifie les rôles et autorisations utilisateur.
Général	Attendre	Retarde l'exécution du workflow pour une durée spécifiée.

Modèles de workflow

Les modèles de workflow suivants peuvent être utilisés comme exemples prédéfinis pour l'automatisation.

Nom du modèle	Catégorie
Workflow de routine de sauvegarde client	Alerte
Gestionnaire d'alerte d'URL bloquée	Alerte
Workflow d'échec de sauvegarde serveur	Alerte
Workflow de mise en quarantaine des menaces	EDR
Workflow d'isolement de ressource	EDR
Incident de malware nécessitant une attention particulière	EDR
Incident nécessitant une attention particulière	EDR
Affectation automatique d'incident	EDR

Gestion de vos workflows

Selon votre rôle, certaines fonctionnalités de workflow peuvent ne pas être disponibles. Le tableau suivant répertorie les fonctionnalités disponibles pour tous les rôles.

Fonctionnalité	Administrateur d'entreprise / Administrateur / Administrateur cyber	Utilisateurs tenant clients et tous les autres utilisateurs
Activation d'un workflow	Oui	Oui, uniquement les workflows qui leur ont été affectés
Gérer qui peut accéder et exécuter les workflows	Oui	Non
Affichage de l'historique d'exécution du workflow	Oui	Oui

© Acronis International GmbH, 2003-2026

Fonctionnalité	Administrateur d'entreprise / Administrateur / Administrateur cyber	Utilisateurs tenant clients et tous les autres utilisateurs
Clonage d'un workflow	Oui	Non
Mise à jour d'un workflow	Oui	Non
Suppression d'un workflow	Oui	Non

Activation d'un workflow

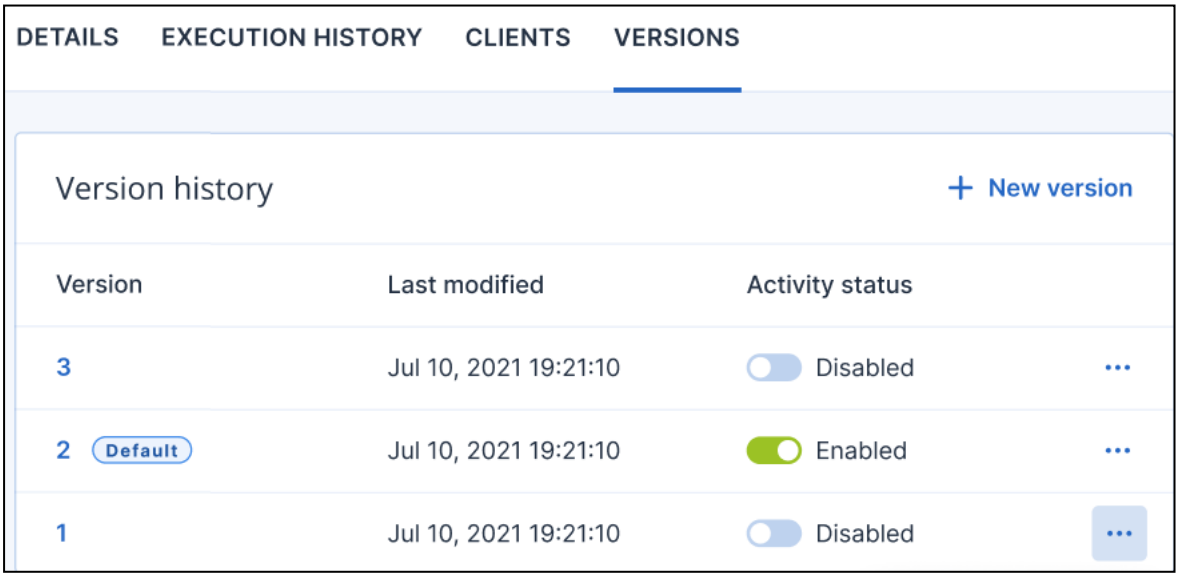
En tant qu'administrateur de l'entreprise, administrateur ou administrateur Cyber, vous pouvez spécifier la version du workflow que vous souhaitez activer pour vos tenants clients.

Les utilisateurs tenants clients peuvent uniquement activer ou désactiver les workflows qui leur ont été affectés.

Remarque
Les administrateurs au niveau du partenaire peuvent avoir plusieurs versions activées. Les utilisateurs des tenants clients ne peuvent avoir qu'une seule version activée à la fois.

Pour activer les workflows

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur l'onglet **Versions**.



3. Dans la liste affichée des versions de workflow, cliquez sur le bouton bascule **Désactivé** pour activer la version.

[Pour l'administrateur de l'entreprise, l'administrateur ou l'administrateur Cyber] Le workflow activé est maintenant disponible pour les tenants clients qui avaient précédemment été affectés au

© Acronis International GmbH, 2003-2026

workflow. Le workflow peut également être affecté à des tenants supplémentaires, si nécessaire. Voir "Affectation des workflows" (p. 1235).

[Pour les utilisateurs des tenants clients] Le workflow activé s'exécutera selon les déclencheurs, conditions et actions définis.

Pour désactiver une version de workflow, cliquez sur le bouton bascule **Activé** afin de le repasser sur **Désactivé**.

Remarque
Si plusieurs workflows sont déclenchés par le même événement, ils sont exécutés un par un selon leur priorité, puis selon leur date et heure d'exécution. Si le premier workflow échoue à s'exécuter pour une raison quelconque, le workflow suivant est automatiquement exécuté.

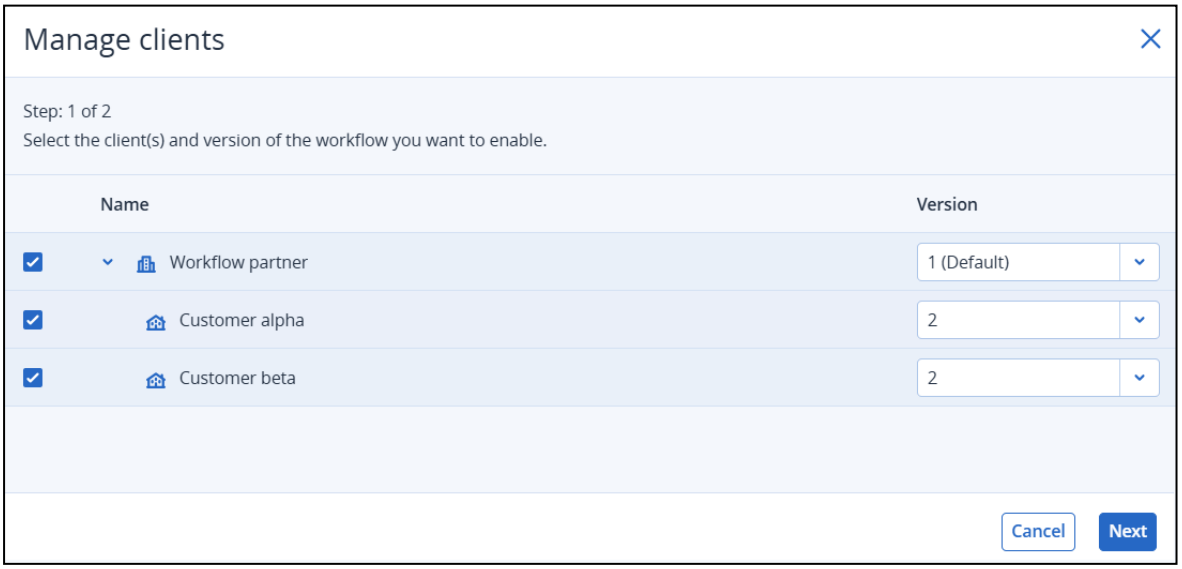
Affectation des workflows

Vous pouvez afficher et affecter les workflows actuellement activés pour un tenant ou client sélectionné dans l'onglet **Clients**. Lorsque vous affectez un workflow, il est automatiquement défini comme **Activé** pour les utilisateurs des tenants clients sélectionnés.

L'onglet **Clients** est uniquement accessible aux utilisateurs affectés avec le rôle d'administrateur de l'entreprise, d'administrateur ou d'administrateur Cyber.

Pour affecter des workflows aux tenants ou clients sélectionnés

1. Accédez à **Gestion** > **Workflows**, puis sélectionnez le workflow concerné.
2. Cliquez sur l'onglet **Clients**.
3. Cliquez sur le lien **Gérer les clients**.
   Si vous n'avez pas encore configuré l'accès à vos clients, il vous est demandé de cliquer sur un bouton **Gérer les clients** distinct.
4. Sélectionnez l'option **Mon entreprise** pour développer la liste des tenants clients disponibles, puis sélectionnez les tenants auxquels vous souhaitez affecter des versions de workflow.



© Acronis International GmbH, 2003-2026

5. Dans la colonne **Version**, sélectionnez la version de workflow concerné que vous souhaitez affecter à chaque tenant client.
   La version de workflow sélectionnée est la seule version disponible affichée au tenant client, et ils ne peuvent accéder à aucune autre version.
6. Cliquez sur **Suivant**.
7. Vérifiez les versions et tenants sélectionnés, puis cliquez sur **Enregistrer**.
   Les versions de workflow sélectionnées sont maintenant disponibles pour chaque tenant client lorsqu'ils accèdent à l'écran principal **Workflows**. Les versions de workflow sont automatiquement définies comme **Activées**.

Visualisation de l'historique d'exécution d'un workflow

L'historique d'exécution d'un workflow sélectionné vous permet de voir quand un workflow a été exécuté, et par quel tenant.

Pour visualiser l'historique d'exécution d'un workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur l'onglet **Historique d'exécution**.
   Chaque exécution du workflow sélectionné est listée dans une ligne distincte. Chaque ligne indique la date et l'heure d'exécution, le statut (**Réussi** ou **Erreur**) de chaque exécution, et le tenant qui a exécuté le workflow. Vous pouvez également filtrer la liste affichée des exécutions par **Statut** et **Client**.

Clonage d'un workflow

Vous pouvez cloner tout workflow existant qui est actuellement défini comme **Activée**.

Lors du clonage d'un workflow, une copie complète de la version par défaut du workflow est clonée, y compris tous les déclencheurs, conditions et actions.

Remarque
Lorsqu'on est connecté en tant qu'administrateur d'entreprise, administrateur ou administrateur Cyber, vous pouvez cloner n'importe quel workflow, y compris les workflows en statut **Brouillon**.

Cloner un workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Assurez-vous que le workflow que vous souhaitez cloner est défini avec le statut **Activé**.
3. Sur la ligne du workflow concerné, cliquez sur l'icône en forme de points de suspension (...), puis sélectionnez **Cloner**.
   Le workflow cloné est enregistré en statut **Brouillon**, et avec le nom `Copié + Ancien nom du workflow`. Par exemple, **Copié Alerte workflow**. Pour changer le nom du workflow cloné, ouvrez

© Acronis International GmbH, 2003-2026

le workflow et mettez à jour le nom dans l'onglet **Paramètres**. Voir "Mise à jour d'un workflow" (p. 1237).

Mise à jour d'un workflow

En tant qu'administrateur de l'entreprise, administrateur ou administrateur Cyber, vous pouvez mettre à jour tous les éléments du workflow, y compris son nom et sa description, ainsi que les déclencheurs, conditions et actions du workflow.

Les utilisateurs de tenant client et tous les utilisateurs non-administrateurs ne peuvent pas mettre à jour les workflows.

Pour mettre à jour un workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Cliquez sur la ligne de workflow concerné, puis cliquez sur **Ouvrir**.
3. Mettre à jour le workflow.
4. Cliquez sur **Mettre à jour**.
   Le workflow est automatiquement mis à jour pour les utilisateurs concernés auxquels le workflow est affecté.

Suppression d'un workflow

En tant qu'administrateur de l'entreprise, administrateur ou administrateur Cyber, vous pouvez supprimer tout workflow que vous avez créé ou qui vous a été affecté.

Pour supprimer un workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Cliquez sur le commutateur **Mes workflows** pour afficher les workflows que vous avez créés, et tous les workflows qui vous ont été affectés.
3. Dans la colonne la plus à droite du workflow concerné, cliquez sur l'icône en forme de points de suspension (...), puis sélectionnez **Supprimer**.
4. Dans le message de confirmation, cliquez sur **Supprimer**.

Versions de workflow

Chaque workflow peut comprendre plusieurs versions, avec une version toujours définie comme la version par défaut.

L'administrateur de l'entreprise, l'administrateur ou l'administrateur Cyber peut modifier, activer ou supprimer toutes les versions de workflow, selon les besoins. Tous les autres utilisateurs ne peuvent pas gérer les versions de workflow.

© Acronis International GmbH, 2003-2026

Remarque
Lorsque vous créez un nouveau workflow, il est automatiquement défini comme version 1. Les nouvelles versions ultérieures du workflow sont automatiquement incrémentées de + 1 lorsque la version est créée. Voir "Création d'un workflow" (p. 1227).

Par exemple, la deuxième version d'un workflow est définie comme version 2, et la troisième version est définie comme version 3. Par la suite, si vous clonez la version 2, cette nouvelle version est définie comme version 4. Voir "Clonage d'une version de workflow" (p. 1240).

Chaque version de workflow peut se trouver dans l'un des états suivants :

- **Brouillon** - Une version modifiable du workflow qui n'a pas été précédemment activée sur un tenant. Seules les versions dans cet état peuvent être modifiées.
- **Actif** - La version est activée pour au moins un tenant. Une version dans cet état ne peut être définie que sur **Désactivé**.
- **Désactivé** - La version était précédemment activée, mais est actuellement désactivée pour tous les tenants.

Visualisation d'une version de workflow

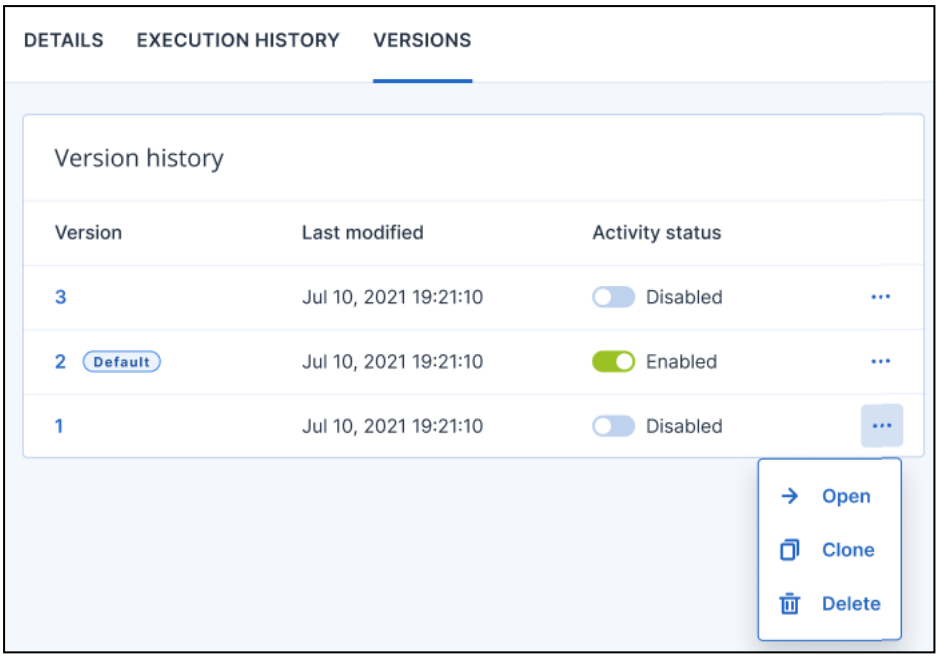
Vous pouvez visualiser et ouvrir tout workflow qui vous est affecté.

Remarque
L'administrateur de l'entreprise, l'Administrateur ou l'administrateur Cyber peut ouvrir et visualiser les versions de tout workflow.

Pour visualiser une version de workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur l'onglet **Versions**.
3. Dans la ligne de la version concernée, cliquez sur l'icône en forme de points de suspension (...), puis sélectionnez **Ouvrir**.

© Acronis International GmbH, 2003-2026



La version du workflow est ouverte. Visualisez et vérifiez les déclencheurs de version, les conditions et les actions, selon les besoins.

L'administrateur de l'entreprise, l'Administrateur ou l'administrateur Cyber peut mettre à jour n'importe lequel des composants du workflow. Pour plus d'informations, voir "Mise à jour d'un workflow" (p. 1237).

Créer une nouvelle version d'un workflow

L'administrateur d'entreprise, l'administrateur ou l'administrateur cyber peut créer une nouvelle version de n'importe quel workflow.

Pour créer une nouvelle version du workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur **Nouvelle version**.

   L'écran de configuration du workflow est affiché, avec la version par défaut du workflow ouverte.
3. Modifiez les déclencheurs de version, les conditions et les actions, selon les besoins. Pour plus d'informations, voir "Création d'un workflow" (p. 1227).

   Une fois terminé, la nouvelle version du workflow est automatiquement enregistrée avec un numéro de version incrémenté automatiquement de 1. Par exemple, la deuxième version d'un workflow est définie comme la version 2, et une troisième version ultérieure est définie comme la version 3.

   La nouvelle version du workflow est définie comme **Brouillon**, et est automatiquement désactivée.

© Acronis International GmbH, 2003-2026

Définir la version par défaut d'un workflow

Une seule version d'un workflow peut être définie comme version par défaut. La version par défaut est la version du workflow qui est automatiquement exécutée selon les déclencheurs, conditions et actions définis.

Lorsqu'une version de workflow est définie comme version par défaut, tous vos utilisateurs clients et enfants tenant avec ce workflow spécifique activé utiliseront automatiquement cette version par défaut.

Remarque
Lorsqu'un workflow est activé pour la première fois, la première version originale est automatiquement définie comme la version par défaut. Après la création de versions ultérieures, vous pouvez alors définir à tout moment quelle version est la version par défaut.

Pour définir la version par défaut du workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur l'onglet **Versions**.
3. Dans la ligne de version concernée, cliquez sur l'icône en forme de points de suspension (...), puis sélectionnez **Définir par défaut**.

La version du workflow est définie comme la version par défaut.

Clonage d'une version de workflow

Vous pouvez cloner toute version de workflow existante qui est actuellement définie comme **Activée**.

Remarque
Lorsque vous êtes connecté en tant qu'administrateur de l'entreprise, Administrateur, ou administrateur Cyber, vous pouvez cloner toute version de workflow, y compris les versions de workflows en statut **Brouillon**.

Pour cloner une version de workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur l'onglet **Versions**.
3. Sur la ligne de version concernée, cliquez sur l'icône en forme de points de suspension (...), puis sélectionnez **Cloner**.

   La version clonée est automatiquement définie comme **Brouillon** et est également désactivée (même si vous avez cloné un workflow défini comme **Activée**).

© Acronis International GmbH, 2003-2026

Suppression d'une version de workflow

Seules les versions de workflow définies comme **Brouillon** peuvent être supprimées.

Pour supprimer une version de workflow

1. Dans la console Cyber Protect, accédez à **Gestion** > **Workflows**.
2. Dans l'écran principal **Workflows**, sélectionnez le workflow concerné, puis cliquez sur l'onglet **Versions**.
3. Dans la ligne de la version concernée, cliquez sur l'icône en forme de points de suspension (...), puis sélectionnez **Supprimer**.
4. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

© Acronis International GmbH, 2003-2026

XDR (Extended Detection and Response)

Remarque
Cette fonctionnalité fait partie du pack de protection Sécurité et RMM, qui fait lui-même partie du service Cyber Protection. Notez que vous devez activer la fonctionnalité Endpoint Detection and Response (EDR) dans un plan de protection pour que XDR fonctionne.

XDR utilise la fonctionnalité EDR pour la mise en corrélation des événements et l'identification des attaques avancées sur les terminaux, puis étend cette fonctionnalité en identifiant les menaces avancées sur les terminaux, les e-mails, les identités, etc.

En utilisant le graphique XDR à travers plusieurs intégrations XDR (y compris FortiMail Workspace Security et Microsoft 365), vous pouvez également répondre aux incidents avec des actions spécifiques disponibles pour chaque type d'intégration, telles que le blocage des expéditeurs d'e-mails ou la suspension des utilisateurs.

La fonctionnalité XDR est compatible avec les postes de travail, les serveurs, les machines virtuelles et les serveurs d'hébergement Web.

Utilité de la fonctionnalité XDR (Extended Detection and Response)

Les MSP proposant des services de sécurité devaient jusqu'à présent choisir entre une protection insuffisante et incomplète ou des solutions coûteuses et complexes. La fonctionnalité XDR permet de dépasse ces limites, car elle étend et enrichit les fonctionnalités fournies par "Endpoint Detection and Response (EDR)" (p. 1251), et identifie les menaces avancées sur les terminaux, dans les e-mails, les identités, etc.

Avec une *surface d'attaque en constante augmentation* (plusieurs clients dans des emplacements distants, mélange de ressources sur site et dans le cloud, utilisation conjointe de clouds privés et publics), des *lacunes dans l'infrastructure de sécurité* (en raison de la multitude d'outils de sécurité déployés pour différents clients, des alertes qui submergent les techniciens et du manque de compétences en matière de sécurité) et des *cybermenaces en constante évolution* (outils basés sur l'IA pour les attaquants qui trouvent et exploitent des vulnérabilités zero-day, et des générateurs de ransomware), il faut impérativement une solution pour arrêter les cybermenaces modernes grâce à des mesures d'intervention simplifiées.

Voici en quoi la fonctionnalité XDR peut vous être utile :

- **Extension de la protection** : protégez des menaces sophistiquées les environnements clients ayant des surfaces d'attaque vulnérables grâce à une visibilité étendue intégrant les terminaux, les e-mails, Microsoft Entra ID et les applications Microsoft 365 (SharePoint, OneDrive et Teams). Cette visibilité améliorée accélère les détections par rapport à la fonctionnalité EDR.

© Acronis International GmbH, 2003-2026

- **Intégration native** : intégrez facilement les plates-formes de cybersécurité, de protection des données et de gestion des terminaux. La fonctionnalité XDR est conçue pour protéger les surfaces d'attaque vulnérables et garantir une continuité des activités inégalée.
- **Efficacité extrême avec réaffectation améliorée** : lancez, gérez, montez en charge et fournissez facilement des services de sécurité. La fonctionnalité XDR inclut également une analyse d'incident basée sur l'IA et une réponse en un clic qui simplifient la recherche et la réaffectation grâce à des mesures d'intervention automatiques et assistées par l'IA ; ces dernières fournissent une protection contre les cybermenaces avancées et à plusieurs étapes. La sécurité proactive permet également aux techniciens d'identifier les problèmes potentiels et de les résoudre avant qu'un attaquant ne les exploite.

Activation de la fonctionnalité XDR (Extended Detection and Response)

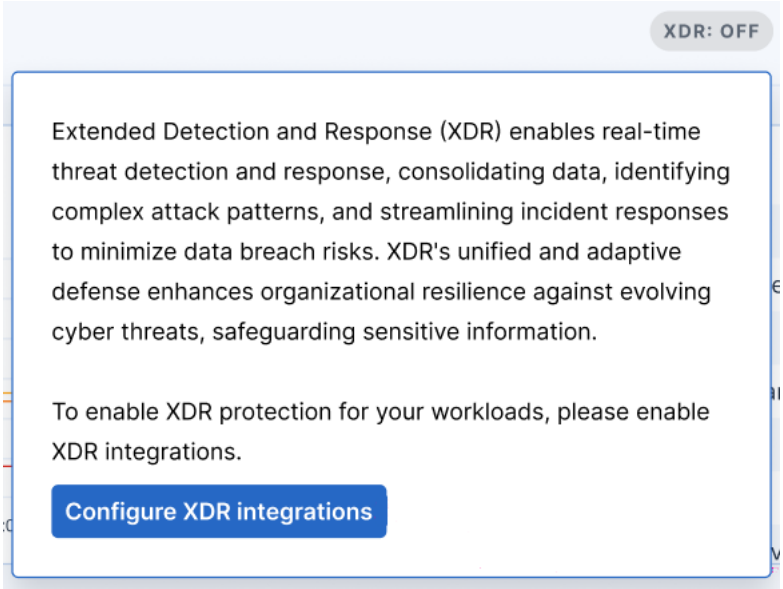
Important
Pour que la fonctionnalité XDR soit opérationnelle, l'option EDR (Endpoint Detection and Response) doit d'abord être activée dans les plans de protection concernés. De cette manière, le paramètre **XDR : Activé/Désactivé** est affiché pour les tenants clients. S'il n'est pas affiché, contactez l'administrateur partenaire.

Pour activer la fonctionnalité XDR

1. Assurez-vous que la fonctionnalité EDR est activée dans vos plans de protection. Pour plus d'informations, voir "Activation de la fonctionnalité EDR (Endpoint Detection and Response)" (p. 1255).
2. Accédez à **Protection** > **Incidents**.
3. En haut à droite de l'écran, cliquez sur 

.
4. Vous êtes invité à configurer les intégrations XDR qui sont nécessaires pour que la fonctionnalité XDR protège vos ressources. Cliquez sur **Configurer les intégrations XDR**.

© Acronis International GmbH, 2003-2026



Si vous avez des intégrations XDR existantes configurées et souhaitez ajouter des intégrations supplémentaires, cliquez sur **Ajouter des intégrations XDR**.

Vous êtes automatiquement redirigé vers le portail de gestion, où vous pouvez sélectionner et configurer les intégrations XDR pertinentes. Pour en savoir plus, consultez Intégration de Advanced Security + XDR avec des plateformes tierces.

Pour plus d'informations sur l'intégration avec Microsoft 365, consultez ces étapes d'intégration.

Pour plus d'informations sur l'intégration avec FortiMail Workspace Security (anciennement Perception Point), voir ces étapes d'intégration.

Lorsqu'une configuration XDR au moins est configurée, le paramètre de l'option XDR est activé XDR: ON et vous pouvez commencer à utiliser cette fonctionnalité.

Utilisation du graphique XDR

Le graphique XDR ajoute une autre perspective enrichie à l'affichage des incidents EDR (Endpoint Detection and Response) en mettant en corrélation les détections et les événements des sources de données XDR, y compris les métadonnées des e-mails et de gestion des identités.

Le type de nœuds affichés dans le graphique dépend des intégrations XDR. Par exemple, lorsqu'ils sont intégrés à la gestion des e-mails et des identités, le graphique affiche des nœuds d'e-mails, des nœuds de pièces jointes d'e-mail et des nœuds d'identités utilisateur. Lorsqu'ils sont intégrés aux services Microsoft 365, le graphique affiche des nœuds d'applications de collaboration telles que Teams, OneDrive et SharePoint.

Pour plus d'informations sur les différentes icônes de nœud affichées dans le graphique XDR, voir "Icônes du graphique XDR" (p. 1249).

Utilisez le graphique XDR pour :

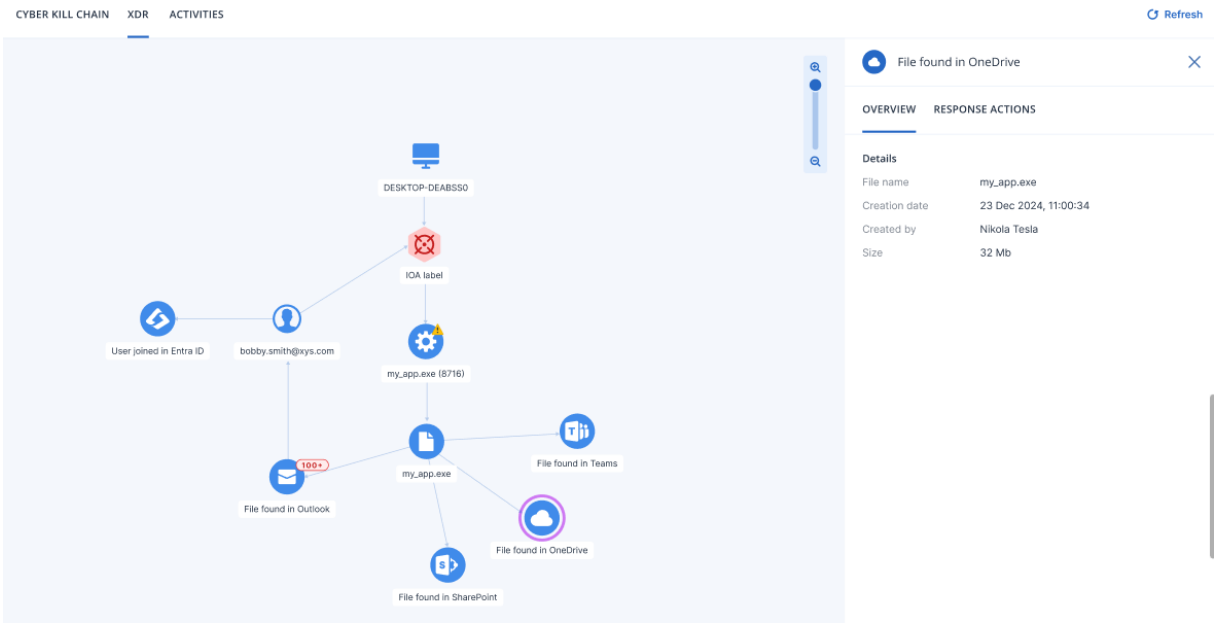
© Acronis International GmbH, 2003-2026

- Rechercher des nœuds individuels
- Appliquer des mesures d'intervention à un nœud
- Afficher les erreurs d'intégration

Pour accéder au graphique XDR, accédez à **Protection > Incidents**, cliquez sur l'incident pertinent, puis sur l'onglet **XDR**.

Pour actualiser le contenu du graphique XDR, cliquez sur Refresh.

Remarque
L'onglet **XDR** est affiché uniquement si la fonctionnalité XDR est activée. Pour plus d'informations, voir "Activation de la fonctionnalité XDR (Extended Detection and Response)" (p. 1243).



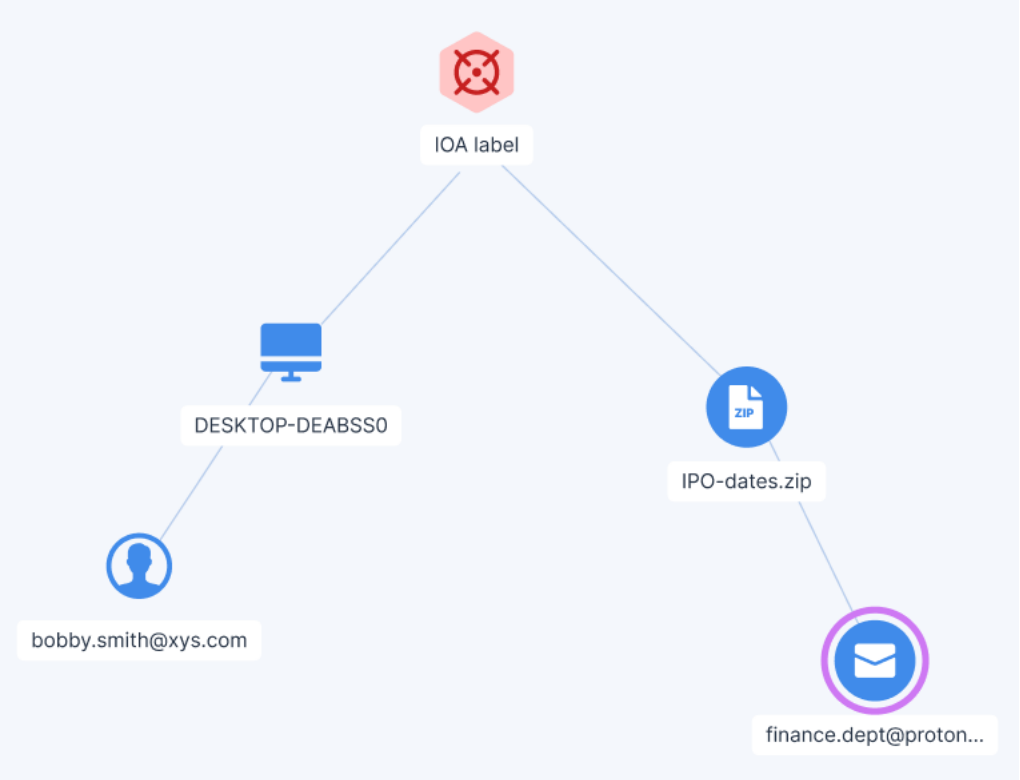
Procédure d'analyse du graphique XDR

La fonctionnalité XDR (Extended Detection and Response) ajoute des détails supplémentaires à un incident EDR (Endpoint Detection and Response), notamment la vérification de la provenance de la menace (pièce jointe, application de collaboration ou lien dans un e-mail) et l'utilisateur connecté et responsable de l'ouverture de la pièce jointe malveillante. En analysant le graphique XDR, vous disposez de contextes supplémentaires sur l'incident et savez si une action au-delà de la fonctionnalité EDR est requise, comme le blocage du compte utilisateur et/ou du destinataire de l'e-mail.

En examinant les nœuds affichés dans le graphique XDR ci-dessous, vous pouvez voir qu'une menace malveillante a été extraite d'un fichier zip joint à un e-mail téléchargé sur **DESKTOP-DEABSS0**. L'adresse e-mail de l'expéditeur était **finance.dept@proton.me**, et l'utilisateur qui s'est connecté et a ouvert le fichier zip était **bobby.smith@xys.com**.

© Acronis International GmbH, 2003-2026

En cliquant sur l'icône de bureau, vous voyez dans l'onglet **Vue d'ensemble** si la ressource est la ressource habituelle de l'utilisateur connecté. Si l'utilisateur s'est connecté avec un système d'exploitation ou une adresse IP qu'il n'a jamais utilisé auparavant, il y a de fortes chances que l'incident soit malveillant. Vous pouvez ensuite prendre les mesures correctives nécessaires aux utilisateurs sur les terminaux compromis pour vous assurer qu'ils n'ont pas accès aux données sensibles ni aux ressources informatiques.



D'autres éléments de graphique XDR vous aident à comprendre exactement ce qui s'est passé.

Par exemple, l'intégration XDR avec les services Microsoft 365 comprend les éléments suivants :

- Lorsqu'un fichier malveillant est situé dans une application Microsoft 365 (OneDrive, SharePoint, Teams ou Outlook), une ligne est affichée pour connecter le nœud du fichier malveillant à l'emplacement d'application de collaboration concerné.

De même, l'intégration XDR avec FortiMail Workspace Security (anciennement Perception Point) inclut ce qui suit :

- Lorsqu'un fichier malveillant est une pièce jointe directe d'un e-mail, une ligne est affichée pour connecter le nœud de fichier malveillant au nœud d'e-mail.
- Lorsque le nœud malveillant est un nœud d'URL, une ligne s'affiche pour connecter le nœud d'URL malveillant au nœud d'e-mail.
- Lorsqu'un fichier malveillant a été extrait d'une pièce jointe d'archive ZIP (ou d'un autre type d'archive compressée), un nœud de fichier est créé pour l'archive ZIP, et une ligne est affichée pour connecter le nœud de fichier malveillant au nœud de pièce jointe.

© Acronis International GmbH, 2003-2026

Recherche de nœuds individuels

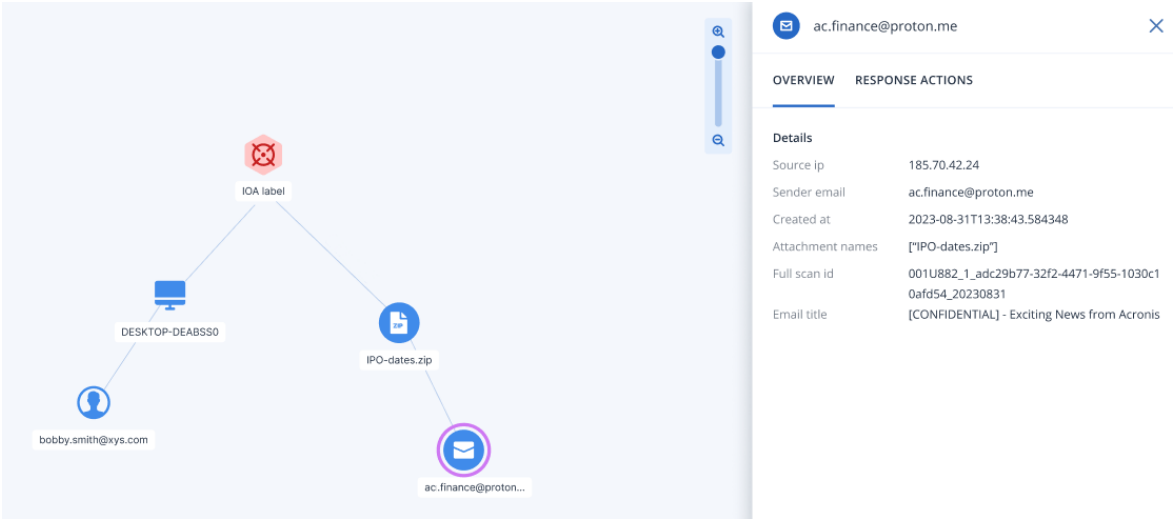
Vous pouvez afficher les détails de n'importe lequel des nœuds du graphique XDR. Cela vous permet de passer à des nœuds spécifiques du graphique, et d'enquêter et d'appliquer des mesures d'intervention à chaque nœud en fonction des besoins.

Les nœuds affichés varient en fonction des intégrations XDR implémentées. Les détails du nœud s'affichent dans l'onglet **Vue d'ensemble** et les mesures d'intervention disponibles pour ce nœud s'affichent dans l'onglet **Mesures d'intervention**.

Remarque
Aucune mesure d'intervention n'est disponible pour les nœuds Indicateurs de compromission (IoC) et Indicateurs d'attaque (IoA).

Pour rechercher des nœuds individuels

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents, cliquez sur dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter.
3. Cliquez sur l'onglet **XDR**.
4. Accédez au nœud pertinent, puis cliquez dessus pour afficher l'encadré correspondant.
   Par exemple, le fait de cliquer sur le nœud de messagerie dans l'exemple ci-dessous ouvre l'encadré correspondant.



5. Examiner les informations incluses dans les onglets de l'encadré :
   - **Vue d'ensemble** : cet onglet inclut des détails sur le nœud sélectionné, en fonction du type de nœud.
     - Nœuds Indicateur d'attaque (IoA) : inclut l'horodatage, la gravité et la description de la détection, la tactique et la technique MITRE, ainsi que le nom de la menace.
     - Nœuds Indicateur de compromission (IoC) : chaque type de nœud IoC (processus, fichier ou URL) possède son propre ensemble de champs qui sont également utilisés dans la

© Acronis International GmbH, 2003-2026

fonctionnalité EDR (Endpoint Detection and Response). Pour plus d'informations, voir "Examiner des nœuds de la cyber kill chain" (p. 1295).

- Nœuds d'intégration : comprend les détails sur le nœud sélectionné, en fonction de l'intégration.

  Par exemple, les nœuds Teams, OneDrive et SharePoint incluent le nom du fichier, sa date de création, l'utilisateur qui a créé le fichier, le dernier utilisateur à avoir modifié le fichier et la taille du fichier.

  De la même manière, le nœud des e-mails inclut des détails sur l'adresse IP de l'expéditeur, son nom et le client utilisé, ainsi que le nom, le format et la taille de chaque pièce jointe.

- **Mesures d'intervention** : ce volet répertorie les différentes mesures d'intervention disponibles, en fonction de l'intégration. Par exemple, le nœud de messagerie affiche des options permettant de bloquer l'adresse e-mail de l'expéditeur et de la considérer comme malveillante, et de supprimer les pièces jointes. Pour plus d'informations, voir "Application des mesures d'intervention" (p. 1248).

Application des mesures d'intervention

Vous pouvez appliquer diverses mesures d'intervention à des nœuds de graphique XDR. Ces mesures vous permettent d'assainir rapidement et facilement n'importe quel nœud.

Pour appliquer une mesure d'intervention

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents, cliquez sur  dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter.
3. Cliquez sur l'onglet **XDR**.
4. Accédez au nœud pertinent, puis cliquez dessus pour afficher l'encadré correspondant.

   Notez que, si le nœud est de type nœud d'identité, d'e-mail ou de collaboration groupé (ce qui est indiqué par un numéro d'étiquette sur le nœud), les mesures d'intervention appliquées à ce nœud sont appliquées à tous les sous-nœuds du nœud de groupe.
5. Cliquez sur l'onglet **Mesures d'intervention**.
6. Cliquez sur **Exécuter** pour la mesure d'intervention requise.

   Par exemple, le FortiMail Workspace Security prend en charge l'action de réponse de l'expéditeur sur la liste noire.

   Pour l'intégration de Microsoft 365, les mesures d'intervention de type arrêt de session, réinitialisation forcée de mot de passe et suspension de l'utilisateur sont disponibles.

   Remarque
   Lorsque vous cliquez sur **Exécuter**, les autres mesures d'intervention sont temporairement désactivées. Lorsque l'action est terminée, les autres mesures d'intervention sont activées.
7. (Facultatif) Cliquez sur l'onglet **Activités** pour examiner toutes les mesures d'intervention appliquées au nœud. Notez que les mesures d'intervention exécutées pour les incidents XDR

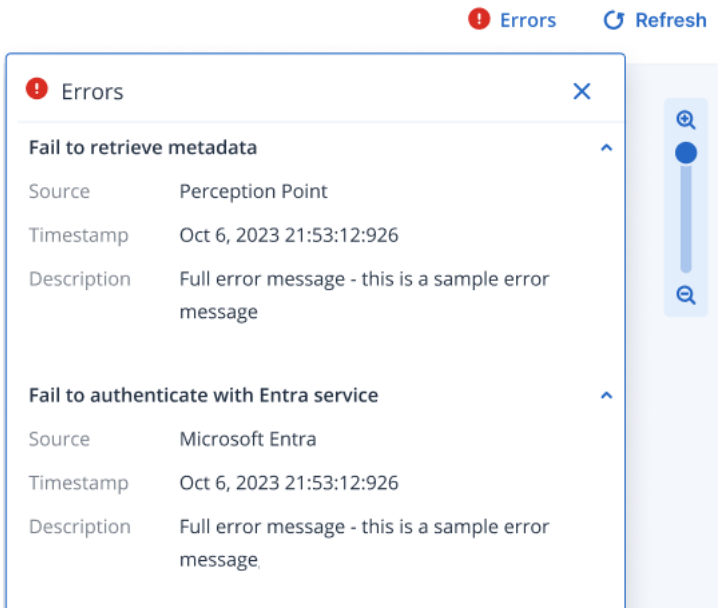
© Acronis International GmbH, 2003-2026

sont affichées avec les incidents EDR (Endpoint Detection and Response). Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Affichage des erreurs d'intégration XDR

En cas d'erreur lors de l'intégration avec des solutions XDR tierces, la boîte de dialogue Erreurs s'affiche. Cette boîte de dialogue affiche les erreurs d'intégration, y compris les échecs de connexion à la source d'intégration ou si l'intégration a été configurée de manière incorrecte.

La boîte de dialogue Erreurs s'affiche automatiquement (en cas d'erreurs) lorsque vous accédez au graphique XDR. Pour accéder à cette boîte de dialogue à tout autre moment, cliquez sur **Erreurs**, dans le coin supérieur droit du graphique XDR. Notez que le bouton **Erreurs** ne s'affiche pas si le graphique XDR ne comporte aucune erreur.



Icônes du graphique XDR

Le tableau ci-dessous répertorie les différentes icônes disponibles dans le graphique XDR.

Notez qu'un nœud peut être « groupé » pour inclure un certain nombre de nœuds du même type. L'icône de ce nœud groupé affiche le nombre de nœuds qui y sont contenus.

Par exemple, 

indique qu'il y a plus de 100 processus dans l'incident. Si le nombre de nœuds groupés est inférieur à 100, le nombre réel est affiché.

Icône	Description
	Indicateur de compromission (IoC) indiquant un processus générique ou injecté. L'icône porte le nom du processus, par exemple **nomduprocessus.exe**.

© Acronis International GmbH, 2003-2026

Icône	Description
	Indicateur de compromission (IoC) indiquant un fichier générique, exécutable, de document ou de script. L'icône porte le nom du fichier, par exemple **nomdefichier.dll**.
	Indicateur de compromission (IoC) indiquant une URL. L'icône porte le nom de l'URL, par exemple **abc.com**.
	Indicateur d'attaque (IoA). L'icône porte le nom de l'IoA, par exemple **Minikatz**.
	Ressource L'icône porte le nom de la ressource, par exemple **DESKTOP-D123**.
	Identité (utilisateur) L'icône indique l'identifiant du compte utilisateur, par exemple **david.durand@b.com**. Ce nœud inclut des informations acquises localement par l'agent, et ne nécessite donc pas de connexion à l'API Microsoft.
	Icône d'e-mail indiquant un e-mail générique Outlook, une pièce jointe ou une URL. Le nom de l'icône dépend de l'intégration concernée. Lors de l'intégration avec FortiMail Workspace Security (l'anciennement Perception Point), l'étiquette affiche l'adresse e-mail de l'expéditeur, par exemple **david.smith@b.com**. Lors de l'intégration avec Microsoft 365, l'indication **Fichier trouvé dans Outlook** est affichée.
	OneDrive L'icône indique **Fichier trouvé dans OneDrive**.
	SharePoint L'icône indique **Fichier trouvé dans SharePoint**.
	Teams L'icône indique **Fichier trouvé dans Teams**.
	Microsoft Entra ID L'icône indique l'identifiant de compte utilisateur, par exemple **david.durand@b.com**. Ce nœud inclut le nom principal de l'utilisateur (UPN) fourni par Entra ID. Cliquez sur le nœud pour afficher ce nom dans le champ **Nom d'utilisateur AD**.

© Acronis International GmbH, 2003-2026

Endpoint Detection and Response (EDR)

Remarque
Cette fonctionnalité fait partie du pack Advanced Security + XDR, qui fait à son tour partie du service de cyberprotection. Notez que, lorsque vous ajoutez la fonctionnalité EDR à un plan de protection, vous êtes susceptible de devoir vous acquitter de frais supplémentaires.

La fonctionnalité EDR détecte toute activité suspecte sur une ressource, y compris les attaques qui n'ont pas été identifiées. Elle génère des incidents qui présentent en détail chaque attaque, ce qui vous permet de comprendre comment l'attaque s'est produite et comment éviter qu'elle se reproduise. Grâce aux interprétations faciles à comprendre de chaque phase de l'attaque, le temps consacré aux enquêtes sur les attaques peut être réduit à quelques minutes.

À partir de la version C24.05, vous pouvez étendre votre fonctionnalité EDR avec Extended Detection and Response (XDR). Utilisez le graphique XDR pour obtenir une perspective enrichie des incidents EDR en corrélant les détections avec les événements provenant des sources de données XDR, incluant les métadonnées de gestion des e-mails et des identités. Pour plus d'informations, voir "XDR (Extended Detection and Response)" (p. 1242).

Utilité de la fonctionnalité EDR (Endpoint Detection and Response)

Aujourd'hui, les cybermenaces et les attaques malveillantes ne cessent de se développer, et la prévention n'est plus synonyme de protection complète. Malgré les différentes couches de prévention, certaines attaques parviennent toujours à se frayer un chemin et à pénétrer dans les réseaux. Les solutions classiques ne voient pas à quel moment l'intrusion se produit, ce qui laisse aux entités malveillantes la liberté de résider dans votre environnement pendant des jours, des semaines, voire des mois.

Les solutions EDR existantes, quant à elles, permettent d'empêcher ces « défaillances silencieuses », car elles recherchent les entités malveillantes et les suppriment dans les meilleurs délais. Toutefois, elles exigent généralement un niveau élevé d'expertise en matière de sécurité ou l'intervention coûteuse d'analystes du centre des opérations de sécurité. Par ailleurs, les analyses d'incident peuvent être extrêmement longues.

La fonctionnalité Acronis Advanced Security + EDR dépasse ces limites en détectant les attaques qui n'ont pas été identifiées. Vous pouvez ainsi comprendre comment une attaque s'est produite et comment éviter qu'elle se reproduise. Les enquêtes menées sur les attaques sont également plus rapides.

Voici en quoi la fonctionnalité EDR peut vous être utile :

- **Visibilité complète** : Vous comprenez l'événement qui s'est produit et comment il s'est produit, même pour les attaques qui n'ont pas été identifiées. L'évolution de chaque attaque est également représentée de manière visuelle, étape par étape (depuis le point d'entrée initial

© Acronis International GmbH, 2003-2026

jusqu'à l'affichage des données ciblées et/ou exfiltrées), ce qui vous permet de mesurer rapidement la portée et l'impact d'un incident. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287).

- **Réduction de la durée de l'enquête** : La durée de l'enquête concernant les incidents passe de quelques heures à quelques minutes. L'option EDR détaille chaque étape de l'attaque de manière claire, dans une langue facile à comprendre, ce qui évite d'avoir à faire appel à des spécialistes coûteux ou à des effectifs supplémentaires. Pour plus d'informations, voir "Enquête sur les incidents" (p. 1286).
- **Recherche de menaces connues dans les ressources** : Vous pouvez rechercher automatiquement dans les ressources des menaces issues de malware, des vulnérabilités, ainsi que d'autres types d'événements survenus dans le monde et qui peuvent avoir une incidence sur votre protection des données. Ces menaces, appelées incidents de compromission, sont basées sur les données concernant les menaces fournies par le centre opérationnel de cyberprotection (CPOC). Pour plus d'informations, voir "Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources" (p. 1300).
- **Réponse rapide aux incidents** : Grâce à l'accès à toutes les activités ultérieures à la violation et au détail de chaque étape de la kill chain, vous pouvez effectuer un certain nombre d'opérations pour traiter chaque point d'attaque. Vous pouvez notamment effectuer une enquête à l'aide du contrôle à distance et de la sauvegarde de données d'investigation (cette fonctionnalité n'est pas disponible dans la version à accès anticipé), mettre des ressources en quarantaine et supprimer des processus de malware. Vous pouvez également reprendre l'activité à l'aide de Disaster Recovery. Pour plus d'informations, voir "Atténuation d'incidents" (p. 1304).
- **Création de rapports fiables sur votre niveau de protection** : Grâce à l'option EDR, vous éliminez une grande part de l'insécurité et de la crainte liées à l'impact des cyberattaques sur votre activité. Par ailleurs, les informations relatives aux incidents sont stockées pendant 180 jours et peuvent être utilisées à des fins d'audit.

Fonctionnalités EDR

La fonctionnalité EDR (Endpoint Detection and Response) comprend les fonctionnalités suivantes :

- Recevoir des notifications d'alerte en cas de violation
- Gèrer vos incidents dans la page Incident
- Visualisation facile à comprendre du scénario de l'attaque
- Recommandations et étapes de réparation
- Consulter les attaques dévoilées publiquement sur vos ressources à l'aide de flux d'informations sur les menaces
- Vue d'ensemble dans le tableau de bord
- "Surveillance étendue" (p. 1254)
- Stocker les événements de sécurité pendant 180 jours

© Acronis International GmbH, 2003-2026

Recevoir des notifications d'alerte en cas de violation

La fonctionnalité EDR fournit des notifications d'alerte dès qu'un incident survient. Ces alertes sont mises en évidence dans le menu principal de la console Cyber Protect. Vous pouvez alors examiner une alerte en cliquant sur le bouton **Enquêter sur l'incident** qui vous redirige vers l'écran d'investigation sur l'incident (appelé également cyber kill chain).

Pour plus d'informations, voir "Examen des incidents" (p. 1259).

Gérer vos incidents dans la page Incident

La fonctionnalité EDR vous permet de gérer tous vos incidents dans la page Incidents (accessible depuis le menu **Protection** de la console Cyber Protect). La page **Incidents**, qui peut être filtrée en fonction de vos besoins, vous permet de comprendre facilement et rapidement l'état actuel de vos incidents, y compris leur gravité, la ressource affectée et le niveau de positivité. Vous pouvez également accéder directement à la cyber kill chain pour visualiser le scénario de l'attaque, nœud par nœud.

Pour plus d'informations sur la page Incidents, reportez-vous à "Examen des incidents" (p. 1259).

Visualisation facile à comprendre du scénario de l'attaque

La fonctionnalité EDR offre une représentation visuelle d'une attaque dans un format facile à lire. De cette manière, même le personnel non spécialisé dans la sécurité peut comprendre les objectifs et la gravité d'une attaque. Vous n'avez plus besoin des services d'un centre des opérations de sécurité ni d'embauche des spécialistes de la sécurité : la fonctionnalité EDR donne tous les détails concernant une attaque :

- Le mode de pénétration employé par l'entité malveillante
- Le mode employé par l'entité malveillante pour effacer sa trace
- Les dommages occasionnés
- Le mode de propagation de l'attaque

Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287).

Recommandations et étapes de réparation

La fonctionnalité EDR offre des recommandations claires et faciles à implémenter pour la résolution d'attaques sur une ressource. Pour résoudre une attaque rapidement, cliquez sur le bouton **Atténuer tout l'incident** pour afficher et suivre les étapes recommandées pour atténuer l'incident. Ces recommandations vous permettent de reprendre rapidement les opérations affectées par une attaque. Toutefois, si vous souhaitez suivre des étapes d'atténuation plus granulaires, vous pouvez accéder à chaque nœud et l'atténuer à l'aide de la mesure pertinente.

© Acronis International GmbH, 2003-2026

Vous pouvez également cliquer sur **Copilot** pour lancer Copilot, l'outil de chat assisté par l'IA et saisir plusieurs demandes, puis recevoir des mesures d'intervention suggérées pour l'incident sélectionné.

Pour plus d'informations, voir "Atténuation d'incidents" (p. 1304).

Consulter les attaques dévoilées publiquement sur vos ressources à l'aide de flux d'informations sur les menaces

La fonctionnalité EDR permet d'examiner les attaques connues et existant dans les flux d'informations sur les menaces visant vos ressources. Ces flux d'informations sur les menaces sont générés automatiquement en fonction des données de menaces reçues du Centre opérationnel de cyberprotection (CPOC). La fonctionnalité EDR vous permet de vérifier si une menace vise votre ressource, puis d'entreprendre les actions nécessaires pour la supprimer.

Pour plus d'informations, voir "Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources" (p. 1300).

Vue d'ensemble dans le tableau de bord

La fonctionnalité EDR offre toute une série de statistiques dans le tableau de bord de la console Cyber Protect. Vous y trouverez :

- L'actuel état des menaces, y compris le nombre d'incidents qui doivent faire l'objet d'une enquête.
- L'évolution des attaques, classées par gravité, avec indication de campagnes d'attaques possibles.
- Le taux d'efficacité de clôture des incidents.
- Les tactiques les plus utilisées pour attaquer vos clients.
- Le statut réseau de la ressource, c'est-à-dire si elle est isolée ou connectée.

Surveillance étendue

Sur les ordinateurs Windows et Linux, EDR peut collecter des données d’événements en continu, même en l’absence de détections particulières.

Important
La surveillance étendue consomme des ressources processeur supplémentaires sur la ressource protégée, nous recommandons donc de vérifier ses performances après avoir activé la fonctionnalité. Selon le nombre d’événements collectés, cela pourrait également augmenter la bande passante utilisée pour la communication avec le centre de données.

Stocker les événements de sécurité pendant 180 jours

La fonctionnalité EDR collecte des événements de ressource et d'application, et les stocke pendant 180 jours. Les événements qui précèdent la période de 180 jours sont supprimés (la suppression

© Acronis International GmbH, 2003-2026

d'événement est basée sur l'ancienneté, pas sur l'espace de stockage). Notez que, même si la fonctionnalité EDR est désactivée, tous les événements collectés précédemment pour une ressource sont conservés, et restent disponibles pour toute enquête relative aux incidents.

Exigences logicielles pour Endpoint Detection and Response

La fonctionnalité EDR (Endpoint Detection and Response) prend en charge les systèmes d'exploitation suivants :

- Microsoft Windows 7 Service Pack 1 et versions ultérieures
- Microsoft Windows Server 2008 R2 et versions ultérieures
- macOS versions 13, 14, 15, 26
- Versions du S.E. Linux :
  - CentOS 7.x
  - Debian 10.x, 11.x
  - CloudLinux 7.x, 8.x
  - Ubuntu 16.04, 18.04, 20.04, et 22.04

Remarque
Cette fonctionnalité n'est prise en charge que sur les processeurs suivants, qui prennent en charge le jeu d'instructions SSE4.2 :

- Processeurs Intel publiés après 2011
- Processeurs AMD publiés après 2012

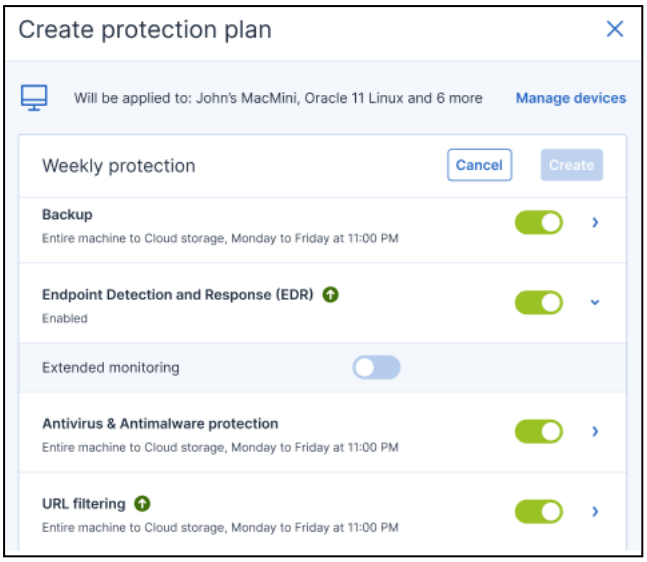
Activation de la fonctionnalité EDR (Endpoint Detection and Response)

Vous pouvez activer la fonctionnalité EDR dans tous les plans de protection.

Pour activer la fonctionnalité EDR

1. Dans la console Cyber Protect, accédez à **Gestion > Plans de protection**.
2. Sélectionnez le plan de protection pertinent dans la liste affichée, puis cliquez sur **Modifier** dans l'encadré de droite.
   Vous pouvez également créer un nouveau plan de protection et passer à l'étape suivante. Pour plus d'informations sur l'utilisation des plans de protection, reportez-vous à "Plans et modules de protection" (p. 243).
3. Dans l'encadré du plan de protection, activez le module **EDR (Endpoint Detection and Response)** en cliquant sur le commutateur à côté du nom du module.

© Acronis International GmbH, 2003-2026



4. Dans la boîte de dialogue affichée, cliquez sur **Activer**. Notez que vous pouvez activer la fonctionnalité EDR et désactiver n'importe laquelle des fonctionnalités Antivirus et antimalware, Active Protection et Filtrage d'URL dans le plan de protection.

© Acronis International GmbH, 2003-2026



Si vous n'avez pas la licence requise, l'icône d'avertissement de licence ( ) apparaît à côté du commutateur. L'icône **Detection and Response**, comme indiqué ci-dessous, est ajoutée à la liste des packs de protection requis pour l'implémentation du plan de protection.

✓ DETECTION AND RESPONSE

Remarque

Si vous ne résolvez pas le problème de licence, la fonctionnalité EDR sera désactivée lorsque le plan sera appliqué aux ressources.

© Acronis International GmbH, 2003-2026

5. [Facultatif] Pour collecter des données pour les événements EDR en continu, même en l'absence de détections particulières, activez **Surveillance étendue**.

   Important
   La surveillance étendue consomme des ressources processeur supplémentaires sur la ressource protégée, nous recommandons donc de vérifier ses performances après avoir activé la fonctionnalité. Selon le nombre d'événements collectés, cela pourrait également augmenter la bande passante utilisée pour la communication avec le centre de données.

   Les données collectées sur les événements de sécurité sont conservées pendant 180 jours sur le centre de données.

Remarque
Si vous activez **Antivirus Microsoft Defender** pour la protection en temps réel, le module **Protection en temps réel** est automatiquement désactivé afin d'éviter les conflits. Les détections de virus/malware et la mise en quarantaine sont gérées par Microsoft Defender Antivirus, et tous les incidents EDR liés aux détections de virus/malware sont créés à partir des informations fournies par Microsoft Defender Antivirus. EDR inclut d'autres moteurs de détection qui peuvent créer d'autres types d'incidents sans l'intervention de Microsoft Defender Antivirus.

De même, si vous activez la **Protection en temps réel**, le module **Antivirus Microsoft Defender** est automatiquement désactivé.

Les paramètres de protection contre la falsification dans Windows doivent également être désactivés pour garantir le bon fonctionnement de l'Antivirus Microsoft Defender dans Cyber Protect Cloud. Pour plus d'informations, consultez cet article de la base de connaissances.

En outre, si **Moteur de comportement** ou **Protection antivirus et antimalware** sont désactivés dans le plan de protection lorsque **Endpoint Detection and Response (EDR)** est activé, cette fonctionnalité est également désactivée.

Méthode d'utilisation de la fonctionnalité EDR (Endpoint Detection and Response)

La fonctionnalité EDR vous permet de détecter des attaques qui n'ont pas été identifiées. Vous pouvez ainsi comprendre comment une attaque s'est produite et comment éviter qu'elle se reproduise. Grâce aux interprétations faciles à comprendre de chaque phase de l'attaque, le temps consacré aux enquêtes sur les attaques peut être réduit à quelques minutes.

Le tableau ci-dessous décrit le workflow général de l'utilisation de la fonctionnalité EDR. À l'origine, vous allez examiner les nouveaux incidents, leur donner un niveau de priorité, enquêter plus en détail dans la cyber kill chain, puis prendre les mesures d'intervention pertinentes.

Étape	Mode d'utilisation de la fonctionnalité EDR
ÉTAPE 1 :	Dans la liste EDR des incidents :

© Acronis International GmbH, 2003-2026

Étape	Mode d'utilisation de la fonctionnalité EDR
Examiner les incidents	• Comprendre la posture de sécurité d'une organisation : combien d'incidents doivent faire l'objet d'une investigation ? • Comprendre les incidents les plus critiques et définir une priorité d'investigation en fonction de leur gravité. • Comprendre si les incidents sont nouveaux ou continus.
ÉTAPE 2 : Enquêter sur les incidents	Dans la cyber kill chain EDR : • Comprendre les objectifs de l'entité malveillante et affichage des techniques d'attaque utilisées. • Vérifier le degré de probabilité qu'un incident soit une véritable attaque malveillante. • Vérifier si un flux d'informations sur les menaces a un impact sur votre ressource. • Consulter les mesures d'intervention déjà appliquées à un incident.
ÉTAPE 3 : Atténuer les incidents	Dans les sections EDR d'atténuation : • Atténuer rapidement et facilement l'intégralité d'un incident en appliquant des mesures d'intervention globales. • Atténuer les différents points d'attaque d'un incident. • Appliquer des mesures visant à empêcher l'attaque (ou les futures attaques) de se propager ou d'affecter les ressources ciblées par l'entité malveillante.

Examen des incidents

La fonctionnalité EDR (Endpoint Detection and Response) fournit une liste des incidents qui comprend des actions de prévention (ou malware) et des détections suspectes sur une ressource. La liste des incidents offre une vue d'ensemble des attaques ou menaces qui affectent vos ressources, y compris les menaces qui doivent encore être atténuées.

Depuis la liste des incidents, vous pouvez déterminer rapidement :

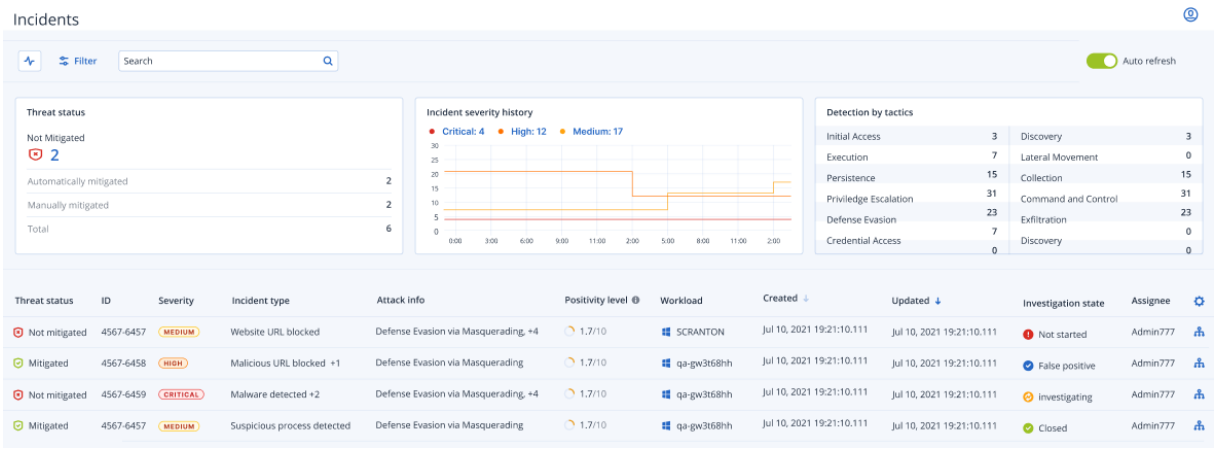
- La posture de sécurité d'une organisation : combien d'incidents doivent faire l'objet d'une investigation ?
- Quels sont les incidents les plus critiques et définir une priorité d'investigation en fonction de leur gravité.
- Si les incidents sont nouveaux ou continus.

Remarque
Lorsqu'un administrateur partenaire est connecté, vous pouvez consulter tous les incidents EDR sur un seul écran qui consolide les incidents de tous vos clients, sans avoir besoin d'accéder à la vue d'incident individuelle de chaque client. Une colonne supplémentaire **Clients** est affichée, incluant le nom du client auquel appartient chaque incident. De plus, les widgets affichés sur le tableau de bord **Vue d'ensemble** présentent des données d'indicateurs agrégées pour tous les clients.

© Acronis International GmbH, 2003-2026

La liste des incidents ci-dessous est accessible depuis le menu **Protection** de la console Cyber Protect. Pour plus d'informations sur l'examen des incidents figurant dans la liste, reportez-vous à "Prioriser les incidents nécessitant une attention immédiate" (p. 1261). Pour en savoir plus sur la date de création d'un incident, reportez-vous à la section Que sont les incidents exactement ?.

Remarque
Si les services gérés de détection et de neutralisation des menaces (MDR) sont activés sur vos ressources, une colonne supplémentaire **Ticket MDR** s'affiche. Elle indique le numéro de ticket fourni par le fournisseur MDR.



Remarque
La console Cyber Protect doit être ouverte pour que vous puissiez recevoir les notifications d'incident.

Que sont les incidents exactement ?

Les incidents, ou incidents de sécurité, peuvent être perçus comme des *conteneurs* comportant au moins un point de prévention ou de détection suspect (ou un mélange des deux) qui comprend tous les événements connexes et les détections d'une attaque. Ces incidents de sécurité peuvent également inclure d'autres événements bénins qui apportent un contexte supplémentaire.

De cette manière, vous pouvez visualiser les événements d'attaque d'un seul incident et comprendre les étapes logiques suivies par l'entité malveillante. Par ailleurs, la durée d'enquête sur une attaque est raccourcie.

Lorsque la fonctionnalité EDR est activée dans le plan de protection, les incidents de sécurité sont créés dans les cas suivants :

- **Une couche de prévention arrête quelque chose :** Ces incidents sont automatiquement fermés par le système, conformément aux paramètres du plan de protection. Toutefois, vous pouvez examiner précisément les opérations effectuées par le malware avant qu'il soit arrêté. Par exemple, le ransomware est arrêté lorsqu'il commence à chiffrer des fichiers, mais avant qu'il ait pu dérober des identifiants ou installé un service.

© Acronis International GmbH, 2003-2026

- **Une activité suspecte est détectée par la fonctionnalité EDR :** Il s'agit de détections qui devraient être examinées et traitées. En examinant la cyber kill chain visuelle améliorée (pour plus d'informations, reportez-vous à "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287)), vous pouvez facilement appliquer les actions d'atténuation pertinentes.

Prioriser les incidents nécessitant une attention immédiate

La liste des incidents de la console Cyber Protect est accessible à tout moment depuis le menu **Protection** de la console Cyber Protect. La liste des incidents offre une vue d'ensemble des attaques ou menaces, ce qui vous permet de donner la priorité aux incidents nécessitant une attention particulière.

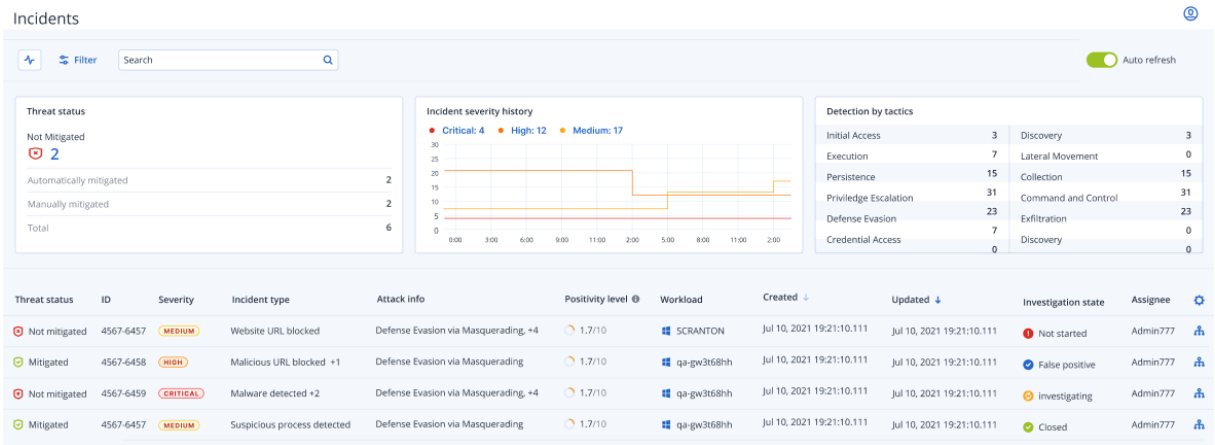
Important
Pour que les ressources restent sécurisées, analysez les incidents et donnez *toujours* la priorité à ceux qui sont en cours ou non atténués.

Comment analyser les incidents de sécurité nécessitant une attention immédiate

La liste des incidents vous permet d'analyser les incidents répertoriés et de donner la priorité à ceux nécessitant une attention particulière. Vous pouvez :

- Afficher les incidents non atténués : Vous pouvez rapidement comprendre, depuis la liste des incidents, si des attaques sont en cours. Les incidents non atténués (leur état est indiqué dans la colonne **Statut de la menace**) doivent être examinés immédiatement. Par défaut, la liste des incidents est filtrée pour afficher ces incidents.
- Comprendre la portée et l'impact des incidents : En fonction du filtrage des attaques, nouvelles ou continues, vous pouvez comprendre la gravité des incidents filtrés, ainsi que leur impact sur votre activité.

Après avoir affiné la liste des incidents les plus importants, vous pouvez alors analyser les détails d'un incident afin de mieux comprendre cet incident, ainsi que les techniques utilisées par une entité malveillante pour atteindre son objectif. Pour plus d'informations, voir "Analyser les détails de l'incident" (p. 1265).

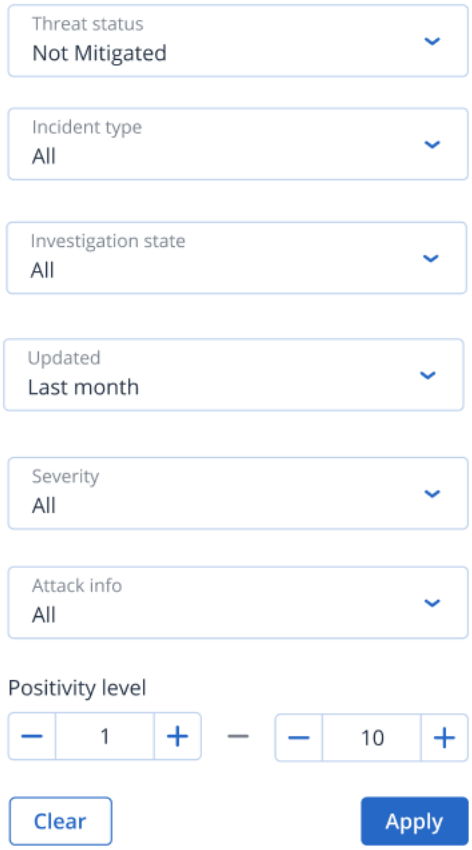


© Acronis International GmbH, 2003-2026

Remarque
Par défaut, la liste des incidents est triée en fonction de la colonne **Mis à jour**, qui indique la date et l'heure de la dernière mise à jour des incidents avec de nouvelles détections enregistrées dans l'incident. Notez que tout incident existant peut être mis à jour à tout moment, même s'il a été clôturé. Vous pouvez également filtrer la liste afin d'afficher les attaques nouvelles ou continues en fonction de vos besoins, en suivant la procédure ci-dessous.

Pour filtrer la liste des incidents

1. En haut de la liste des incidents, cliquez sur **Filtrer** pour la filtrer. Par exemple, si vous sélectionnez une date de début et une date de fin dans le champ **Créé**, la liste des incidents et les widgets affichent les incidents pertinents créés pendant la période définie.



2. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Affichage des incidents non atténués

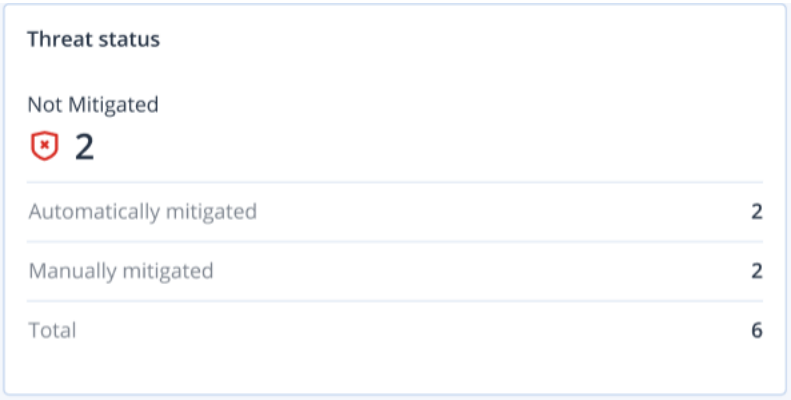
Vous pouvez voir le statut d'une menace dans la colonne **Statut de la menace**, qui indique si l'incident est **Atténué** ou **Non atténué**. Le statut de la menace est défini automatiquement par la fonctionnalité EDR ; tout incident n'étant pas atténué doit faire l'objet d'une enquête dans les plus brefs délais.

Vous pouvez alors affiner encore la liste des incidents en appliquant des filtres. Par exemple, si vous souhaitez filtrer la liste en fonction du statut de la menace *et* d'un niveau de gravité spécifique,

© Acronis International GmbH, 2003-2026

sélectionnez les options de filtre pertinentes. Après avoir filtré les incidents qui vous intéressent, vous pouvez alors effectuer une enquête, comme décrit dans "Enquête sur les incidents" (p. 1286).

Vous pouvez également utiliser le widget **Statut de la menace**, comme indiqué ci-dessous, afin d'avoir une vue d'ensemble du statut de la menace. Notez que les données affichées dans ce widget reflètent les filtres que vous avez appliqués ; reportez-vous à " Pour filtrer la liste des incidents" (p. 1262).



Compréhension de la portée et de l'impact des incidents

Vous pouvez comprendre rapidement la portée et l'impact des incidents en examinant les colonnes **Gravité**, **Informations concernant l'attaque** et **Niveau de positivité**. Comme indiqué ci-dessus, vous pouvez filtrer encore ces colonnes après avoir déterminé quels sont les incidents en cours. Pour ce faire, procédez comme suit :

- Examinez les incidents qui sont les plus critiques dans la colonne **Gravité**. L'état de gravité d'un incident peut être **Critique**, **Élevé** ou **Moyen**.
  - **Critique :** Il existe un fort risque de cyberactivité malveillante, avec un risque de compromission des hôtes critiques de votre environnement.
  - **Élevé :** Il existe un risque élevé de cyberactivité malveillante, avec un risque de dommages graves dans votre environnement.
  - **Moyen :** Il existe un risque accru de cyberactivité malveillante.

    Remarque
    Lors de la détermination de la gravité, l'algorithme EDR prend en compte le type de ressource, ainsi que la portée de chaque étape de l'attaque. Par exemple, un incident qui inclut des étapes relatives à l'usurpation d'identifiants est défini comme **Critique**.

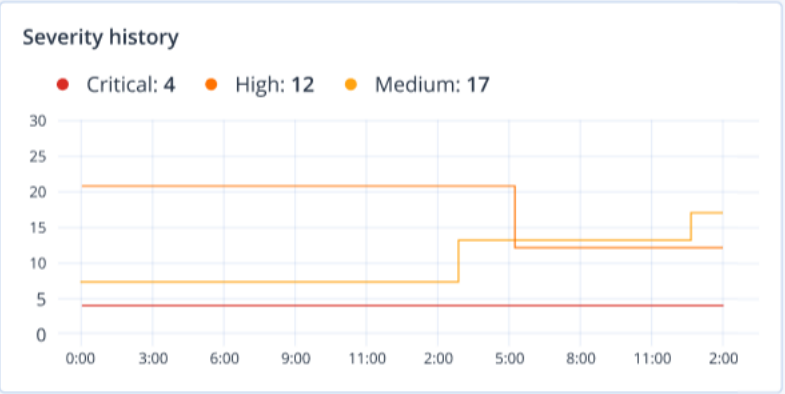
- La colonne **Type d'incident** permet de comprendre pourquoi un incident a été créé. Le type d'incident peut comprendre un ou plusieurs des éléments suivants :
  - **Ransomware détecté**
  - **Malware détecté**
  - **Processus suspect détecté**
  - **Processus malveillant détecté**

© Acronis International GmbH, 2003-2026

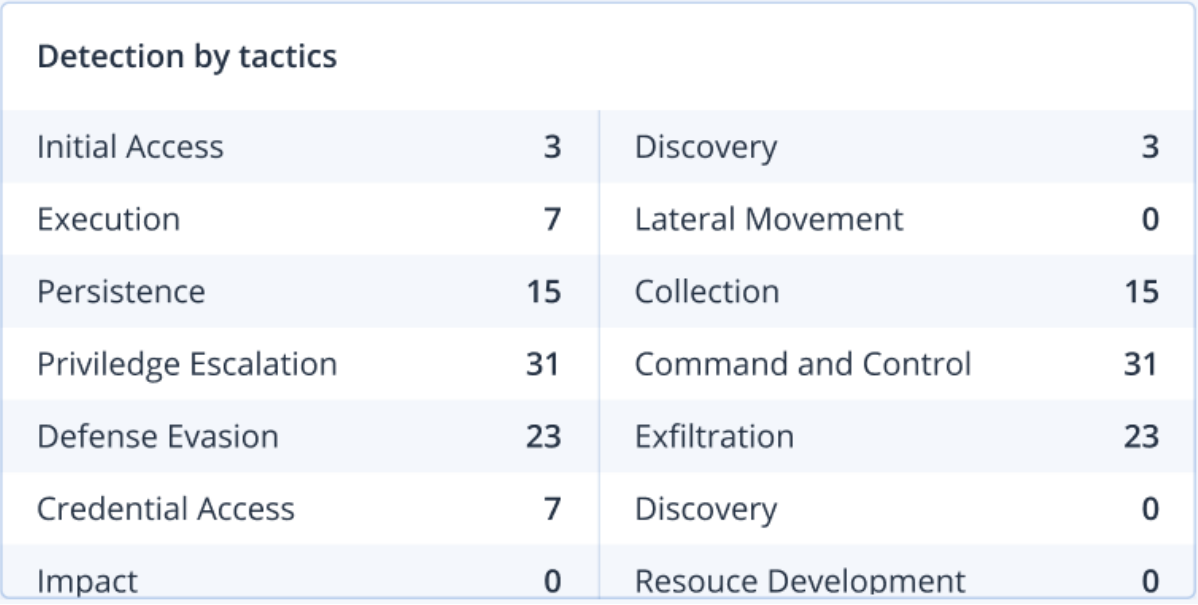
  - **URL suspectes bloquées**
  - **URL malveillante bloquée**
- Déterminez les techniques d'attaque utilisées dans la colonne **Informations concernant l'attaque**, puis évaluez s'il existe un thème ou un modèle commun aux attaques.
- Vérifiez si un incident est susceptible d'être une véritable attaque malveillante : la colonne **Niveau de positivité** indique une note comprise entre 1 et 10 (plus la note est élevée, plus l'attaque est susceptible d'être une véritable attaque malveillante).

Après avoir identifié les incidents qui nécessitent une attention immédiate, vous pouvez alors effectuer une enquête, comme décrit dans "Enquête sur les incidents" (p. 1286).

Vous pouvez également utiliser les widgets **Historique de gravité de l'incident** et **Détection par tactique** afin d'avoir une vue d'ensemble de la gravité et des techniques d'attaque.



Le widget **Détection par tactique** affiche les différentes techniques d'attaque utilisées, avec des valeurs en vert ou en rouge qui indiquent l'augmentation ou la diminution par rapport à la période précédente spécifiée. Ce widget fournit une vue consolidée de tous les objectifs des incidents filtrés, ce qui permet d'avoir une vue rapide de l'impact sur vos clients.



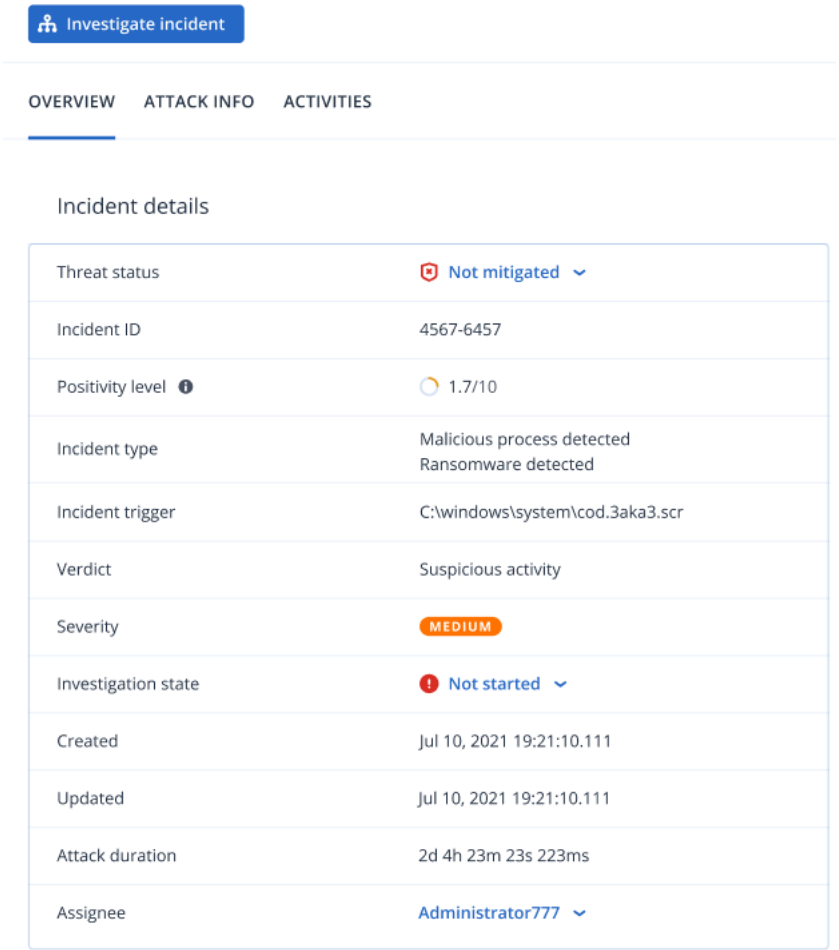
© Acronis International GmbH, 2003-2026

Analyser les détails de l'incident

Pendant la phase d'examen des incidents, vous pouvez également analyser les détails de chaque incident depuis la liste des incidents de la fonctionnalité EDR (Endpoint Detection and Response). Ces informations détaillées vous permettent d'examiner l'intégralité de l'incident et de comprendre comment et à quel moment il est survenu. Par ailleurs, vous pouvez attribuer un incident à des utilisateurs spécifiques à des fins d'examen, et définir le statut d'enquête.

Pour analyser les détails de l'incident

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**. La liste des incidents s'affiche.
2. Cliquez sur l'incident que vous souhaitez examiner. Les détails de l'incident sélectionné s'affichent.
3. Dans l'onglet **Vue d'ensemble**, vous pouvez examiner les détails de l'incident et de la ressource, y compris le statut et la gravité de la menace. Vous pouvez également définir l'**état de l'enquête** (vous avez le choix parmi **Enquête en cours**, **Non démarré** (état par défaut), **Faux positif** ou **Fermé**), puis sélectionnez l'utilisateur auquel vous souhaitez attribuer l'incident dans la liste déroulante **Cessionnaire**.



© Acronis International GmbH, 2003-2026

4. Cliquez sur l'onglet **Informations concernant l'attaque** pour examiner les détails de l'attaque et les techniques qu'elle utilise. Cliquez sur le lien situé en regard de la technique d'attaque répertoriée afin d'examiner plus en détail les informations sur la technique sur MITRE.org.
5. Cliquez sur l'onglet **Activités** pour examiner les actions entreprises dans la cyber kill chain afin d'atténuer l'incident. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287).
   Par exemple, si un correctif a été installé sur la ressource, vous voyez qui l'a installé, la durée de son installation et toutes les erreurs qui sont survenues pendant son implémentation.
6. Cliquez sur **Enquêter sur l'incident** pour accéder à la cyber kill chain dans laquelle vous pouvez enquêter sur l'incident, nœud par nœud. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287).

Recherche d'indicateurs de compromission (IoC) et d'activités suspectes

Pour détecter et atténuer les menaces avant qu'elles ne se transforment en incidents à fort impact, utilisez la fonction de **recherche d'événements**. Cette fonction de recherche vous permet de repérer les IoC et les activités suspectes dans toutes les ressources dotées de la fonction EDR (Endpoint Detection and Response).

Utilisez la fonction de **recherche d'événements** pour :

- Exécuter des requêtes personnalisées sur les données d'événements collectées à partir de toutes les ressources pour rechercher des hachages. Vous pouvez également obtenir des indicateurs pour répondre à certaines questions (par exemple, afficher les ressources présentant un nombre anormalement élevé de processus).
- Filtrer les requêtes à l'aide d'attributs fournis par les terminaux EDR et de données provenant d'autres intégrations telles que les activités du système d'exploitation, de l'utilisateur et du réseau.
- Affichez un résumé intuitif des données en fonction de vos requêtes pour vous aider dans l'investigation d'incidents ou la recherche de menaces.
- Enregistrez et partagez des requêtes avec les utilisateurs de la même organisation.

La fonction de **recherche d'événements** est accessible à partir du menu **Protection** de la console Cyber Protect.

Remarque
La période de rétention par défaut des résultats de la recherche d'événements EDR est de sept jours.

Recherche d'événements

Vous pouvez rechercher des événements EDR (Endpoint Detection and Response) dans toutes les ressources protégées par EDR.

© Acronis International GmbH, 2003-2026

Remarque
Vous pouvez effectuer une recherche d'événements uniquement au sein d'un client sélectionné.

Si vous utilisez la console Cyber Protect au niveau du tenant partenaire (lorsque **Tous les clients** est sélectionné), vous ne pouvez pas rechercher des événements de tous vos clients gérés.

Pour rechercher des événements

1. Dans la console Cyber Protect, accédez à **Protection** > **Recherche d'événements**.
2. Saisissez votre requête de recherche à l'aide du langage de requête Acronis XDR (XQL) et définissez une plage d'heures.

   Notez que le langage XQL utilise la saisie automatique pour vous aider à construire une requête. Pour plus d'informations sur la syntaxe et les options de requête disponibles, voir "Exemples de requêtes" (p. 1275).

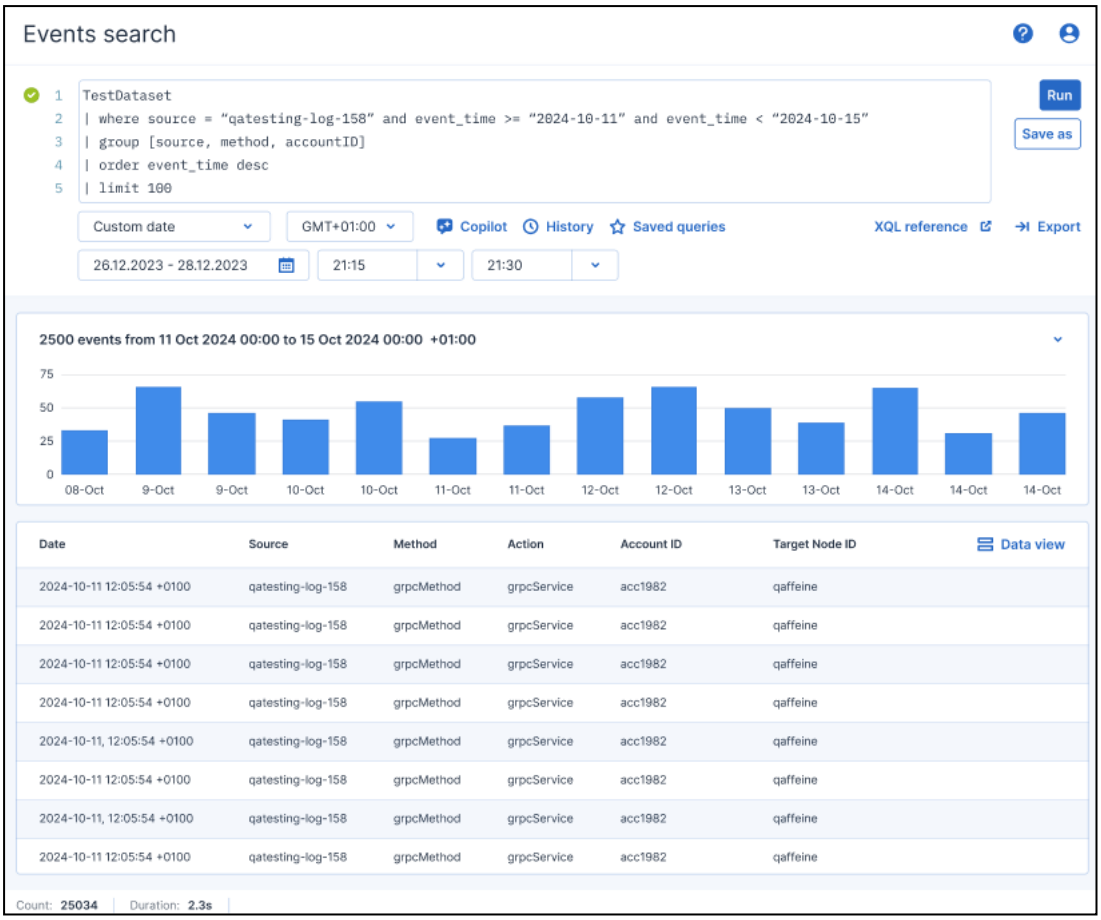
   Lors de la création de la requête, les opérations suivantes sont également disponibles :
   - Appuyez sur **Entrée** pour envoyer le curseur à la ligne suivante. Le caractère « | » est également ajouté au début de la nouvelle ligne (ce qui est utile lors de l'écriture de requêtes en plusieurs étapes).
   - Appuyez sur **Maj+Entrée** pour envoyer le curseur à la ligne suivante.

   Remarque
   Pour utiliser l'une des dix dernières requêtes exécutées, cliquez sur **Historique**, puis sélectionnez la requête concernée. Le champ de requête de recherche est automatiquement rempli avec la requête. Pour en savoir plus, consultez "Utilisation des requêtes enregistrées" (p. 1271).
3. Cliquez sur **Exécuter** pour lancer la requête.

   Vous pouvez également appuyer sur **Ctrl+Entrée** pour exécuter la requête.

   Les résultats de la requête s'affichent. Pour plus d'informations, voir "Affichage et compréhension des résultats de requête" (p. 1269).

© Acronis International GmbH, 2003-2026



4. Affinez votre recherche si nécessaire. Par exemple, choisissez d'afficher des champs ou des événements spécifiques contenant un certain nom de fichier.
5. [Facultatif] Pour enregistrer la requête actuelle, cliquez sur **Enregistrer sous**. Pour en savoir plus, consultez "Utilisation des requêtes enregistrées" (p. 1271).

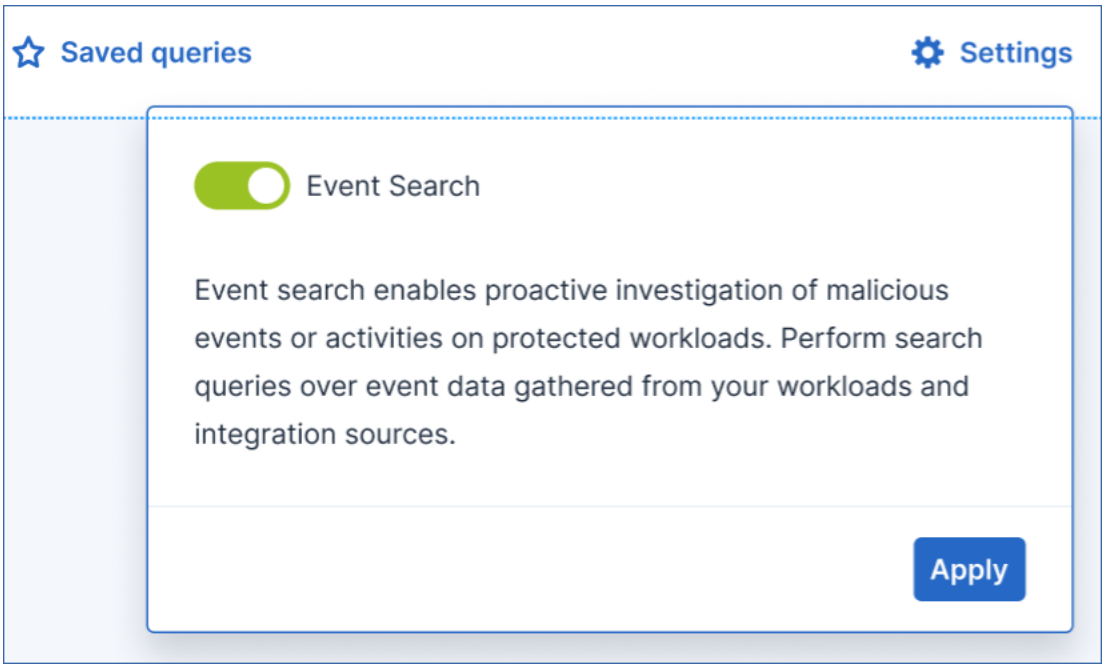
Désactivation de la recherche d'événements

La recherche d'événements nécessite de stocker et de traiter les données d'événements dans un entrepôt de données cloud tiers externe. Si vous ne souhaitez pas que les données d'événements soient stockées en dehors de votre centre de données, vous pouvez désactiver la recherche d'événements pour les événements EDR.

Pour désactiver la recherche d'événements

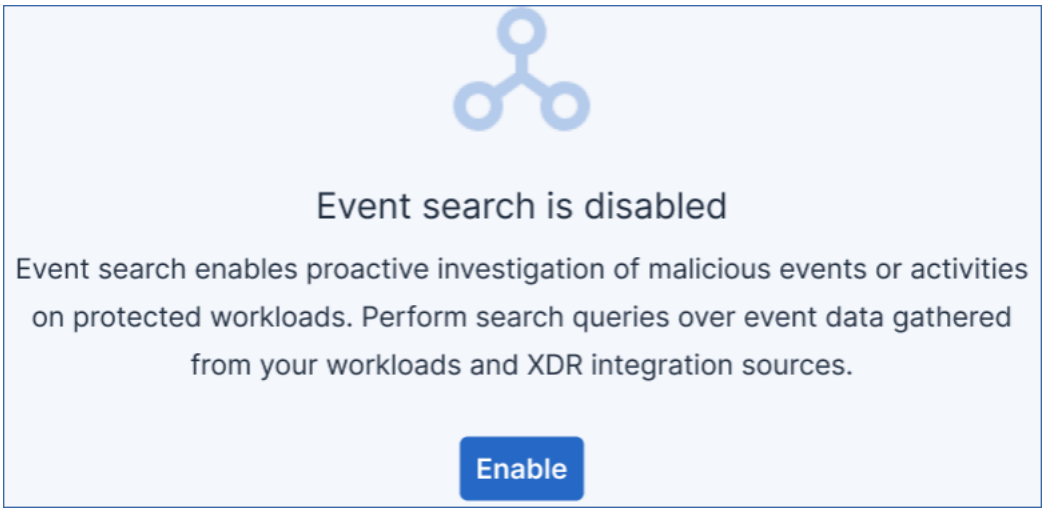
1. Dans la console Cyber Protect, accédez à **Protection** > **Recherche d'événements**.
2. Au-dessus de la liste des requêtes de recherche, cliquez sur **Paramètres**.

© Acronis International GmbH, 2003-2026



3. Désactivez le commutateur **Recherche d'événements**, puis cliquez sur **Appliquer**.

Le message **Recherche d'événements désactivée** reste à l'écran.



Pour réactiver la recherche d'événements

Cliquez sur **Activer**.

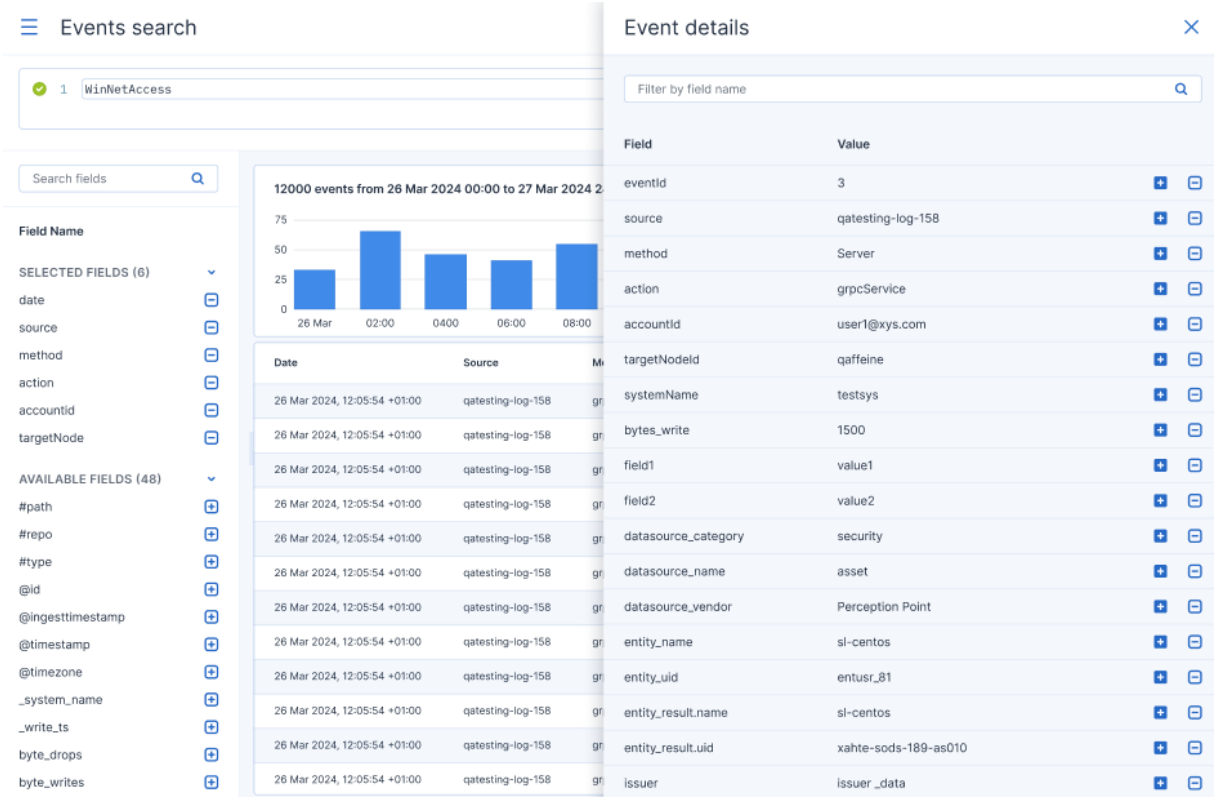
Affichage et compréhension des résultats de requête

Lorsque vous avez défini et exécuté votre requête de recherche (voir "Recherche d'événements" (p. 1266)), les résultats s'affichent sous la zone de requête de recherche dans une vue de disposition de tableau. À partir de cette vue, vous pouvez effectuer les opérations suivantes :

- Affichez tous les événements de la période sélectionnée.
- Cliquez sur une ligne d'événement pour afficher les détails d'un événement.

© Acronis International GmbH, 2003-2026

- Ajoutez ou supprimez des colonnes affichées dans les résultats de la requête. Voir "Ajout ou suppression de colonnes dans la vue de disposition en tableau" (p. 1270).
- Basculez vers la **vue Données**, qui affiche toutes les données d'événement au format JSON.
- Survolez une colonne dans le graphique à barres pour afficher la date, le fuseau horaire, le nombre et la durée des événements.



Ajout ou suppression de colonnes dans la vue de disposition en tableau

Dans la vue de disposition en tableau, il existe trois façons d'ajouter ou de supprimer les colonnes affichées dans les résultats de la requête :

- Dans le volet **Nom du champ**, cliquez sur ⊕ à côté du nom du champ pertinent (dans la section **Champs disponibles**) pour ajouter ce champ en tant que colonne dans les résultats de la requête.

  Pour supprimer une colonne, cliquez sur ⊖ à côté du nom du champ pertinent (dans la section **Champs sélectionnés**).
- Cliquez sur un événement pour afficher le volet **Détails de l'événement**, puis cliquez sur ⊕ ou sur ⊖ pour ajouter ou supprimer le champ pertinent des résultats de la requête de recherche.
- Survolez une colonne pour afficher une icône X. Cliquez sur cette icône pour supprimer la colonne.

© Acronis International GmbH, 2003-2026

Si vous incluez l'opérateur `Column` dans la requête, seuls les champs spécifiés par l'opérateur `Column` sont affichés dans la vue de disposition du tableau. Vous pouvez toujours ajouter ou supprimer des champs via le panneau **Champs**.

Si la requête n'inclut pas l'opérateur `Column`, les résultats sont affichés par défaut dans la disposition de la **vue de données** (au format JSON). Cependant, vous pouvez cliquer sur **Vue de tableau** pour passer d'une vue à l'autre, ou ajouter des champs via le panneau **Champs** pour passer automatiquement à la **vue de tableau** dans laquelle ne sont affichés que les champs que vous avez sélectionnés.

Pour plus d'informations sur l'opérateur `Column` et d'autres éléments XQL, voir "Exemples de requêtes" (p. 1275).

Remarque
Une fois que vous avez ajouté ou supprimé des colonnes via le volet **Détails de l'événement** ou le panneau **Champs**, la requête est automatiquement réexécutée.

Utilisation des requêtes enregistrées

La fonctionnalité **Recherche d'événements** vous permet d'enregistrer, de réutiliser et de mettre à jour des requêtes, selon les besoins. Vous pouvez :

- Enregistrer une nouvelle requête
- Exécuter une requête enregistrée auparavant
- Mettre à jour une requête enregistrée
- Supprimer une requête

Pour enregistrer une nouvelle requête

1. Dans la console Cyber Protect, accédez à **Protection** > **Recherche d'événements**.
2. Définissez votre requête dans la zone de requête de recherche. Pour plus d'informations sur la syntaxe et les options de requête disponibles, voir "Exemples de requêtes" (p. 1275).
3. Cliquez sur **Enregistrer sous**.
4. Dans la boîte de dialogue **Enregistrer la nouvelle requête**, définissez les éléments suivants :
   - Saisissez un nom de requête unique et, si besoin, ajoutez une description (facultatif).
   - Cochez la case **Enregistrer le filtre de temps** pour que le filtre de date défini soit inclus dans la requête.
   - Cochez la case **Autoriser les autres à utiliser cette requête** pour que d'autres utilisateurs du même tenant de client puissent utiliser la requête. Si cette case n'est pas cochée, seuls l'administrateur, l'administrateur d'entreprise et l'utilisateur qui a créé la requête peuvent utiliser la requête.
5. Cliquez sur **Enregistrer**.

   Lorsque vous enregistrez une requête, seule sa partie texte et la plage horaire sélectionnée sont enregistrées.

© Acronis International GmbH, 2003-2026

Remarque
Un maximum de 300 requêtes peuvent être enregistrées par compte tenant de client. Une fois cette limite atteinte, vous serez invité lors de l'enregistrement de requête suivant à supprimer d'abord une requête enregistrée avant d'enregistrer la nouvelle requête.

Pour exécuter une requête enregistrée auparavant

1. Dans la zone de recherche de requêtes, cliquez sur **Requêtes enregistrées**.
2. Dans la liste des requêtes enregistrées, cliquez sur la requête pertinente.
   La requête est ajoutée à la zone de requête de recherche, puis est exécutée automatiquement.

Pour mettre à jour une requête enregistrée

1. Dans la zone de recherche de requêtes, cliquez sur **Requêtes enregistrées**.
2. Dans la liste affichée des requêtes enregistrées, survolez la requête que vous souhaitez mettre à jour et cliquez sur l'icône en forme de crayon.
3. Apportez les modifications nécessaires à la requête, puis cliquez sur **Enregistrer**.
   Pour plus d'informations sur les champs modifiables, voir Pour enregistrer une nouvelle requête.
4. [Facultatif] Cliquez sur la requête enregistrée pour l'exécuter.

Pour supprimer une requête

1. Dans la zone de recherche de requêtes, cliquez sur **Requêtes enregistrées**.
2. Dans la liste des requêtes enregistrées, survolez la requête à supprimer, puis cliquez sur l'icône de la corbeille.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Langage d'interrogation XDR d'Acronis (XQL)

Utilisez le langage XQL pour rechercher des événements Endpoint Detection and Response (EDR), puis accédez aux événements recherchés. Cette section énumère les différents éléments de XQL avec lesquels vous devez vous familiariser lors de la recherche d'événements EDR :

- Syntaxe (y compris des exemples de requêtes)
- Types et champs d'événements

Pour plus d'informations sur l'utilisation de la fonctionnalité de **recherche d'événements**, voir "Recherche d'indicateurs de compromission (IoC) et d'activités suspectes" (p. 1266).

Syntaxe

Opération	Exemple
Sélection de la source de données et de colonnes	`eventType`

© Acronis International GmbH, 2003-2026

Opération	Exemple
Sélectionne la source de données et les colonnes sur lesquelles la requête doit s'appliquer. Cet opérateur doit être le premier de la requête. Les requêtes de sélection de sources de données et de colonnes ne sont pas sensibles à la casse.	`eventType | where column = 'string'`

Filtrage des données
 	
Filtre les données sur la base de conditions et doit commencer par le mot-clé `where`.
 	
Notez les options de filtrage suivantes :
 	
• Des guillemets simples ou doubles peuvent être ajoutés de part et d'autre de chaînes de caractères.
• Les recherches dans les colonnes sont sensibles à la casse par défaut. Pour effectuer une recherche insensible à la casse, utilisez « ~= » :
`eventType | where column = 'String'` est sensible à la casse et ne correspond qu'à `'String'`.
`eventType | where column ~= 'String'` n'est pas sensible à la casse et correspond à tous les cas de `'string'`.
• Les opérateurs logiques tels que `AND` et `OR` peuvent être utilisés pour combiner les filtres.
`key = value AND key < value OR key = value`
• Des parenthèses peuvent être ajoutées de part et d'autre des opérateurs :
`(key = value) AND (key < value OR key = value)`
• Utilisez `CONTAINS` pour une correspondance partielle des chaînes de caractères :
`key CONTAINS 'value'`
• Lors de la recherche dans les colonnes, la valeur `CONTAINS` peut inclure des éléments uniques ou une liste d'éléments :
`CONTAINS 'String'`
`CONTAINS ('String1', 'String2', 'String3')`
• Utilisez `ICONTAINS` pour une correspondance partielle entre les chaînes de caractères, sans tenir compte des majuscules et des minuscules :
`key ICONTAINS 'value'`
• Utilisez `IN` pour vérifier l'appartenance (sensible à la casse) :
`key IN ('value1', 'value2')`
• Utilisez IIN pour la vérification de l'appartenance (non sensible à la casse) :
`key IIN ('value1', 'value2')`
• Utilisez `ago` pour filtrer les dates. Cette syntaxe n'accepte qu'une valeur numérique suivie de jours (d), d'heures (h), de minutes (m)
	`eventType | where field == 'value'`
	
	`eventType | where field != 'value'`
	
	`eventType | where field > 'value'`
	
	`eventType | where field < 'value'`
	
	`eventType | where field >= 'value'`
	
	`eventType | where field <= 'value'`
	
	`eventType | where field CONTAINS 'substring'`
	
	`eventType | where field NOT CONTAINS 'substring'`
	
	`eventType | where field ICONTAINS 'substring'`
	
	`eventType | where column ICONTAINS 'substring'`
	
	`eventType | where field NOT ICONTAINS 'substring'`
	
	`eventType | where column NOT ICONTAINS 'substring'`
	
	`eventType | where field IN ('value1', 'value2')`
	
	`eventType | where column IIN ('value1'. 'value2')`
	
	`eventType | where field NOT IN ('value1', 'value2')`
	
	`eventType | where field MATCHES 'value1*'`
	
	`eventType | where field NOT MATCHES 'value1*'`

© Acronis International GmbH, 2003-2026

Opération	Exemple

ou de secondes (s) :
`column < ago(3d)`
`column < ago(3h)`
`column < ago(3m)`
`column < ago(30s)`
• Utilisez la correspondance des expressions régulières (regex) conformément à la norme RE2 :
`key MATCHES 'regex string'`
	`eventType | where event_time > ago(5d)`

Choix des champs Spécifie les champs à sélectionner et à renvoyer à partir d'une requête.	`eventType | columns field1, field2, field3 ...`

Tri
Trie les résultats de la requête, dans l'ordre croissant ou décroissant. Si aucun ordre n'est spécifié, l'ordre par défaut est croissant.
	`eventType | order field1, field2, field3 ...`
	`eventType | order field asc`
	`eventType | order field desc`

Recherche dans des colonnes Recherche une chaîne dans toutes les colonnes d'un tableau.	`eventType | search 'query string'`
Limite Limite le résultat de la requête.	`eventType | limit 10` `eventType | limit 1000 | group [field1, field2] | limit 10`

Fonctionnement du groupe
Effectue une `group operation` sur les données.
(Facultatif) Vous pouvez spécifier les fonctions d'agrégation à exécuter sur les champs agrégés, ou spécifier uniquement les fonctions d'agrégation sans effectuer `group operation` sur des champs spécifiques.
	`eventType | group [field]`
	`eventType | group [field1, field2, field3, ...]`
	`eventType | group with [max (field1), min(field2), avg (field3)]`
	`eventType | group [field1, field2, field3, ...] with [max (field1), min(field2), avg (field3)]`
	`eventType | group [field1, field2, field3, ...] with [max (field1) as max_field, min (field2), avg(field3) as avg_ field]`

Agrégation Agrège les résultats de la requête pour effectuer une opération.	`min(field)` `max(field)`

© Acronis International GmbH, 2003-2026

Opération	Exemple

Ces fonctions ne peuvent être utilisées que dans le cadre d'une `group operation` (voir ci-dessus).	`avg(field)`
	`count()`
	`count(field)`
	`countdistinct(field)`

Remarque
Habituellement, dans les langages de programmation, '==' est utilisé pour déclarer des conditions, et '=' pour affecter des valeurs.

Avec Acronis XDR Query Language, vous pouvez uniquement déclarer des conditions et utiliser '=' et '==' de manière interchangeable.

Exemples de requêtes

Cette section comprend un certain nombre d'exemples de requêtes qui illustrent la manière dont vous pouvez appliquer les règles syntaxiques XQL à votre requête.

- Sélection de champs dans le type d'événement `WinProcCreate` :

```
WinProcCreate | columns host_name, parent_start, parent_gpid, parent_pid, parent_
user, proc_name
```

- Filtrage avec conditions, avant le regroupement des résultats par `proc_name` et l'application des fonctions d'agrégation `min()` sur `parent_pid` :

```
WinProcCreate | where host_name == 'BNi-Kub' AND parent_pid != -1 AND proc_name
CONTAINS '1' AND host_name IN ('Computer1') | group [proc_name] with [min(parent_
pid)]
```

- Sélection de données à l'aide de filtres, puis décompte du nombre de lignes renvoyées et classement :

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [count() as new_count] |
order new_count
```


© Acronis International GmbH, 2003-2026

- Sélection de données avec filtres regex :

```
WinProcCreate | where host_name matches 'BNi.*'
```

- Sélection de données à l'aide de filtres complexes et limitation des résultats :

```
WinProcCreate | where (host_name contains 'BNi-Kub') OR (host_name in
('Computer1', 'Computer2')) | limit 10
```

- Sélection de données à l'aide de filtres, puis décompte du nombre de lignes distinctes renvoyées :

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [countdistinct(*)]
```

- Sélection de données à l'aide de filtres, classement des données par champ et limitation du nombre de lignes renvoyées :

```
WinProcCreate | where host_name == 'BNi-Kub' | order host_name | limit 10
```

Types d'événements et champs

Cette section comprend :

- Types d'événements
- Exemples de types de données
- Champs d'événements

Types d'événements

Nom	Description	Type
WinProcCreate Pour plus d'informations sur les champs disponibles, voir WinProcCreate.	Événements de création de processus Windows	Événements
WinProcTerminate Pour plus d'informations sur les champs disponibles, voir WinProcTerminate.	Événements de fin de processus Windows	Événements

© Acronis International GmbH, 2003-2026

Nom	Description	Type
WinNetAccess Pour plus d'informations sur les champs disponibles, voir WinNetAccess.	Événements d'accès au réseau Windows	Événements
WinRegAccess Pour plus d'informations sur les champs disponibles, voir WinRegAccess.	Événements d'accès au registre Windows	Événements
WinScriptExec Pour plus d'informations sur les champs disponibles, voir WinScriptExec.	Événements liés à l'exécution de scripts Windows (y compris PowerShell, VBS, etc.)	Événements
WinFileAccess Pour plus d'informations sur les champs disponibles, voir WinFileAccess.	Événements d'accès aux fichiers Windows (lecture/écriture)	Événements
WinLogin Pour plus d'informations sur les champs disponibles, voir WinLogin.	Événements de connexion des utilisateurs de Windows	Événements
WinLogout Pour plus d'informations sur les champs disponibles, voir WinLogout.	Événements de déconnexion des utilisateurs de Windows	Événements
WinAgentDetection Pour plus d'informations sur les champs disponibles, voir WinAgentDetection.	Événements de détection de Windows	Détections

Exemples de types de données

Type de données	Exemple	Description

Chaîne	`WinProcCreate | where host_name == 'BNi-Kub'`
	
	`WinProcCreate | where host_name == "BNi-Kub"`
		Des guillemets simples ou doubles doivent être ajoutés de part et d'autre des chaînes de caractères.

UUID	`WinProcCreate | where agent_id == '61f0c404-5cb3-11e7-907b-a6006ad3dba0'`
	
	`WinProcCreate | where agent_id == "61f0c404-5cb3-11e7-907b-`
		Les UUID étant des chaînes de caractères, des guillemets simples ou doubles doivent être placés de part et d'autre.
		
		Les valeurs UUID doivent être dans une séquence 8-4-4-4-12.

© Acronis International GmbH, 2003-2026

Type de données	Exemple	Description
	`a6006ad3dba0"`	
DateTime	`WinProcCreate | where event_time < '2022-11-01'` `WinProcCreate | where event_time < "2022-11-01"`	La valeur DateTime étant une chaîne de caractères, des guillemets simples ou doubles doivent être placés de part et d'autre. La valeur DateTime doit être au format AAAA-MM-JJ.

Valeur booléenne	`WinLogin | where is_admin == 1`
	`WinLogin | where is_admin == 0`
	`WinLogin | where is_admin == true`
	`WinLogin | where is_admin == false`
		Les valeurs booléennes peuvent être représentées par `1`, `0`, `true` ou `false`.

Entier	`WinLogin | where proc_pid > 25`	Valeur entière.

Champs d'événements

Type d'événement	Champ (type de données)
WinProcCreate	• `agent_id (UUID)` • `customer (String)` • `event_time (DateTime)` • `host_name (String)` • `id (UUID)` • `owner (String)` • `parent_args (String)` • `parent_gpid (UUID)` • `parent_integrity_level (String)` • `parent_md5 (String)` • `parent_name (String)` • `parent_oname (String)` • `parent_path (String)` • `parent_pid (Int)` • `parent_sha1 (String)` • `parent_sha256 (String)` • `parent_start (DateTime)` • `parent_upn (String)` • `parent_user (String)` • `parent_user_domain (String)` • `proc_args (String)`

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_prod (String) • proc_prod_desc (String) • proc_sha1 (String) • proc_sha256 (String) • proc_signatures (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinProcTerminate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • term_args (String)

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• term_gpid (UUID) • term_integrity_level (String) • term_md5 (String) • term_name (String) • term_oname (String) • term_path (String) • term_pid (Int) • term_sha1 (String) • term_sha256 (String) • term_start (DateTime) • term_upn (String) • term_user (String) • term_user_domain (String) • timestamp (DateTime)
WinNetAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • net_dst_ip (String) • net_dst_port (Int) • net_host (String) • net_http_method (String) • net_http_url (String) • net_protocol (String) • net_src_ip (String) • net_src_port (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String)

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinRegAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID)

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • reg_key (String) • reg_operation (String) • reg_original_key (String) • reg_original_value_data (String) • reg_value_data (String) • reg_value_name (String) • reg_value_type (String) • resource_id (UUID) • timestamp (DateTime)
WinScriptExec	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String)

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • script_data (String) • script_fragment (Bool) • script_size (Int) • script_type (String) • timestamp (DateTime)
WinFileAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_op (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String)

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinLogin	• agent_id (UUID) • customer (String) • domain (String) • event_time (DateTime) • host_name (String) • id (UUID) • is_admin (Bool) • login_time (DateTime) • name (String) • owner (String) • resource_id (UUID) • security_id (String) • timestamp (DateTime) • type (String)
WinLogout	• agent_id (UUID) • customer (String) • event_time (DateTime)

© Acronis International GmbH, 2003-2026

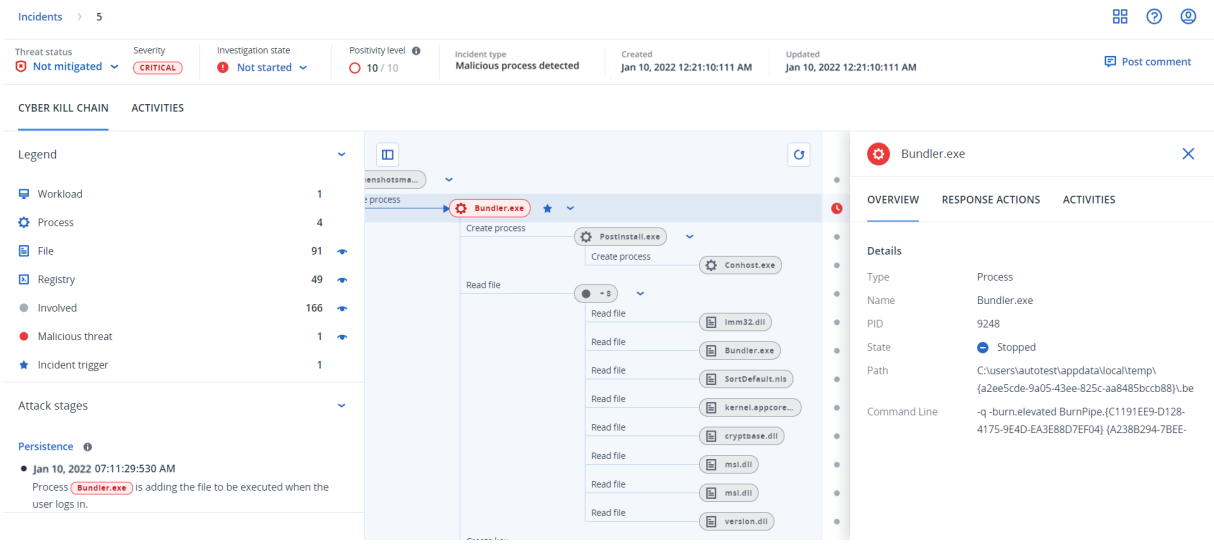
Type d'événement	Champ (type de données)
	• host_name (String) • id (UUID) • logout_time (DateTime) • resource_id (UUID) • security_id (String) • timestamp (DateTime)
WinAgentDetection	• agent_id (UUID) • customer (String) • detection_type (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • mitre_stid (Int) • mitre_tactics (Int) • mitre_tid (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String)

© Acronis International GmbH, 2003-2026

Type d'événement	Champ (type de données)
	• proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • severity (String) • threat_name (String) • timestamp (DateTime) • url (String) • url_blocked (Bool) • url_cat (Array(String)) • url_list (String) • url_md5 (String)

Enquête sur les incidents

La fonctionnalité EDR (Endpoint Detection and Response) vous permet d'enquêter sur l'intégralité d'un incident, y compris toutes les phases et les objets de l'attaque (processus, valeurs de registre, tâches planifiées et domaines) impactés par une attaque. Ces objets sont représentés dans la cyber kill chain par des nœuds faciles à comprendre, comme indiqué ci-dessous. Utilisez la cyber kill chain pour comprendre rapidement ce qui s'est passé exactement, et le moment où l'incident s'est produit.



© Acronis International GmbH, 2003-2026

Chaque étape d'une attaque est visible dans la cyber kill chain et vous fournit une interprétation détaillée des circonstances de l'incident. La cyber kill chain utilise des phrases et des graphiques faciles à comprendre, qui expliquent chaque étape de l'attaque. La durée d'investigation est, par conséquent, réduite.

Vous pouvez rapidement comprendre la portée et l'impact d'un incident grâce à l'évolution de l'attaque mappée à la structure MITRE. De cette manière, vous pouvez analyser les événements qui sont survenus à chaque étape d'une attaque :

- Point d'entrée initial
- Mode d'exécution de l'attaque
- Toute élévation des privilèges
- Techniques d'évitement des détections
- Déplacements latéraux vers d'autres ressources
- Usurpation des informations d'identification
- Tentatives d'exfiltration

Vous pouvez également cliquer sur **Copilot** pour lancer Copilot, l'outil de chat qui vous permet de saisir plusieurs demandes et de recevoir des mesures d'intervention suggérées pour l'incident sélectionné. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287).

Remarque
Chaque objet impacté par l'attaque, qu'il s'agisse d'un processus, du registre, d'une tâche planifiée ou d'un domaine, est représenté par un nœud dans la cyber kill chain.

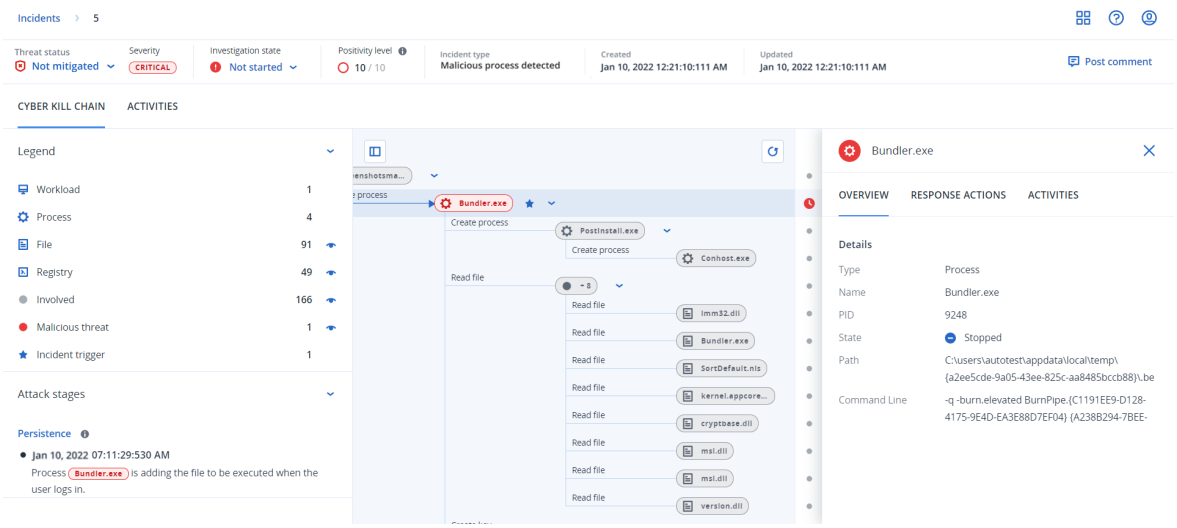
Comment enquêter sur des incidents dans la cyber kill chain

Vous pouvez enquêter à chaque étape d'une attaque dans la cyber kill chain. Suivez les phrases et les graphiques de la cyber kill chain ; ils sont faciles à interpréter et permettent de comprendre chaque étape de l'attaque, ce qui vous permet de réduire la durée de l'enquête.

Pour commencer une enquête dans la cyber kill chain

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents affichée, cliquez sur  dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.

© Acronis International GmbH, 2003-2026



3. Affichez une synthèse de l'incident dans la barre d'état de la menace, en haut de la page. La barre d'état de la menace comprend les informations suivantes :
   - Statut actuel de la menace : Le statut de la menace est défini automatiquement par le système. Tout incident ayant le statut **Non atténué** doit faire l'objet d'une enquête dans les plus brefs délais.

     Important
     Un incident est défini comme étant **Atténué** lorsqu'une sauvegarde est restaurée avec succès ou que toutes les détections ont été traitées avec succès par un processus d'arrêt, une mise en quarantaine ou une restauration.

     Un incident est défini comme étant **Non atténué** lorsqu'une restauration de sauvegarde n'a pas abouti ou qu'une détection au moins n'a pas été traitée par un processus d'arrêt, une mise en quarantaine ou une restauration.

     Vous pouvez également définir manuellement le statut de la menace sur **Atténué** ou sur **Non atténué**. Lorsque vous sélectionnez l'un de ces statuts, vous êtes invité à saisir un commentaire. Ce commentaire est enregistré dans le cadre des activités d'investigation et est visible dans l'onglet **Activités**. Notez que la fonctionnalité EDR peut toujours rétablir le statut de la menace sur **Atténué** ou **Non atténué** si l'incident a été de nouveau détecté ou si des mesures d'intervention ont été exécutées avec succès.

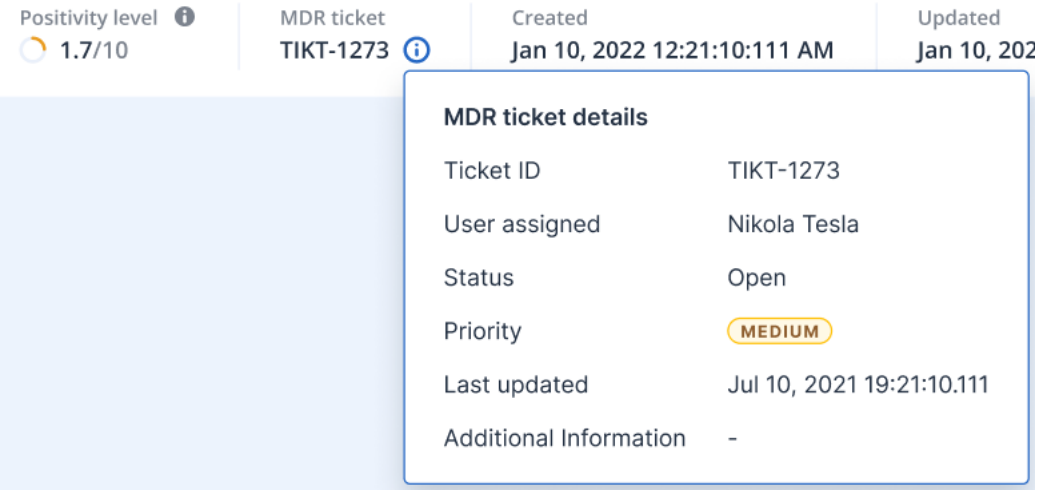
   - Gravité des incidents : **Critique**, **Élevée** ou **Moyenne**. Pour plus d'informations, voir "Examen des incidents" (p. 1259).
   - État actuel de l'enquête : L'un des états **Enquête en cours**, **Non démarré** (état par défaut), **Faux positif** ou **Fermé**. Lorsque vous démarrez une enquête sur un incident, vous devez changer le statut de cet incident afin que les autres collègues soient informés de toutes les modifications qui lui sont apportées.

© Acronis International GmbH, 2003-2026

- Niveau de positivité : Indique le degré de probabilité, noté entre 1 et 10, qu'un incident soit une véritable attaque malveillante. Pour plus d'informations, voir "Examen des incidents" (p. 1259).
- Type d'incident : un ou plusieurs des éléments suivants : **Ransomware détecté**, **Malware détecté**, **Processus suspect détecté**, **Processus malveillant détecté**, **Détection Microsoft Defender**, **URL suspecte bloquée**, et **URL malveillante bloquée**.

Remarque
Si l'Antivirus Microsoft Defender est activé pour la protection en temps réel au lieu de Acronis Protection en temps réel, seuls les types d'incidents **Détection Microsoft Defender**, **URL suspecte bloquée** et **URL malveillante bloquée** sont affichés.

- Si les services gérés de détection et de neutralisation des menaces (MDR) sont activés sur la ressource, un champ **Ticket MDR** s'affiche. Vous pouvez consulter les détails du ticket MDR créé pour l'incident et l'analyste de sécurité MDR affecté à l'incident.



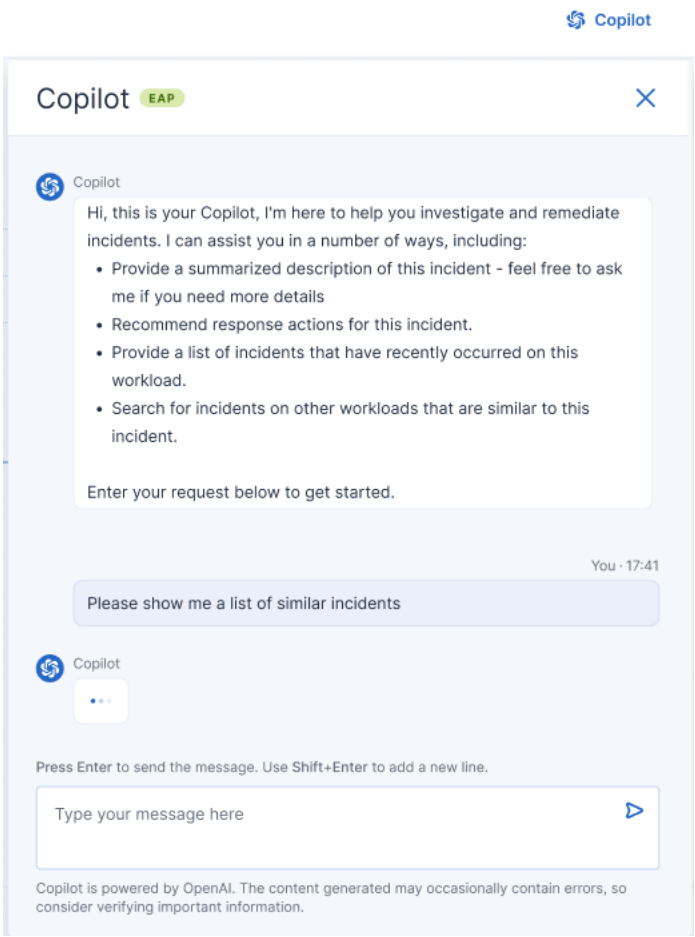
- Date de création et de mise à jour de l'incident : Date et heure de détection de l'incident ou de sa dernière mise à jour avec de nouvelles détections enregistrées dans l'incident.



4. Cliquez sur l'onglet **Légende** afin d'afficher les différents nœuds qui composent le graphique de la kill chain, puis définissez les nœuds à afficher. Pour plus d'informations, voir "Compréhension et personnalisation de la vue de la cyber kill chain" (p. 1290).
5. Enquêtez et corrigez l'incident en effectuant les opérations suivantes. Notez qu'il s'agit du workflow type d'enquête et de correction d'un incident, mais qu'il peut varier en fonction de chaque incident et de vos propres exigences.
   a. Examinez chaque phase de l'attaque dans l'onglet **Phases de l'attaque**. Pour plus d'informations, voir "Examiner les phases d'attaque d'un incident" (p. 1292).
   b. Cliquez sur **Corriger l'incident complet** pour appliquer les actions de correction. Pour plus d'informations, voir "Atténuer l'intégralité d'un incident" (p. 1305). Vous pouvez également corriger des nœuds dans la chaîne de cyberattaques, comme décrit dans "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 1310).

© Acronis International GmbH, 2003-2026

Sinon, cliquez sur **Copilot** pour lancer Copilot, l'outil de chat assisté par l'IA. Copilot fournit des options de réponse, en fonction de l'incident, et des informations contextuelles pertinentes pour l'incident telles que des détails sur le type d'attaque. Vous pouvez sélectionner l'option de réponse pertinente, puis suivre les instructions à l'écran. Ces options de réponse sont décrites dans "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 1310).



Important
Il existe une limite mensuelle de 1 000 demandes par tenant partenaire lors de l'utilisation de Copilot. Lorsque cette limite est atteinte, un message d'erreur s'affiche, vous informant que vous avez dépassé la limite mensuelle.

c. Examinez les actions entreprises pour limiter l'incident dans l'onglet **Activités**. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Compréhension et personnalisation de la vue de la cyber kill chain

Pour comprendre quels sont les nœuds impactés dans la cyber kill chain, accédez à la légende. La légende affiche tous les nœuds concernés par un incident, ce qui vous permet de comprendre comment ces différents nœuds ont été impactés par l'attaque de l'entité malveillante. Vous pouvez également définir les nœuds que vous souhaitez masquer ou afficher dans la cyber kill chain.

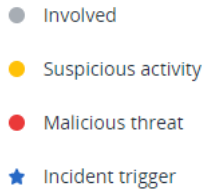
© Acronis International GmbH, 2003-2026

Pour accéder à la légende

1. Cliquez sur l'icône représentant une flèche à droite de la section Légende.
   La section Légende se développe, comme indiqué ci-dessous.



2. La légende utilise quatre couleurs principales qui vous permettent de comprendre rapidement les événements survenus dans chaque nœud de la cyber kill chain, comme indiqué ci-dessous. Ces nœuds à code couleur sont également inclus dans les phases de l'attaque, comme indiqué dans "Examiner les phases d'attaque d'un incident" (p. 1292).



Pour masquer ou afficher des nœuds dans la cyber kill chain

1. Dans la section Légende développée, vérifiez que s'affiche en regard des nœuds que vous souhaitez afficher dans la cyber kill chain. Si l'icône affichée est , cliquez dessus pour qu'elle devienne .
2. Pour masquer un nœud de la cyber kill chain, cliquez sur . L'icône change et devient , et le nœud n'est plus affiché dans la cyber kill chain.

© Acronis International GmbH, 2003-2026

Examiner les phases d'attaque d'un incident

Les phases d'attaque d'un incident permettent de comprendre les interprétations de chaque incident.

Chaque phase d'attaque récapitule les événements qui se sont produits, ainsi que les objets (appelés *nœuds* de la cyber kill chain) qui étaient ciblés. Par exemple, si le nom d'un fichier téléchargé a été modifié (masquerading), la phase de l'attaque l'indique et comprend des liens vers le nœud pertinent de la cyber kill chain que vous pouvez examiner, et vers la technique MITRE ATT&CK pertinente.

Chaque phase de l'attaque fournit les informations dont vous avez besoin pour répondre à ces questions essentielles :

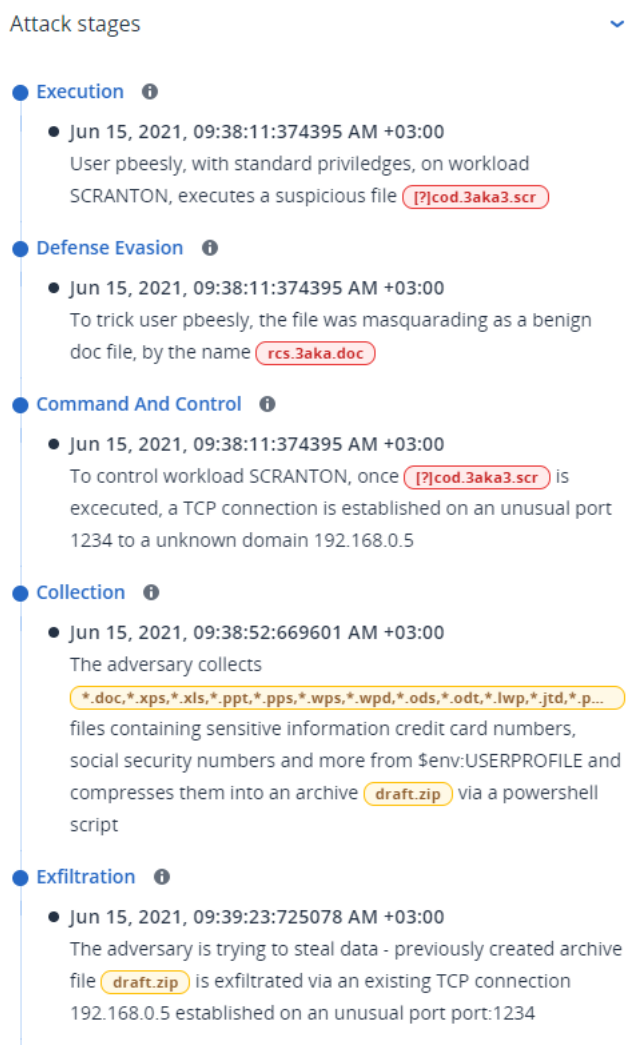
- Quel était l'objectif de l'entité malveillante ?
- Dans quelle mesure l'entité malveillante a atteint cet objectif ?
- Quels nœuds étaient ciblés ?

Mais avant tout, l'interprétation permet de réduire considérablement le temps nécessaire à l'enquête sur l'incident, car vous n'avez plus à parcourir chaque événement de sécurité sur une chronologie ou un nœud graphique afin de tenter de créer une interprétation de l'attaque.

Les phases de l'attaque comprennent des informations sur les fichiers compromis contenant des informations sensibles telles que des informations de santé protégées (PHI), des numéros de carte de crédit et des numéros de sécurité sociale, comme indiqué dans la phase **Collecte** dans l'exemple ci-dessous.

Pour plus d'informations, voir "Quelles sont les informations incluses dans une phase d'attaque ?" (p. 1293).

© Acronis International GmbH, 2003-2026



Comment parcourir les phases d'une attaque

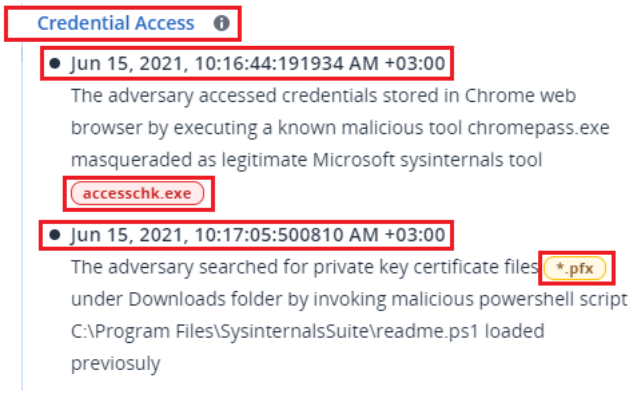
Les phases d'une attaque sont répertoriées dans l'ordre chronologique. Faites défiler la liste complète des phases d'attaque de l'incident.

Pour examiner plus en détail une phase d'attaque spécifique, cliquez n'importe où dans la phase d'attaque pour accéder au nœud pertinent dans le graphique de la cyber kill chain. Pour plus d'informations sur la navigation dans le graphique de la cyber kill chain et des nœuds spécifiques, reportez-vous à "Examiner des nœuds de la cyber kill chain" (p. 1295).

Quelles sont les informations incluses dans une phase d'attaque ?

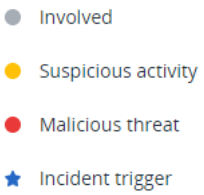
Chaque phase d'attaque fournit une interprétation facile à comprendre de l'attaque, dans une langue facile à comprendre. Cette interprétation est composée d'un certain nombre d'éléments, comme indiqué ci-dessous et dans le tableau suivant.

© Acronis International GmbH, 2003-2026



Élément de phase d'attaque	Description
En-tête	Décrit l'opération que l'entité malveillante a essayé d'effectuer, ainsi que son objectif (dans l'exemple ci-dessus, **Accès par identifiants**), avec un lien vers une technique MITRE ATT&CK connue. Cliquez sur le lien pour plus d'informations sur le site Web MITRE ATT&CK. **Remarque** Si une phase d'attaque n'est pas une technique MITRE ATT&CK connue, le texte d'en-tête n'est pas lié. Ce système est pertinent pour les techniques génériques telles que des fichiers détectés dans un dossier aléatoire.
Horodatage	Heure à laquelle la phase d'attaque s'est produite.
Technique	Mode employé par l'entité malveillante pour atteindre son objectif et objets (entrées de registre, fichiers ou tâches planifiées) concernés. La description de la technique d'attaque inclut des liens à code couleur vers chaque nœud affecté de la cyber kill chain, comme indiqué dans l'exemple ci-dessus. Ces liens à code couleur vous permettent d'accéder rapidement au nœud affecté et d'enquête sur les événements exacts qui sont survenus. Les couleurs utilisées dans une phase d'attaque indiquent les éléments suivants :

© Acronis International GmbH, 2003-2026

Élément de phase d'attaque	Description
	 En observant la légende ci-dessus, nous voyons que la phase d'attaque exemple Accès par identifiants comporte un lien vers un nœud de malware accesschk.exe et un nœud de fichier suspect *.pfx (cliquez sur les liens pour accéder au nœud correspondant dans la cyber kill chain). Pour plus d'informations sur la navigation dans ces nœuds et sur les actions disponibles, voir "Examiner des nœuds de la cyber kill chain" (p. 1295). Notez que les phases de l'attaque comprennent également des liens vers des nœuds de fichier comportant des informations sur les fichiers compromis contenant des informations sensibles : informations de santé protégées (PHI), numéros de carte de crédit et numéros de sécurité sociale.

Remarque
Chaque phase d'attaque est un événement de détection unique. Le contenu répertorié à chaque étape (en-tête, horodatage, technique) est généré en fonction de paramètres spécifiques dans l'événement de détection, qui sont basés sur les modèles de phase d'attaque stockés par EDR (Endpoint Detection and Response).

Examiner des nœuds de la cyber kill chain

Outre l'examen des phases d'attaque, vous pouvez également parcourir chacun des nœuds de l'attaque dans la cyber kill chain. De cette manière, vous pouvez accéder à des nœuds spécifiques de la cyber kill chain, et d'examiner et atténuer chaque nœud en fonction des besoins.

Par exemple, vous pouvez déterminer la probabilité avec laquelle un incident est une véritable attaque malveillante. En fonction de votre enquête, vous pouvez également appliquer un certain nombre de mesures d'intervention au nœud, y compris isoler une ressource ou mettre un fichier suspect en quarantaine.

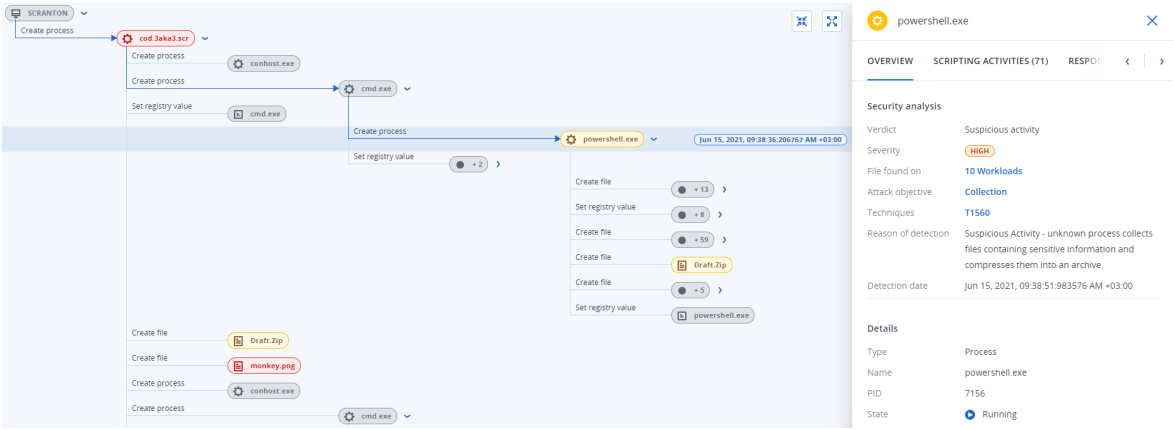
Pour examiner des nœuds de la cyber kill chain

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents affichée, cliquez sur dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.
3. Accédez au nœud pertinent, puis cliquez dessus pour afficher l'encadré correspondant.

   Remarque
   Cliquez sur le nœud pour le développer et afficher les nœuds associés.

   Par exemple, le fait de cliquer sur le nœud **powershell.exe** dans l'exemple ci-dessous ouvre l'encadré correspondant. Vous pouvez également cliquez sur l'icône en forme de flèche en regard du nœud pour afficher les nœuds associés, y compris les fichiers et les valeurs de registre, qui peuvent être affectés par le nœud **powershell.exe**. Vous pouvez ensuite cliquer sur ces nœuds associés afin d'approfondir votre enquête.



4. Examiner les informations incluses dans les onglets de l'encadré :
   - **Vue d'ensemble** : Comprend deux sections principales qui fournissent un résumé relatif à la sécurité du nœud attaqué.
     - **Analyse de la sécurité** : Fournit une analyse du nœud attaqué, y compris le verdict de la fonctionnalité EDR concernant la menace (activité suspecte, par exemple), l'objectif de l'attaque d'après les techniques d'attaque MITRE (cliquez sur le lien pour accéder au site Web MITRE), le motif de la détection, ainsi que le nombre de ressources qui peuvent être affectées par l'attaque (cliquez sur le lien **n ressources** pour afficher les ressources affectées).

       Remarque
       Le lien **n ressources** indique qu'un objet malveillant ou suspect a été *trouvé* sur d'autres ressources. Cela ne signifie pas que l'attaque se produit sur ces autres ressources, mais qu'il existe un indicateur de compromission les concernant. L'attaque s'est peut-être déjà produite (et a créé un autre incident) ou l'entité malveillante se prépare à attaquer ces autres ressources à l'aide de sa « boîte à outils ».

© Acronis International GmbH, 2003-2026

  - **Détails** : Comprend des détails sur le nœud (son type, son nom et son état actuel), le chemin d'accès au nœud, ainsi que tous les hachages de fichier et les signatures numériques (numéros de série MD5 et de certificat).
- **Activités de script** : Comprend des détails sur les scripts appelés ou chargés dans l'attaque. Cliquez sur pour copier le script dans le Presse-papiers afin d'approfondir l'examen.

  Remarque
  L'onglet **Activités de script** n'est affiché que pour les nœuds de processus qui exécutent des commandes ou des scripts (par exemple, les commandes cmd ou PowerShell).

- **Mesures d'intervention** : Comprend un certain nombre de sections qui fournissent des actions supplémentaires d'examen, d'atténuation et de prévention, selon le type de nœud. Par exemple, pour les nœuds de ressource, vous pouvez définir un certain nombre de réponses qui comprennent une sauvegarde de données d'investigation et une restauration à partir de la sauvegarde. En ce qui concerne les nœuds malveillants ou suspects, vous pouvez les arrêter ou les mettre en quarantaine, annuler les modifications apportées par l'attaque, et les ajouter à la liste d'autorisation ou à la liste de blocage d'un plan de protection.
  Pour plus d'informations sur l'application de mesures d'intervention à des nœuds spécifiques, reportez-vous à "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 1310).
- **Activités** : Affiche les actions appliquées à l'incident dans l'ordre chronologique. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Comprendre les actions entreprises pour réduire un incident

Après avoir examiné un incident et enquêté sur le déroulement de l'attaque, vous appliquez généralement des mesures d'intervention. Une fois appliquées, ces mesures d'intervention sont visibles à différents endroits et vous permettent de mieux comprendre les actions entreprises pour réduire l'incident.

Remarque
Les incidents créés par les couches de prévention appliquent automatiquement les mesures configurées dans le plan de protection. Pour les points de détection, vous devez définir les mesures d'intervention pertinentes afin de limiter chaque scénario d'attaque.

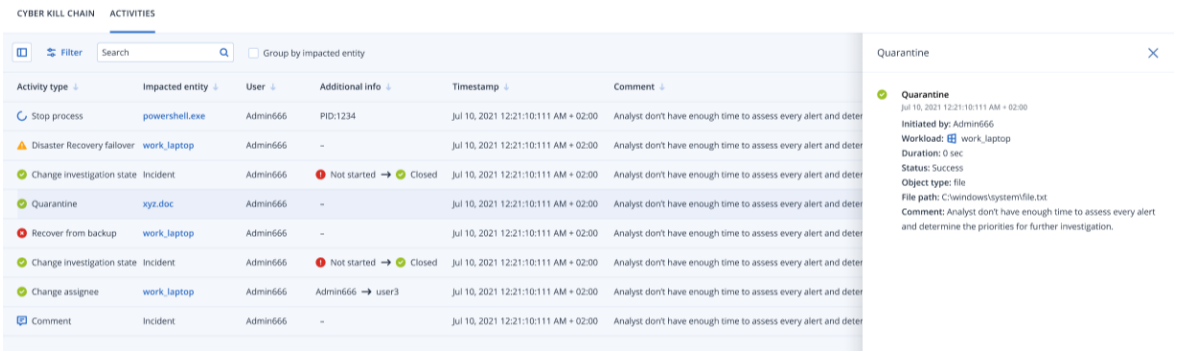
Pour comprendre les mesures d'intervention qui ont été prises, vous pouvez afficher toutes les mesures appliquées à l'intégralité d'un incident ou à un nœud spécifique dans la cyber kill chain de l'incident.

Pour afficher toutes les mesures d'intervention appliquées à un incident

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.

© Acronis International GmbH, 2003-2026

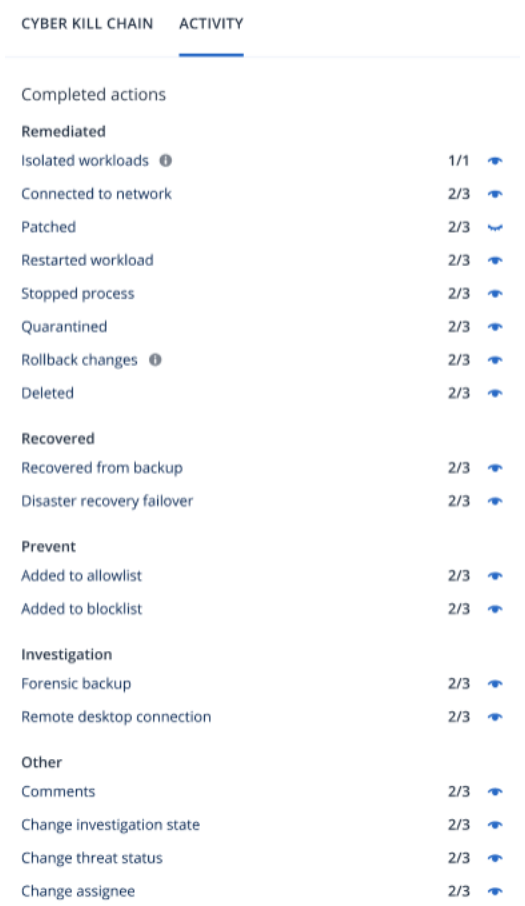
2. Dans la liste des incidents affichée, cliquez sur dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.
3. Cliquez sur l'onglet **Activités**.
   La liste des mesures d'intervention déjà appliquées à l'incident s'affiche.



Remarque
Si la mesure d'intervention a été initiée dans le cadre d'un workflow automatisé, le champ **Initié par** affiche **Workflow automatisé**. Pour plus d'informations, voir "Utilisation de workflows automatisés" (p. 1333).

4. Vous pouvez effectuer différentes opérations sur la liste affichée :
   - Cliquez sur une ligne de type d'activité pour afficher plus d'informations sur l'activité sélectionnée. Ces informations sont affichées dans un encadré, comme illustré à l'étape 3, et indiquent l'auteur et le statut de l'action, le chemin d'accès au fichier, ainsi que tout commentaire ajouté par l'auteur.
   - Pour rechercher une action spécifique, utilisez la case **Rechercher**.
   - Cliquez sur **Filtre** pour appliquer des filtres à la liste.
   - Cochez la case **Regrouper par entité impactée** afin de regrouper les actions pertinentes en fonction de l'entité.
   - Cliquez sur pour afficher/masquer la liste des actions entreprises.
     Vérifiez que s'affiche en regard des actions que vous souhaitez afficher. Si vous souhaitez masquer une action dans la liste, cliquez une nouvelle fois pour que l'icône change et devienne .

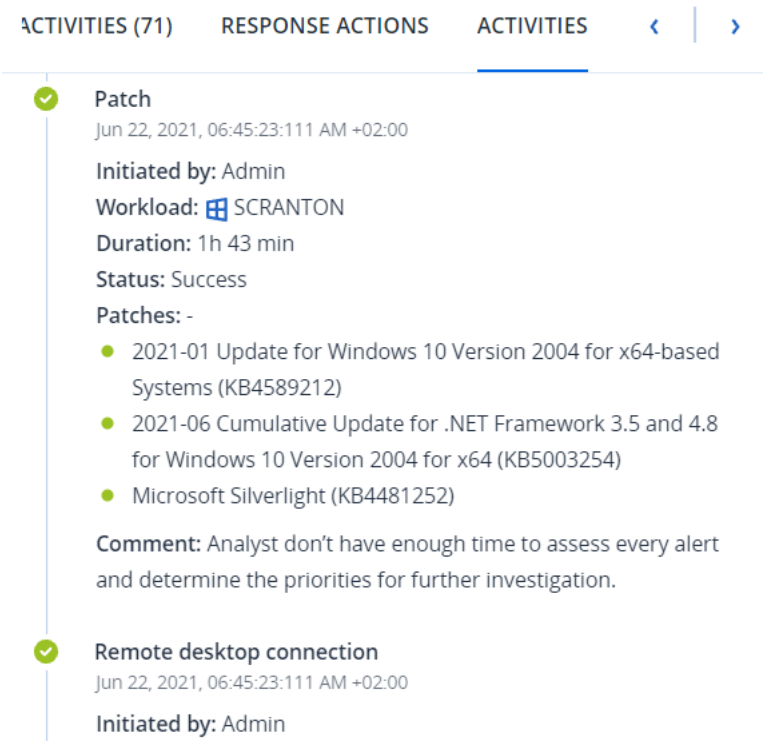
© Acronis International GmbH, 2003-2026



Pour afficher les mesures d'intervention appliquées à un nœud spécifique

© Acronis International GmbH, 2003-2026

1. Dans la cyber kill chain, cliquez sur un nœud pour afficher son encadré.
2. Cliquez sur l'onglet **Activités**.



3. Pour bien comprendre les mesures entreprises et les raisons de ce choix, vous devrez peut-être parcourir les mesures d'intervention appliquées au nœud. Par exemple, pour une connexion Bureau à distance, vous pouvez voir différentes informations : son auteur, son heure, sa durée et son statut global (si elle a abouti avec succès, a échoué ou a abouti avec des erreurs).

Remarque
Si la mesure d'intervention a été initiée dans le cadre d'un workflow automatisé, le champ **Initié par** affiche **Workflow automatisé**. Pour plus d'informations, voir "Utilisation de workflows automatisés" (p. 1333).

Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources

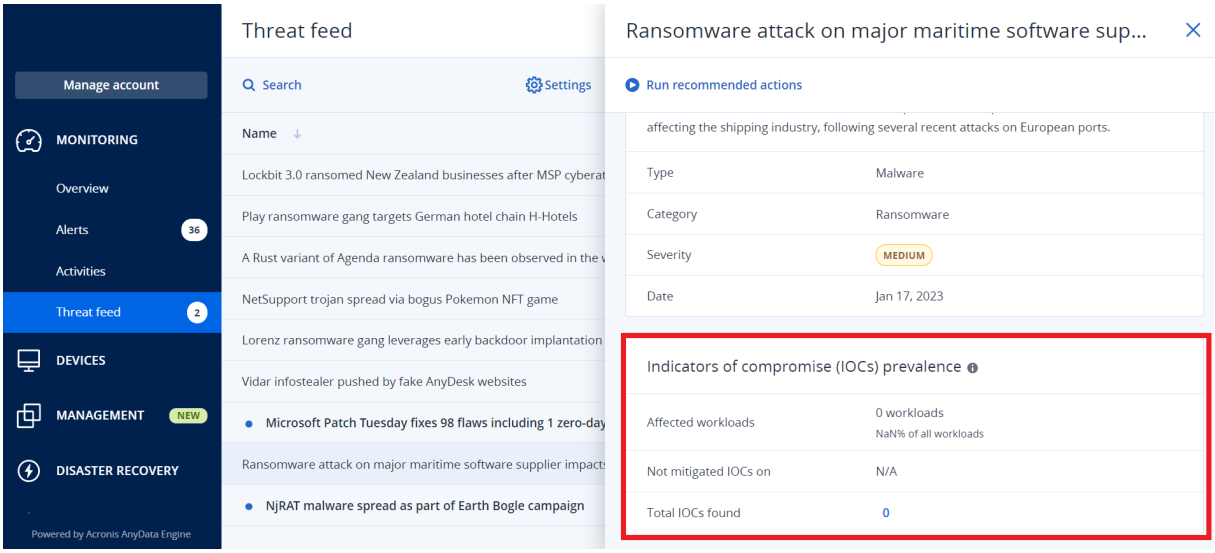
La fonctionnalité EDR (Endpoint Detection and Response) permet d'examiner les attaques connues et existant dans les flux d'informations sur les menaces visant vos ressources. Ces flux d'informations sur les menaces sont générés automatiquement en fonction des données de menaces reçues du Centre opérationnel de cyberprotection (CPOC). La fonctionnalité EDR vous permet de vérifier si une menace vise votre ressource, puis d'entreprendre les actions nécessaires pour la supprimer.

Vous pouvez accéder aux flux d'informations sur les menaces à partir du menu **Surveillance** dans la console Cyber Protect. Pour plus d'informations, voir "Flux de menaces" (p. 364).

© Acronis International GmbH, 2003-2026

Pour examiner une menace spécifique en détail et vérifier si elle impacte vos ressources, cliquez sur un flux d'informations sur les menaces. Vous y trouverez le nombre d'indicateurs de compromission détectés et de ressources affectées, et pourrez accéder aux ressources comportant des indicateurs de compromission non atténués.

Remarque
Si l'option EDR n'est pas activée dans le plan de protection, cette fonctionnalité supplémentaire de flux d'informations sur les menaces indiquée ci-dessous n'est pas affichée.



Définir les paramètres de flux d'informations sur les menaces

Vous pouvez définir un certain nombre de paramètres de flux d'informations sur les menaces afin de localiser et de limiter automatiquement les menaces connues.

Pour définir les paramètres de flux d'informations sur les menaces

1. Dans la console Cyber Protect, accédez à **Surveillance > Flux d'informations sur les menaces**.
2. Dans la page du flux d'informations sur les menaces qui s'affiche, cliquez sur **Paramètres**.

© Acronis International GmbH, 2003-2026

3. Dans la boîte de dialogue affichée, sélectionnez l'une des options suivantes :

Option	Description
Recherche d'indicateurs de compromission	Cliquez sur le commutateur pour activer la recherche automatique des indicateurs de compromission dans les ressources. Lorsque cette option est activée, les options **Action lors de la détection** et **Générer une alerte** sont également affichées.
Action lors de la détection	Dans la liste déroulante, sélectionnez l'action à entreprendre sur les fichiers concernés en cas de détection d'une menace sur une ressource : • **Aucune action** • **Quarantaine** • **Supprimer** • **Isoler les ressources**
Générer une alerte	Cochez la case pour générer une alerte si un indicateur de compromission est détecté dans une ressource. L'alerte s'affiche dans la page Alertes.

4. Cliquez sur **Appliquer**.

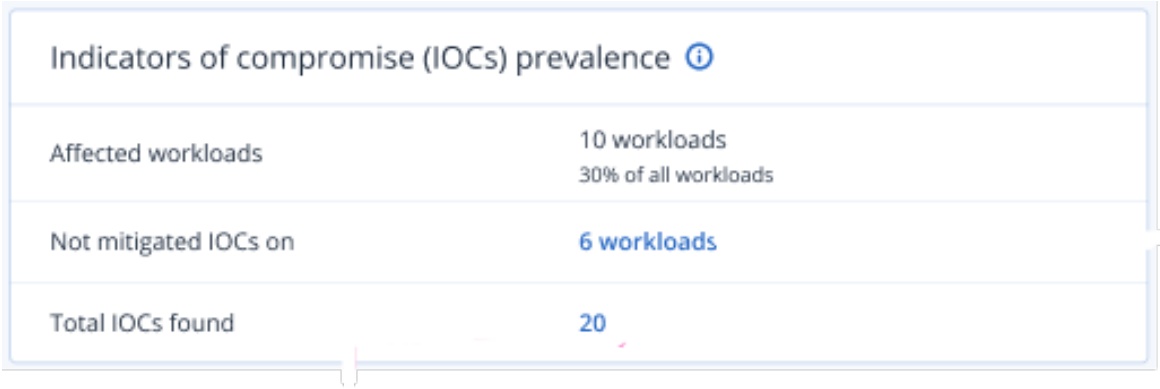
Examiner et atténuer les indicateurs de compromission sur les ressources affectées

Si la fonctionnalité EDR (Endpoint Detection and Response) est activée dans un plan de protection, vous pouvez visualiser toutes les menaces connues qui affectent des ressources dans le plan de protection. Vous pouvez également atténuer les autres indicateurs de compromission qui n'ont pas été atténués automatiquement. Pour plus d'informations sur l'atténuation automatique des indicateurs de compromission, reportez-vous à "Définir les paramètres de flux d'informations sur les menaces" (p. 1301).

Pour examiner et atténuer les ressources affectées

1. Dans la console Cyber Protect, accédez à **Surveillance > Flux d'informations sur les menaces**.
2. Cliquez sur une menace pour afficher ses détails.
3. Dans la section **Prévalence des indicateurs de compromission**, cliquez sur le lien ***n* ressources** pour afficher les ressources présentant des indicateurs de compromission non atténués.

© Acronis International GmbH, 2003-2026



4. Dans la page Ressources, cliquez sur la ressource pertinente et examinez ses détails. Vous pouvez exécuter une fonctionnalité spécifique sur la ressource, en définissant également d'autres adresses URL à filtrer (voir "Filtrage d'URL" (p. 1197)) et en bloquant les processus malveillants (reportez-vous à la section Exclusions dans "Paramètres de protection contre les virus et les malwares" (p. 1170)).
   Par exemple, si un flux d'informations sur les menaces indique qu'une ressource a été affectée par un indicateur de compromission, commencez par localiser et analyser cet indicateur en suivant les indications de "Examiner et analyser les indicateurs de compromission découverts" (p. 1303). Accédez ensuite au plan de protection de la ressource, puis définissez une protection supplémentaire telle que le blocage de hachages de fichiers ou de processus malveillants.

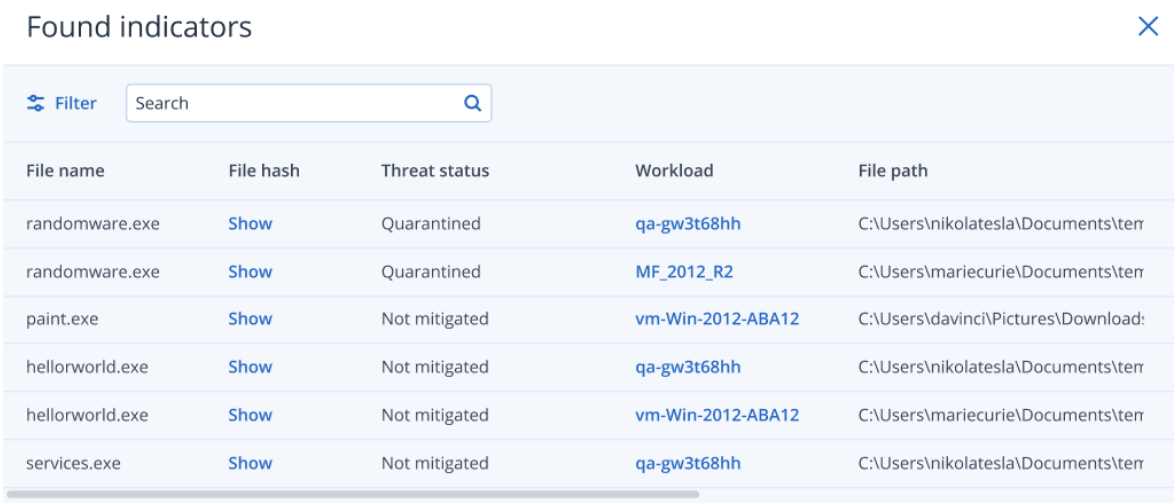
Examiner et analyser les indicateurs de compromission découverts

Outre l'examen des ressources affectées par des menaces connues, vous pouvez également examiner et analyser des indicateurs de compromission spécifiques. Vous pouvez ainsi visualiser les différentes ressources affectées par un indicateur de compromission et réduire cet indicateur.

Pour examiner et analyser des indicateurs de compromission

1. Dans la console Cyber Protect, accédez à **Surveillance > Flux d'informations sur les menaces**.
2. Cliquez sur une menace pour afficher ses détails.
3. Dans la section **Prévalence des indicateurs de compromission**, cliquez sur le lien **Nombre total d'indicateurs de compromission trouvés**.
   La page Indicateurs trouvés s'affiche.

© Acronis International GmbH, 2003-2026



4. (Facultatif) Utilisez l'option **Filtre** pour filtrer la liste des indicateurs de compromission en fonction de leur état. Vous pouvez également utiliser l'option **Recherche** pour rechercher des indicateurs de compromission spécifiques.
5. Pour afficher la ressource affectée par un indicateur de compromission, cliquez sur le lien figurant dans la colonne **Ressource**. Vous pouvez alors effectuer différentes opérations sur la ressource, notamment gérer les correctifs ou modifier un plan de protection.
6. (Facultatif) Dans la colonne **Hachage de fichier**, cliquez sur **Afficher** pour afficher les hachages de fichiers trouvés pour un indicateur de compromission spécifique. Dans la boîte de dialogue qui s'affiche, cliquez sur pour copier le hachage de fichier de l'indicateur de compromission dans un éditeur de texte.

Atténuation d'incidents

La fonctionnalité EDR (Endpoint Detection and Response) vous permet d'atténuer des incidents complets ou les différents points d'attaque d'un incident.

En atténuant l'intégralité d'un incident, vous pouvez choisir la ou les atténuations que vous souhaitez exécuter sur tout l'incident. Si vous devez gérer l'incident de manière plus granulaire, vous pouvez atténuer les différents points d'attaque en fonction de vos besoins. Par exemple, vous souhaiterez peut-être isoler le réseau d'une ressource afin d'arrêter le déplacement latéral ou les activités de commande et contrôle. De cette manière, même si la ressource est isolée, toutes les technologies Acronis Cyber Protect restent opérationnelles et une enquête peut être lancée.

La fonctionnalité EDR garantit une atténuation efficace par :

- Atténuation, afin de garantir que la menace est arrêtée.
- Restauration, afin de garantir que les services sont de nouveau en ligne immédiatement.
- Prévention, afin de garantir que les techniques utilisées dans une attaque ne seront plus détectées dans les futures attaques.

© Acronis International GmbH, 2003-2026

Atténuer l'intégralité d'un incident

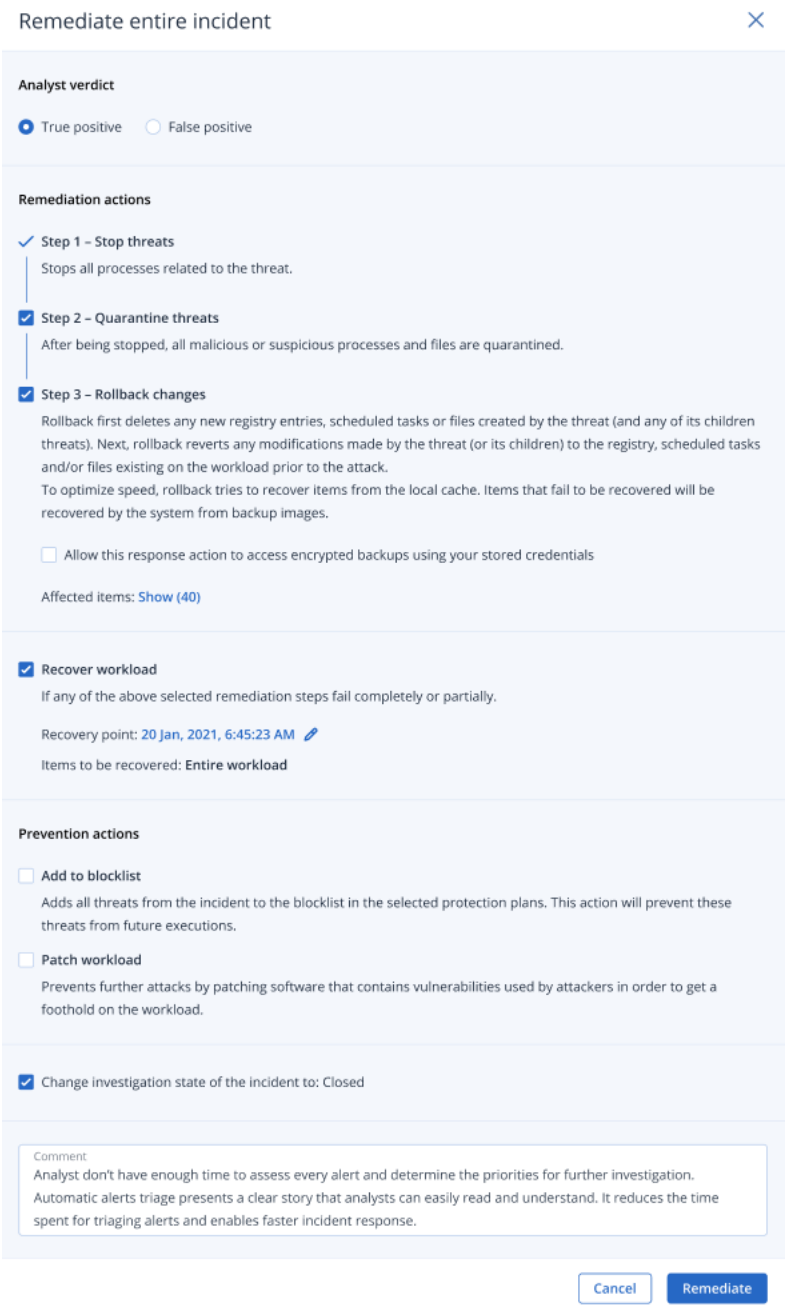
En atténuant l'intégralité d'un incident, vous pouvez choisir rapidement et facilement la ou les atténuations que vous souhaitez exécuter sur tout l'incident. La fonctionnalité EDR (Endpoint Detection and Response) vous accompagne dans tout le processus d'atténuation, étape par étape.

Si vous devez gérer votre réseau et l'incident de manière plus granulaire, reportez-vous à "Mesures d'intervention pour les différents nœuds de la cyber kill chain" (p. 1310).

Pour atténuer l'intégralité d'un incident

1. Dans la console Cyber Protect, accédez à **Protection > Incidents**.
2. Dans la liste des incidents affichée, cliquez sur  dans la colonne à l'extrême droite de l'incident sur lequel vous souhaitez enquêter. La cyber kill chain de l'incident sélectionné est affichée.
3. Cliquez sur **Atténuer tout l'incident**. La boîte de dialogue Atténuer tout l'incident s'affiche.

© Acronis International GmbH, 2003-2026



4. Dans la section **Verdict des analystes**, selon votre enquête sur l'incident, sélectionnez l'une des options suivantes :
   - **Vrai positif** : Sélectionnez cette option si vous avez la certitude que l'attaque est légitime. Une fois l'option sélectionnée, vous ajoutez les mesures d'atténuation et de prévention, comme le décrivent les étapes suivantes.
   - **Faux positif** : Sélectionnez cette option si vous avez la certitude que l'attaque n'est pas légitime. Dans ce mode, vous pouvez définir comment empêcher que ce classement se reproduise, par exemple en ajoutant l'incident à la liste d'autorisation d'un plan de protection.

© Acronis International GmbH, 2003-2026

Remarque
Après avoir sélectionné **Faux positif**, vous ne pouvez définir que des actions de prévention. Pour plus d'informations, voir "Atténuer un incident faux positif" (p. 1309).

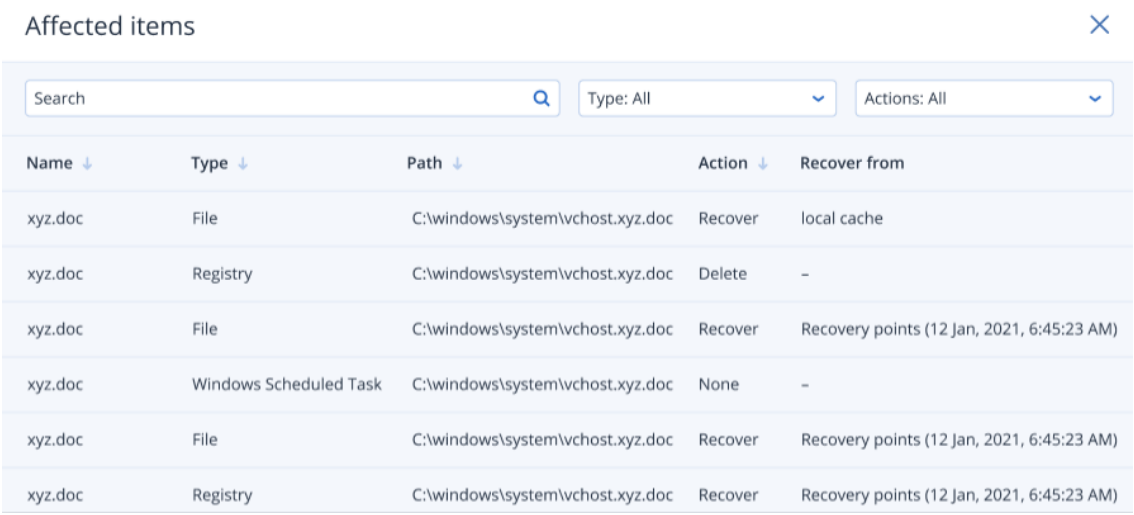
5. Dans la section **Actions de réparation**, effectuez les opérations de réparation suivantes. Notez qu'elles doivent être effectuées de manière séquentielle. Par exemple, vous ne pouvez pas sélectionner l'étape 2 avant la fin de l'étape 1.
   a. **Étape 1 - Arrêter les menaces** : Cochez la case pour stopper tous les processus associés à la menace.
   b. **Étape 2 - Mettre les menaces en quarantaine** : Une fois que la menace est stoppée, cochez la case pour mettre en quarantaine tous les processus et fichiers malveillants et suspects.
   c. **Étape 3 - Annuler les modifications** : Une fois les menaces mises en quarantaine, cochez la case pour supprimer tout nouveau fichier, entrée de registre ou tâche planifiée créé par la menace (et toute menace enfant). Le processus d'annulation annule alors toute modification apportée par la menace (ou ses enfants) au registre, aux tâches planifiées et/ou aux fichiers existants sur la ressource avant l'attaque. Pour une rapidité optimale, le processus d'annulation tente de restaurer les éléments depuis le cache local. Les éléments non restaurés le seront par le système à partir d'images de sauvegarde.

Remarque
Le processus de restauration ne concerne que les éléments stockés dans le cache local. La restauration à partir d'archives de sauvegarde sera disponible dans les prochaines versions.

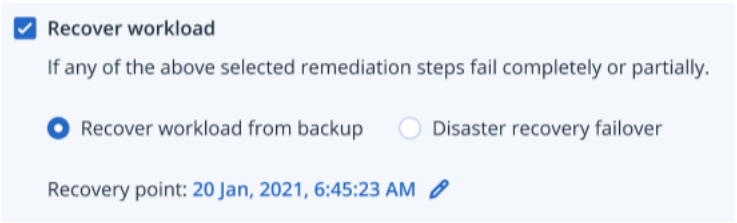
Cochez la case **Autoriser cette mesure d'intervention à accéder aux sauvegardes chiffrées à l'aide des identifiants stockés** si l'accès aux sauvegardes pertinentes est chiffré. La fonctionnalité EDR accède aux identifiants utilisateur stockés pour déchiffrer les archives chiffrées et rechercher les fichiers pertinents.

Vous pouvez également cliquer sur **Éléments affectés** pour afficher tous les éléments (fichiers, registre ou tâches planifiées) affectés par l'annulation, les actions appliquées (**Supprimer**, **Restaurer** ou **Aucune**) et indiquer si les éléments sont restaurés depuis le cache local ou les images de sauvegarde.

© Acronis International GmbH, 2003-2026



d. **Restaurer la ressource** : Cochez cette case pour restaurer une ressource si l'une des étapes de réparation ci-dessus échoue totalement ou partiellement.



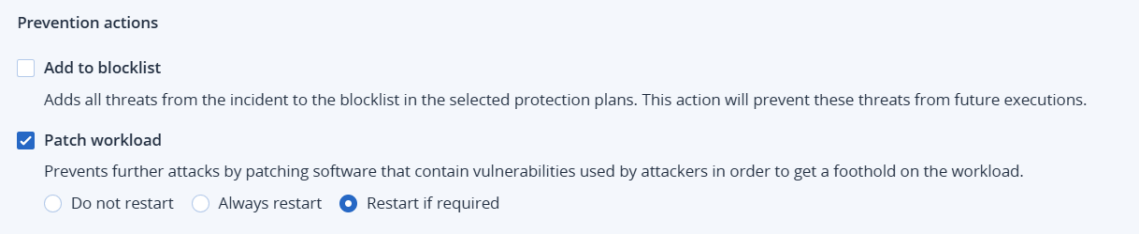
Sélectionnez l'une des options de restauration suivantes :

- **Restaurer la ressource depuis la sauvegarde** : Vous permet de restaurer une ressource à partir d'un point de restauration spécifique. Cliquez sur l'icône de modification du point de restauration pour sélectionner l'une des sauvegardes de restauration de la liste.
- **Basculement pour Disaster Recovery** : Vous permet d'exécuter une reprise d'activité après sinistre si cette fonctionnalité est activée dans votre plan de protection. Nous vous recommandons d'utiliser cette option pour les ressources critiques telles que les serveurs AD ou de bases de données. Pour plus d'informations, voir "Implémentation de la reprise d'activité après sinistre" (p. 1016).

6. Dans la section **Actions de prévention**, sélectionnez les étapes d'atténuation pertinentes :
   - **Ajouter à la liste de blocage** : cochez la case, puis sélectionnez les plans de protection concernés dans la liste affichée. Cette action de prévention garantit que toutes les détections de l'incident seront bloquées pour les plans de protection sélectionnés.
   - **Correction de ressource** : cochez la case pour corriger tout logiciel vulnérable et empêcher les attaquants d'accéder à la ressource. Vous pouvez ensuite sélectionner l'action à effectuer une fois la correction terminée (**Ne pas redémarrer**, **Toujours redémarrer** ou **Redémarrer**

© Acronis International GmbH, 2003-2026

si nécessaire), selon que l'utilisateur est connecté ou non.



7. Cochez la case **Modifier l'état de l'enquête sur l'incident en : Fermé**. Si cette option n'est pas sélectionnée, l'état antérieur de l'enquête est conservé.
8. Cliquez sur **Réparer**. Les actions d'atténuation que vous avez sélectionnées sont exécutées, étape par étape. La boîte de dialogue Atténuer tout l'incident indique la progression de chaque étape.
   Une fois que vous avez cliqué, le bouton indique **Aller à Activités**. Cliquez sur **Aller à Activités** pour examiner toutes les mesures d'intervention appliquées à l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Atténuer un incident faux positif

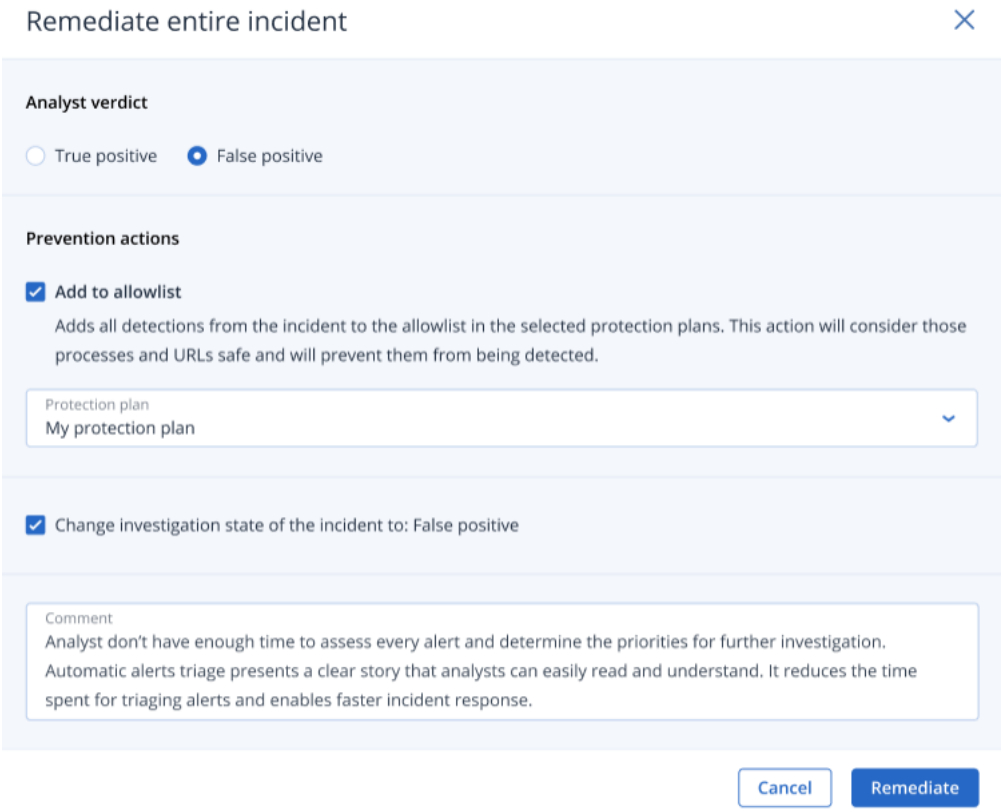
Si vous avez la certitude qu'une attaque n'est pas une attaque authentique, en d'autres termes, si vous savez qu'il s'agit d'un faux positif, vous pouvez définir comment empêcher l'incident de survenir une nouvelle fois. Par exemple, vous pouvez ajouter l'incident à la liste d'autorisation d'un plan de protection.

Pour atténuer un incident faux positif

1. Dans la cyber kill chain de l'incident sélectionné, cliquez sur **Atténuer tout l'incident**. La boîte de dialogue Atténuer tout l'incident s'affiche.

© Acronis International GmbH, 2003-2026

2. Dans la section **Verdict des analystes**, sélectionnez **Faux positif**.



3. Dans la section **Actions de prévention**, cochez la case **Ajouter à la liste d'autorisation**. Dans la liste des plans de protection, sélectionnez les plans de protection pertinents.
   Cette action préventive garantit que toutes les détections de l'incident ne seront plus détectées pour les plans de protection sélectionnés.
4. Cochez la case **Modifier l'état de l'enquête sur l'incident en : Faux positif**.
5. Cliquez sur **Réparer**.
   Une fois que vous avez cliqué, le bouton indique **Aller à Activités**. Cliquez sur **Aller à Activités** pour examiner les mesures d'intervention appliquées à l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Mesures d'intervention pour les différents nœuds de la cyber kill chain

Si vous devez gérer l'incident de manière plus granulaire, vous pouvez appliquer des mesures d'intervention différentes à chacun des nœuds de la cyber kill chain. Ces mesures d'intervention vous permettent d'atténuer les nœuds rapidement et facilement.

Remarque
Pour appliquer des mesures d'intervention globales à l'intégralité d'un incident, reportez-vous à "Atténuer l'intégralité d'un incident" (p. 1305).

Les mesures d'intervention sont divisées dans les catégories suivantes. Toutefois, les nœuds n'incluent pas tous la totalité des catégories suivantes :

© Acronis International GmbH, 2003-2026

- **Réparer** : Les actions de cette catégorie vous permettent d'appliquer une réponse immédiate à l'attaque. Elles incluent la gestion de l'isolation réseau d'une ressource, ainsi que la suppression et la mise en quarantaine de fichiers, de processus et de valeurs de registre.
- **Investigation** : Les actions de cette catégorie (applicables uniquement aux ressources) vous permettent d'exécuter une sauvegarde de données d'investigation, une connexion de bureau à distance ou une ligne de commande ou un terminal à distance pour une investigation plus approfondie.
- **Restauration** : Les actions de cette catégorie (applicables uniquement aux ressources) vous permettent de répondre aux attaques intensives en exécutant une restauration à partir d'une sauvegarde ou un basculement de Disaster Recovery.
- **Prévenir** : Les actions de cette catégorie vous permettent de prévenir les futures menaces ou les faux positifs en les ajoutant à la liste d'autorisation ou la liste de blocage d'un plan de protection.

Remarque
Si un incident est clos, vous ne pouvez pas appliquer de mesure d'intervention à un nœud. En revanche, vous pouvez rouvrir un incident clos en modifiant son état d'investigation et en choisissant **Enquête en cours**. Une fois qu'il est rouvert, vous pouvez lui appliquer des mesures d'intervention.

Le tableau suivant décrit chacun des types de nœuds de la cyber kill chain, les catégories applicables pour chaque nœud et les mesures d'intervention disponibles.

Nœud	Catégorie	Mesures d'intervention
Ressource	Réparer	• Gérer l'isolation du réseau • Redémarrer la ressource
	Examiner	• Sauvegarde de données d'investigation • Connexion à distance au bureau • Exécuter la ligne de commande à distance (Windows) • Exécuter le terminal (macOS)
	Restauration	• Restauration à partir d'une

© Acronis International GmbH, 2003-2026

Nœud	Catégorie	Mesures d'intervention
		sauvegarde • Basculement pour Disaster Recovery
	Prévenir	• Correctif
Processus	Réparer	• Stopper le processus • Quarantaine
	Prévenir	• Ajouter à la liste d'autorisation • Ajouter à la liste de blocage
Fichier	Réparer	• Supprimer • Quarantaine
	Prévenir	• Ajouter à la liste d'autorisation • Ajouter à la liste de blocage
Registre	Réparer	• Supprimer
Réseau	Prévenir	• Ajouter à la liste d'autorisation • Ajouter à la liste de blocage

Définir des mesures d'intervention pour une ressource affectée

Dans le cadre de votre réponse à une attaque, vous pouvez appliquer les actions suivantes aux ressources affectées :

- **Gérer l'isolation du réseau** : Vous permet de gérer l'isolation réseau d'une ressource afin d'arrêter le déplacement latéral ou les activités de commande et contrôle. Pour plus d'informations, voir "Gérer l'isolation réseau d'une ressource" (p. 1313).
- **Correctif** : Vous permet d'installer un correctif sur une ressource afin d'éviter toute exploitation future des vulnérabilités lors de prochaines attaques potentielles. Pour plus d'informations, voir "Correction de ressource" (p. 1317).
- **Redémarrer la ressource** : Vous permet de redémarrer une ressource immédiatement, ou de la redémarrer en fonction d'un délai d'expiration prédéfini. Pour plus d'informations, voir "Redémarrer une ressource" (p. 1319).

© Acronis International GmbH, 2003-2026

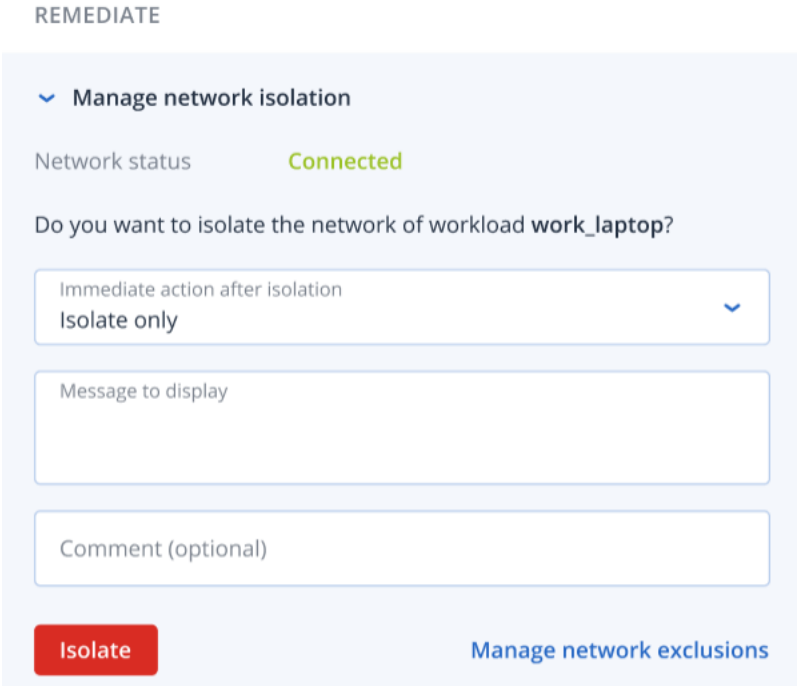
- **Sauvegarde de données d'investigation** : Vous permet d'effectuer une sauvegarde de données d'investigation à la demande à des fins d'audit ou d'investigation. Pour plus d'informations, voir "Exécuter une sauvegarde de données d'investigation à la demande sur une ressource" (p. 1321).
- **Connexion Bureau à distance** : Vous permet d'accéder à distance à la ressource faisant l'objet d'investigations. Pour plus d'informations, voir "Connexion à distance à une ressource" (p. 1322).
- **Restauration à partir d'une sauvegarde** : Vous permet de restaurer à partir de la sauvegarde l'intégralité de votre ordinateur, ou des fichiers ou dossiers spécifiques. Pour plus d'informations, voir "Restauration à partir d'une sauvegarde" (p. 1323).
- **Basculement pour Disaster Recovery** : Vous permet d'exécuter "Implémentation de la reprise d'activité après sinistre" (p. 1016). Notez que votre ressource doit avoir un abonnement à Advanced Disaster Recovery. Pour plus d'informations, voir "Basculement pour Disaster Recovery" (p. 1324).

Gérer l'isolation réseau d'une ressource

La fonctionnalité EDR vous permet de gérer l'isolation réseau d'une ressource afin d'arrêter le déplacement latéral ou les activités de commande et contrôle. Selon vos exigences, vous avez le choix parmi différentes options d'isolation. Notez que toutes les technologies Acronis Cyber Protect sont fonctionnelles, même si une ressource est isolée, ce qui garantit le bon déroulement d'une enquête.

Pour isoler une ressource du réseau

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez traiter.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Gérer l'isolation du réseau**.



© Acronis International GmbH, 2003-2026

Remarque
La valeur **État du réseau** indique si la ressource est connectée. Si la valeur indique **Isolé**, vous pouvez reconnecter la ressource isolée au réseau en suivant la procédure ci-dessous. Si la ressource est hors ligne, vous pouvez toujours l'isoler. Lorsqu'elle revient en ligne, elle passe automatiquement à l'état **Isolé**.

4. Dans la liste déroulante **Action immédiate après isolation**, sélectionnez l'une des options suivantes :
   - **Isoler uniquement**
   - **Isoler et sauvegarder la ressource**
   - **Isoler et sauvegarder la ressource avec des données d'investigation**
   - **Isoler la ressource et la mettre hors tension**

   Pour plus d'informations sur la définition de l'emplacement de sauvegarde de la ressource et des options de chiffrement, voir "Gestion de la sauvegarde et de la restauration des ressources et fichiers" (p. 513).
5. [Facultatif] Dans le champ **Message à afficher**, ajoutez un message qui sera visible par les utilisateurs finaux lorsqu'ils accéderont à la ressource isolée. Par exemple, vous pouvez informer les utilisateurs que la ressource est désormais isolée et que l'accès réseau (entrant et sortant) de la ressource n'est pas disponible pour l'instant. Notez que ce message s'affiche également sous la forme d'une notification dans la zone de notification et qu'il reste affiché jusqu'à ce que l'utilisateur le ferme.
6. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
7. Cliquez sur **Gérer les exclusions du réseau** pour ajouter des ports, des adresses URL, des noms d'hôte et des adresses IP qui auront accès à la ressource pendant l'isolation. Pour plus d'informations, consultez la procédure de gestion des exclusions réseau.
8. Cliquez sur **Isoler**.
   La ressource est isolée. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Remarque
La ressource est également affichée dans l'état **Isolé** dans le menu **Ressources** de la console Cyber Protect. Vous pouvez également isoler une ou plusieurs ressources à partir du menu **Ressources > Ressources avec agents** : sélectionnez la ou les ressources pertinentes, puis **Gérer l'isolation du réseau** dans l'encadré de droite. Dans la boîte de dialogue affichée, vous pouvez gérer les exclusions réseau, puis cliquer sur **Isoler** ou **Tout isoler** afin d'isoler les ressources sélectionnées.

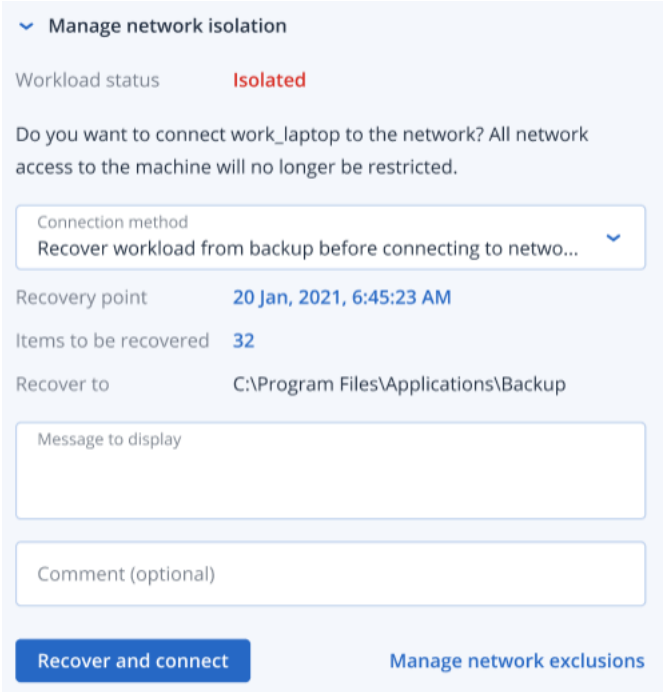
Pour reconnecter une ressource isolée au réseau

© Acronis International GmbH, 2003-2026

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez reconnecter.

   Remarque
   Si la ressource isolée est hors ligne, vous pouvez toujours la reconnecter au réseau. Lorsqu'elle revient en ligne, elle prend automatiquement l'état **Connecté**.

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Gérer l'isolation du réseau**.
4. Sélectionnez l'une des options suivantes :
   - **Connecter immédiatement au réseau** : La ressource est reconnectée au réseau.
   - **Restaurer la ressource depuis la sauvegarde avant connexion au réseau** : Sélectionnez un point de restauration à partir duquel récupérer la ressource.
     a. Dans le champ **Point de restauration**, cliquez sur **Sélectionner**.
     b. Dans l'encadré affiché, sélectionnez le point de restauration pertinent.
     c. Cliquez sur **Restaurer > Intégralité de la ressource** pour restaurer tous les fichiers et dossiers de la ressource.
     Ou
     Cliquez sur **Restaurer > Fichiers/dossiers** pour restaurer des fichiers et dossiers spécifiques sur la ressource. Vous êtes alors invité à sélectionner les fichiers ou dossiers pertinents. Une fois la sélection effectuée, vous pouvez afficher la liste des éléments en cliquant sur la valeur pertinente dans le champ **Éléments à restaurer**.



   Remarque
   Si le point de restauration que vous sélectionnez est chiffré, vous êtes invité à fournir le mot de passe.

© Acronis International GmbH, 2003-2026

5. [Facultatif] Cochez la case **Redémarrer automatiquement la ressource, si nécessaire**. Cette option n'est pertinente que si vous avez sélectionné **Restaurer > Intégralité de la ressource** à l'étape 4.
6. [Facultatif] Dans le champ **Message à afficher**, ajoutez un message qui sera visible par les utilisateurs finaux lorsqu'ils accéderont à la ressource connectée. Par exemple, vous pouvez informer les utilisateurs qu'une sauvegarde a été restaurée sur la ressource et que l'accès réseau (entrant et sortant) de la ressource est de nouveau opérationnel.
7. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
8. Cliquez sur **Connexion** si vous avez sélectionné l'option **Connecter immédiatement au réseau** à l'étape 4.
   Ou
   Cliquez sur **Restaurer et connecter** si vous avez sélectionné l'option **Restaurer la ressource depuis la sauvegarde avant connexion au réseau** à l'étape 4.
   La ressource est reconnectée au réseau, et tout accès réseau à cette ressource n'est plus limité.

Remarque
Vous pouvez également connecter une ou plusieurs ressources à partir du menu **Ressources > Ressources avec agents** dans la console Cyber Protect : sélectionnez la ou les ressources pertinentes, puis **Gérer l'isolation du réseau** dans l'encadré de droite. Dans la boîte de dialogue qui s'affiche, cliquez sur **Connexion** ou **Connecter tout** pour reconnecter la ou les ressources sélectionnées au réseau.

Pour gérer les exclusions du réseau

Remarque
Même si toutes les technologies Acronis Cyber Protect sont opérationnelles lorsque la ressource est isolée, certains scénarios nécessitent l'établissement d'autres connexions réseau (par exemple, vous devrez peut-être transférer un fichier de la ressource vers un répertoire partagé). Dans ces scénarios, vous pouvez ajouter une exclusion du réseau ; toutefois, veillez au préalable à ce que toutes les menaces soient supprimées.

1. Dans la section **Réparer** de l'onglet **Mesures d'intervention**, cliquez sur **Gérer les exclusions du réseau**.
2. Dans l'encadré Exclusion du réseau, ajoutez les exclusions pertinentes. Pour chacune des options disponibles (Ports, Adresse URL et Nom d'hôte/Adresse IP), procédez comme suit :
   a. Cliquez sur **Ajouter**, puis saisissez le ou les ports, adresses URL ou nom d'hôte/adresses IP pertinents.
   b. Dans la liste déroulante **Direction du trafic**, sélectionnez l'une des **connexions entrantes et sortantes**, des **connexions entrantes uniquement** ou des **connexions sortantes**

© Acronis International GmbH, 2003-2026

uniquement.

c. Cliquez sur **Ajouter**.

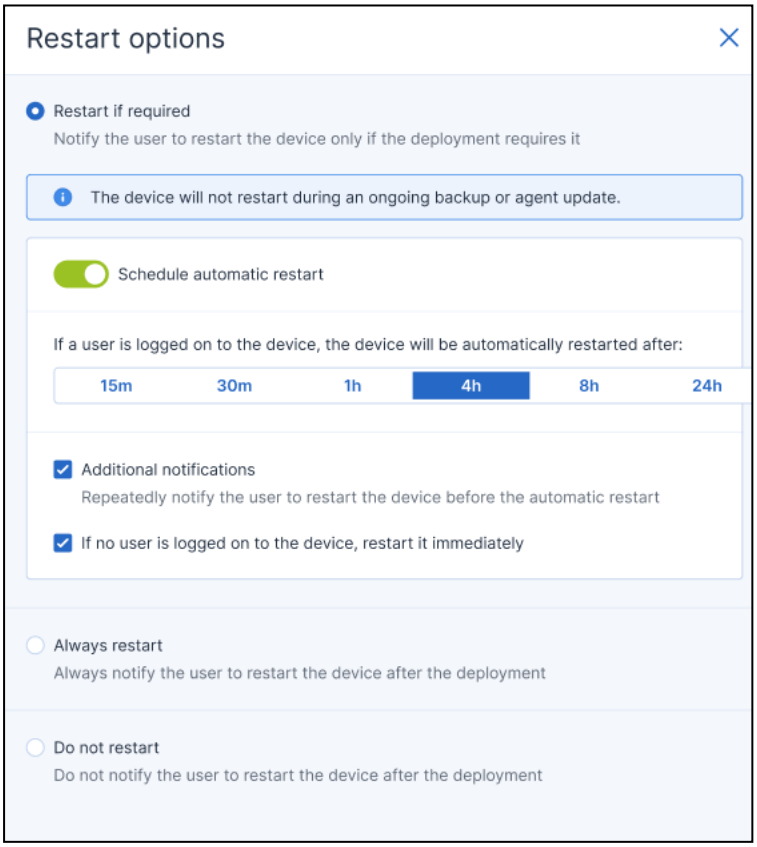
3. Cliquez sur **Enregistrer**.

Correction de ressource

La fonctionnalité EDR détecte automatiquement si une ressource nécessite un correctif. Elle vous permet d'installer ce correctif afin d'éviter toute exploitation des vulnérabilités lors de prochaines attaques potentielles. Notez que cette fonctionnalité n'est disponible que si la ressource du partenaire comprend un abonnement pour RMM.

Pour corriger une ressource

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez corriger.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Correctif**.
4. Dans le champ **Correctifs à installer**, cliquez sur **Sélectionner**. Dans la boite de dialogue qui s'affiche, sélectionnez les correctifs pertinents, puis cliquez sur **Sélectionner**.
5. Dans le champ **Options de redémarrage**, cliquez sur le lien affiché. La boîte de dialogue **Options de redémarrage** s'affiche.
6. Sélectionnez si vous souhaitez que la ressource soit redémarrée après l'installation des correctifs.



Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

© Acronis International GmbH, 2003-2026

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage.

© Acronis International GmbH, 2003-2026

Option	Description
	• 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

7. Cliquez sur **Enregistrer**.
8. Dans l'onglet **Mesures d'intervention**, cliquez sur **Correctif**.
   Le correctif sélectionné est exécuté. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Redémarrer une ressource

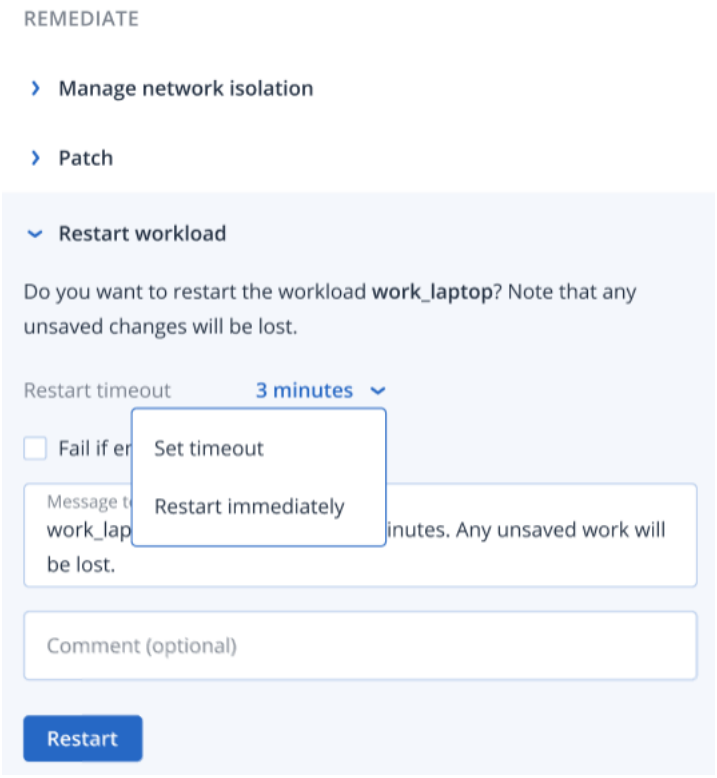
Dans le cadre de votre réponse d'atténuation à une attaque, la fonctionnalité EDR vous permet de redémarrer une ressource immédiatement, ou de la redémarrer en fonction d'un délai d'expiration prédéfini.

Pour redémarrer une ressource

1. Dans la cyber kill chain, cliquez sur le nœud de ressource pour lequel vous souhaitez planifier le redémarrage.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Réparer**, cliquez sur **Redémarrer la ressource**.



4. Dans le champ **Délai d'attente de redémarrage**, cliquez sur le lien affiché, puis sélectionnez l'une des options suivantes :
   - **Définir le délai d'attente** : Dans la boîte de dialogue Délai d'attente de redémarrage, définissez la période de redémarrage de la ressource, puis cliquez sur **Enregistrer**.
   - **Redémarrer immédiatement** : Sélectionnez cette option pour redémarrer la ressource immédiatement.
5. [Facultatif] Cochez la case **Échec si l'utilisateur final est connecté** afin que la ressource ne soit pas redémarrée si l'utilisateur est connecté.
6. Dans le champ **Message à afficher**, ajoutez un message qui sera visible par les utilisateurs lorsqu'ils accéderont à la ressource isolée.
7. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
8. Cliquez sur **Redémarrer**.
   La ressource est configurée pour redémarrer en fonction de la planification définie. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

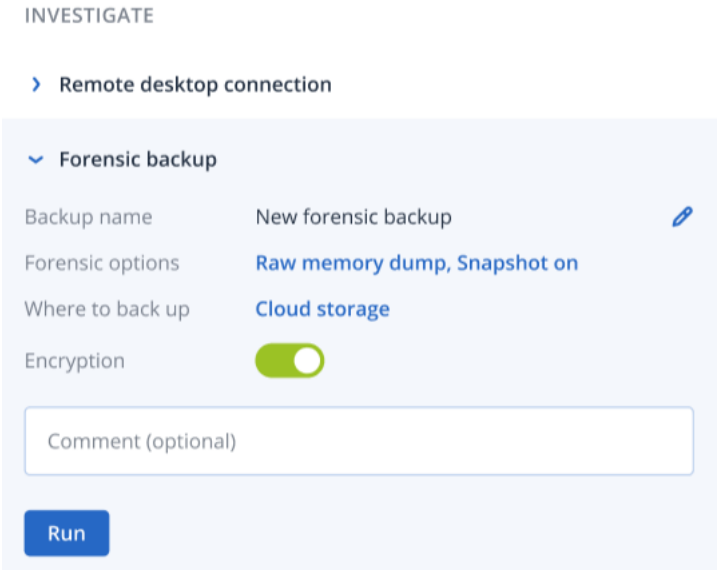
© Acronis International GmbH, 2003-2026

Exécuter une sauvegarde de données d'investigation à la demande sur une ressource

Dans le cadre de votre enquête sur une attaque, la fonctionnalité EDR vous permet d'effectuer une sauvegarde de données d'investigation à la demande à des fins d'audit ou d'investigation.

Pour exécuter une sauvegarde de données d'investigation

1. Dans la cyber kill chain, cliquez sur le nœud de la ressource sur laquelle vous souhaitez exécuter une sauvegarde de données d'investigation.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Examiner**, cliquez sur **Sauvegarde de données d'investigation**.



4. [Facultatif] Dans le champ **Nom de la sauvegarde**, cliquez sur l'icône de modification pour modifier le nom de la sauvegarde.
5. Dans le champ **Options d'investigation**, cliquez sur le lien affiché. Dans la boîte de dialogue Options d'investigation, sélectionnez l'une des options suivantes :
   - **Collecter le vidage mémoire brut**
   - **Collecter le vidage mémoire du noyau**

   Vous pouvez également cocher la case **Instantané des processus en cours d'exécution** pour ajouter des informations sur les processus en cours d'exécution au démarrage de la sauvegarde. Ces informations sont stockées dans une image de sauvegarde.

   Cliquez sur **Enregistrer** pour fermer la boîte de dialogue Options d'investigation.
6. Dans le champ **Où sauvegarder**, cliquez sur le lien pour définir l'emplacement de la sauvegarde.
7. [Facultatif] Cliquez sur l'option **Chiffrement** pour activer le chiffrement. Dans la boîte de dialogue qui s'affiche, saisissez le mot de passe de la sauvegarde chiffrée et sélectionnez l'algorithme de chiffrement pertinent.
8. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous

© Acronis International GmbH, 2003-2026

aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.

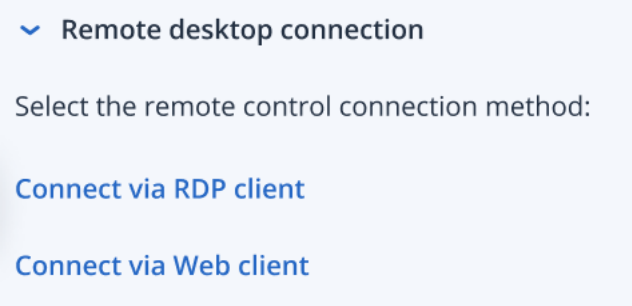
9. Cliquez sur **Exécuter**.
   La sauvegarde de données d'investigation démarre. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Connexion à distance à une ressource

Dans le cadre de votre enquête sur une attaque, la fonctionnalité EDR vous permet d'accéder à distance à la ressource faisant l'objet d'investigations.

Pour vous connecter à distance à une ressource

1. Dans la cyber kill chain, cliquez sur le nœud de la ressource à laquelle vous souhaitez vous connecter à distance.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Examiner**, cliquez sur **Connexion Bureau à distance**.



4. Sélectionnez l'une des méthodes de connexion à distance suivantes :
   - **Se connecter via un client RDP** : Cette méthode vous invite à télécharger et à installer le client Connexion Bureau à distance. Vous pouvez alors vous connecter à distance à une ressource à partir de la console Cyber Protect.
   - **Se connecter via le client Web** : Cette méthode ne nécessite l'installation d'aucun client RDP sur la ressource. Vous êtes redirigé vers l'écran de connexion dans lequel vous devez saisir vos identifiants de connexion à la machine distante.

   Lorsque la connexion à distance est démarrée, cette action est visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Exécution de la ligne de commande à distance

Dans le cadre de votre enquête sur une attaque, vous pouvez exécuter à distance la ligne de commande de la ressource en cours d'enquête.

Pour exécuter à distance la ligne de commande d'une ressource

1. Dans la chaîne de cyberkill, cliquez sur le nœud de la ressource auquel vous souhaitez vous connecter à distance.

© Acronis International GmbH, 2003-2026

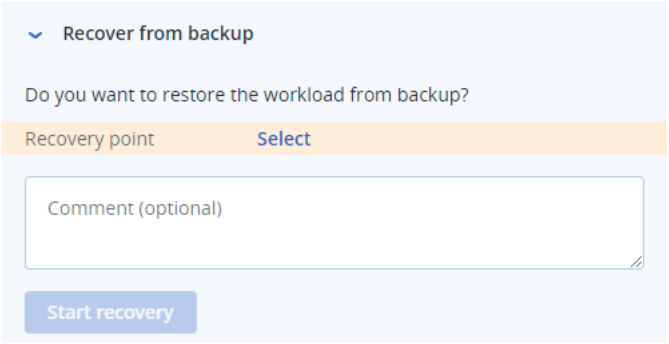
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. En fonction du système d'exploitation de la ressource, effectuez l'une des opérations suivantes :
   - [Pour les ressources Windows] Dans la section **Investigation**, développez **Interface de ligne de commande à distance**, puis cliquez sur **Exécuter la ligne de commande**.
   - [Pour les ressources macOS] Dans la section **Investigation**, développez **Terminal à distance**, puis cliquez sur **Exécuter le terminal**.

Restauration à partir d'une sauvegarde

Dans le cadre de votre réponse de restauration à une attaque, la fonctionnalité EDR vous permet de restaurer à partir de la sauvegarde l'intégralité de votre ordinateur, ou des fichiers ou dossiers spécifiques.

Pour restaurer votre ressource depuis la sauvegarde

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez restaurer.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Restauration**, cliquez sur **Restauration à partir d'une sauvegarde**.



4. Dans le champ **Point de restauration**, cliquez sur **Sélectionner** et effectuez les opérations suivantes :
   a. Dans l'encadré affiché, sélectionnez le point de restauration pertinent.
   b. Cliquez sur **Restaurer > Intégralité de la ressource** pour restaurer tous les fichiers et dossiers de la ressource.
   Ou
   Cliquez sur **Restaurer > Fichiers/dossiers** pour restaurer des fichiers et dossiers spécifiques sur la ressource. Vous êtes alors invité à sélectionner les fichiers ou dossiers pertinents. Une fois la sélection effectuée, vous pouvez afficher les éléments sélectionnés pour la restauration en cliquant sur la valeur pertinente dans le champ **Éléments à restaurer**.

   Remarque
   Si le point de restauration que vous sélectionnez est chiffré, vous êtes invité à fournir le mot de passe.

5. [Facultatif] Cochez la case **Redémarrer automatiquement la ressource**. Cette option n'est pertinente que si vous avez sélectionné **Restaurer > Intégralité de la ressource** à l'étape 4.

© Acronis International GmbH, 2003-2026

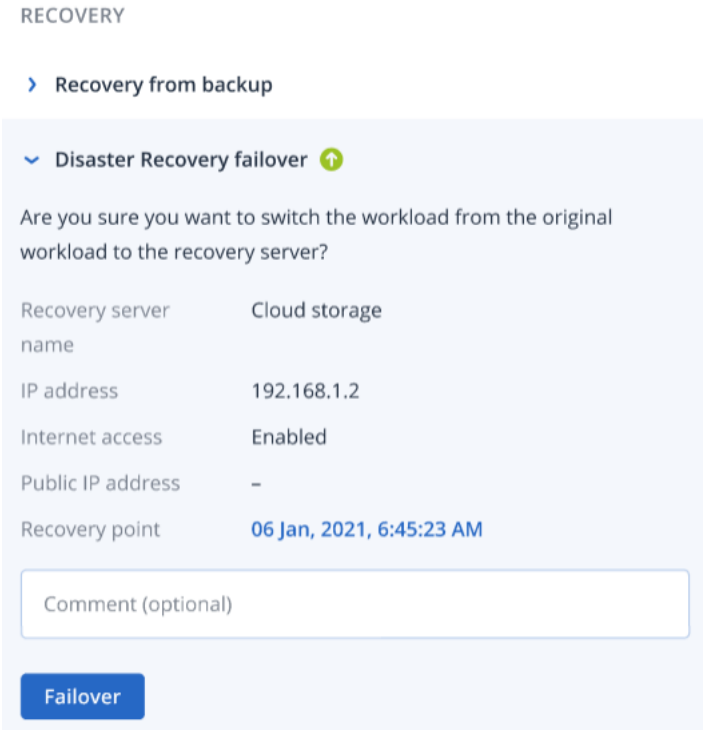
6. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
7. Cliquez sur **Démarrer la restauration**.
   Le processus de restauration de la ressource démarre. La progression de cette action est visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Basculement pour Disaster Recovery

Dans le cadre de votre réponse de restauration à une attaque, la fonctionnalité EDR vous permet d'exécuter "Implémentation de la reprise d'activité après sinistre" (p. 1016) et de basculer la ressource vers le serveur de restauration. Notez que votre ressource doit avoir un abonnement à Advanced Disaster Recovery.

Pour effectuer un basculement pour Disaster Recovery

1. Dans la cyber kill chain, cliquez sur le nœud de ressource que vous souhaitez restaurer.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Restauration**, cliquez sur **Basculement pour Disaster Recovery**.



4. Dans le champ **Point de restauration**, effectuez les opérations suivantes :
   a. Cliquez sur la date du point de restauration actuel pour sélectionner un point de restauration.
   b. Dans l'encadré affiché, sélectionnez le point de restauration pertinent.

© Acronis International GmbH, 2003-2026

Remarque
Si vous avez un abonnement à Advanced Disaster Recovery, vous pouvez sélectionner le serveur de restauration pertinent (la machine virtuelle hors ligne) créée dans Disaster Recovery. Si vous n'avez pas d'abonnement, vous êtes invité à configurer Disaster Recovery.

5. [Facultatif] Dans le champ **Commentaire**, ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Basculement**.
   La ressource est basculée vers le serveur de restauration. Cette action est visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Définir des mesures d'intervention pour un processus suspect

Dans le cadre de votre réponse de réparation à une attaque, vous pouvez appliquer les actions suivantes aux processus suspects :

- Arrêter un processus (voir ci-dessous)
- Mettre un processus en quarantaine (voir ci-dessous)
- Annuler les modifications apportées par un processus (voir ci-dessous)
- Ajouter le processus à la liste d'autorisation ou à la liste de blocage d'un plan de protection (voir "Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection" (p. 1331))

Pour arrêter un processus suspect

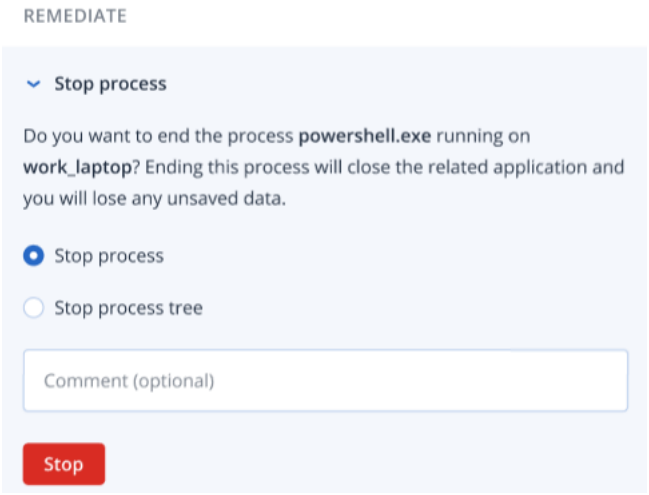
1. Dans la cyber kill chain, cliquez sur le nœud de processus que vous souhaitez traiter.

Remarque
Les processus Windows critiques ou les processus qui ne sont pas en cours d'exécution ne peuvent pas être arrêtés, et sont désactivés dans la cyber kill chain.

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Réparer**, cliquez sur **Stopper le processus**.



4. Sélectionnez l'une des options suivantes :
   - **Stopper le processus** (arrête le processus spécifique)
   - **Stopper l'arborescence de processus** (arrête le processus spécifique et tous les processus enfants)
5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Arrêter**. Le processus est arrêté.

Remarque
L'application associée est fermée et toutes les données non enregistrées sont perdues.

Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Pour mettre un processus suspect en quarantaine

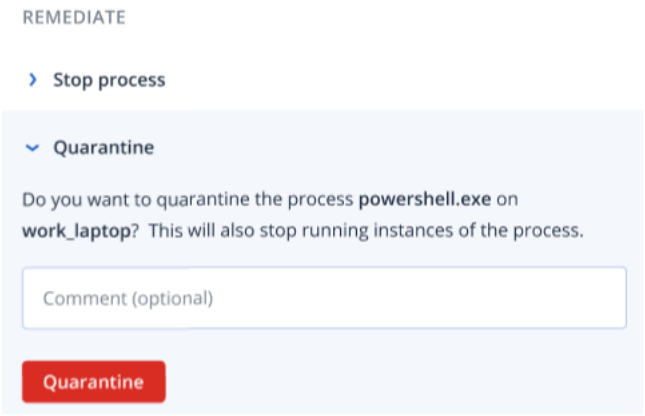
1. Dans la cyber kill chain, cliquez sur le nœud de processus que vous souhaitez mettre en quarantaine.

Remarque
Les processus Windows critiques ne peuvent pas être mis en quarantaine et sont désactivés dans la cyber kill chain.

2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Réparer**, cliquez sur **Quarantaine**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
5. Cliquez sur **Quarantaine**. Le processus est arrêté, puis mis en quarantaine.

Remarque
Le processus est ajouté à la section de quarantaine disponible dans Protection antimalware, d'où il est géré.

Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Pour annuler les modifications

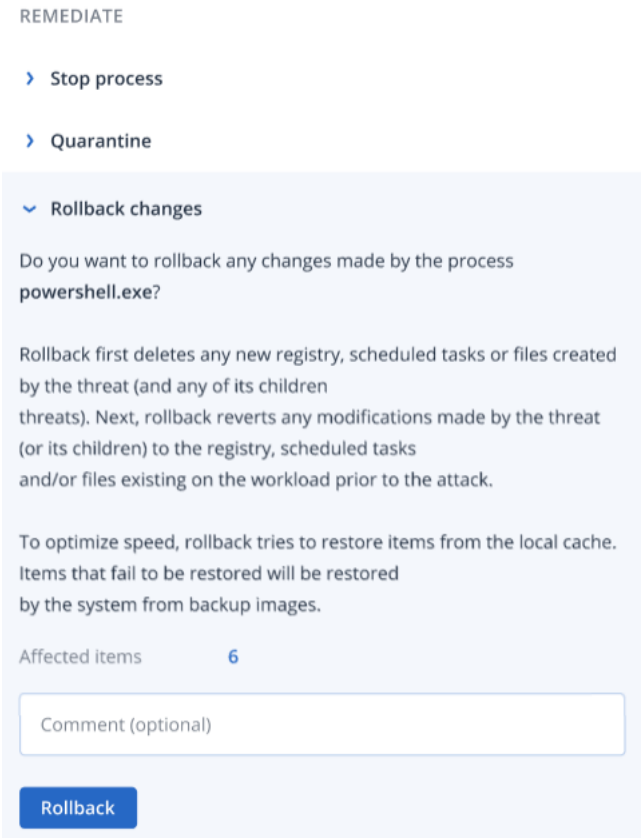
1. Dans la cyber kill chain, cliquez sur le nœud de processus dont vous souhaitez annuler les modifications.

Remarque
Cette action est disponible uniquement pour les nœuds de détection (indiqués en rouge ou en jaune).

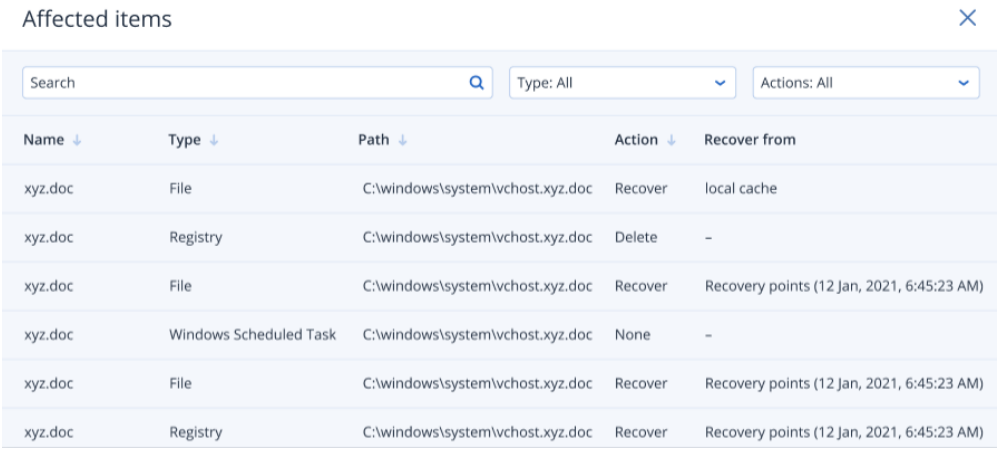
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Réparer**, cliquez sur **Annuler les modifications**.



4. Pour afficher les éléments affectés par l'annulation des modifications, cliquez sur le lien **Éléments affectés**. La boîte de dialogue qui s'affiche répertorie tous les éléments (fichiers, registre, tâches planifiées) que l'annulation rétablit, ainsi que l'action utilisée (**Supprimer**, **Restaurer** ou **Aucune**). Par ailleurs, vous voyez également si les éléments restaurés sont récupérés du cache local ou des points de restauration de sauvegarde.



5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.

© Acronis International GmbH, 2003-2026

6. Cliquez sur **Annuler**. La fonctionnalité d'annulation rétablit les modifications apportées par le processus au registre, à un fichier ou à une tâche planifiée dans les étapes suivantes :
   a. Toutes les nouvelles entrées (registre, tâches planifiées ou fichiers) créées par la menace (et ses menaces enfants) sont supprimées.
   b. Toute modification apportée par la menace (et ses menaces enfants) au registre, aux tâches planifiées et/ou aux fichiers existants sur la ressource avant l'attaque est rétablie.
   c. L'annulation tente de restaurer les éléments depuis le cache local. Pour les éléments qui ne peuvent pas être restaurés, la fonctionnalité EDR les restaure automatiquement à partir d'images de sauvegarde intègres.

   L'action d'annulation est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

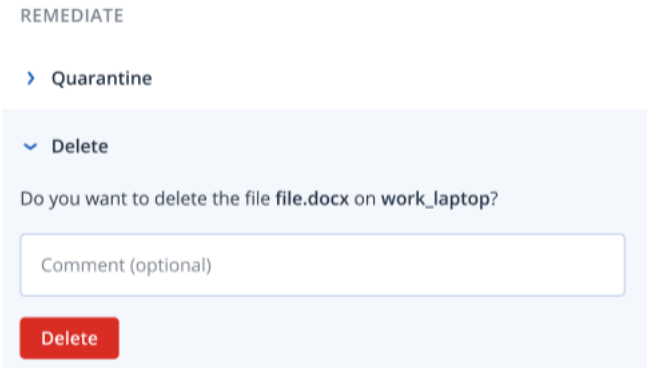
Définir des mesures d'intervention pour un fichier suspect

Dans le cadre de votre réponse de réparation à une attaque, vous pouvez appliquer les actions suivantes aux fichiers suspects :

- Supprimer un fichier (voir ci-dessous)
- Mettre un fichier en quarantaine (voir ci-dessous)
- Ajouter le fichier à la liste d'autorisation ou à la liste de blocage d'un plan de protection (voir "Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection" (p. 1331))

Pour supprimer un fichier suspect

1. Dans la cyber kill chain, cliquez sur le nœud de fichier que vous souhaitez traiter.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Supprimer**.



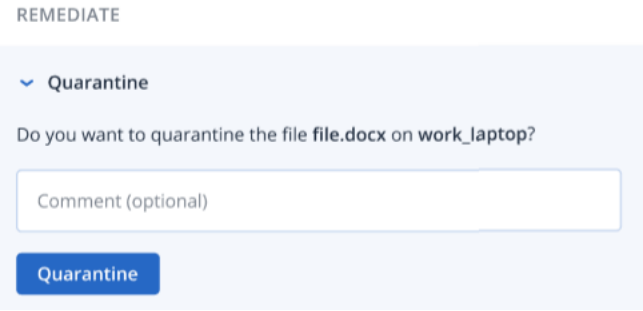
4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.

© Acronis International GmbH, 2003-2026

5. Cliquez sur **Supprimer**.
   Le fichier est supprimé. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Pour mettre un fichier suspect en quarantaine

1. Dans la cyber kill chain, cliquez sur le nœud de fichier que vous souhaitez traiter.
2. Dans l'encadré affiché, accédez à **Mesures d'intervention**.
3. Dans la section **Réparer**, cliquez sur **Quarantaine**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
5. Cliquez sur **Quarantaine**.
   Le fichier est mis en quarantaine. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Définir des mesures d'intervention pour une entrée de registre suspecte

Dans le cadre de votre réponse de réparation à une attaque, vous pouvez supprimer les entrées de registre suspectes.

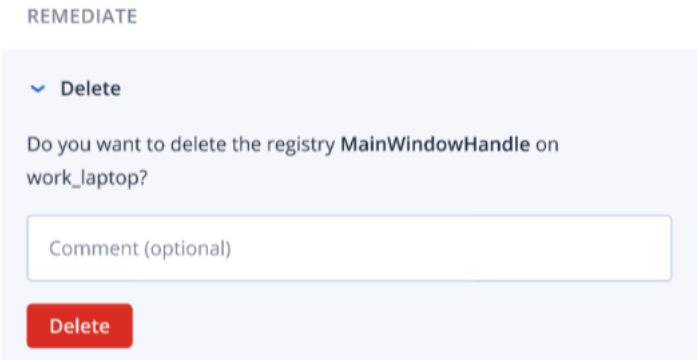
Cette option est disponible pour les nœuds de cyber kill chain du registre.

Pour supprimer une entrée de registre suspecte

1. Dans la cyber kill chain, cliquez sur le nœud que vous souhaitez traiter.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Réparer**, cliquez sur **Supprimer**.



4. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
5. Cliquez sur **Supprimer**.
   L'entrée de registre est supprimée. Cette action est également visible dans les onglets **Activités** du nœud et de l'intégralité de l'incident. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection

Dans le cadre de votre réponse préventive à une attaque, vous pouvez ajouter un nœud à la liste d'autorisation ou à la liste de blocage de votre plan de protection.

Vous pouvez ajouter un nœud à une liste d'autorisation si vous considérez le nœud comme étant sécurisé et souhaitez éviter à l'avenir d'autres détections le concernant. Ajoutez un nœud à une liste de blocage pour que le nœud ne s'exécute plus à l'avenir.

Vous pouvez également supprimer un nœud de la liste d'autorisation ou de la liste de blocage afin d'autoriser ou d'empêcher tout accès futur à ce nœud.

Cette option est disponible pour les nœuds de cyber kill chain suivants :

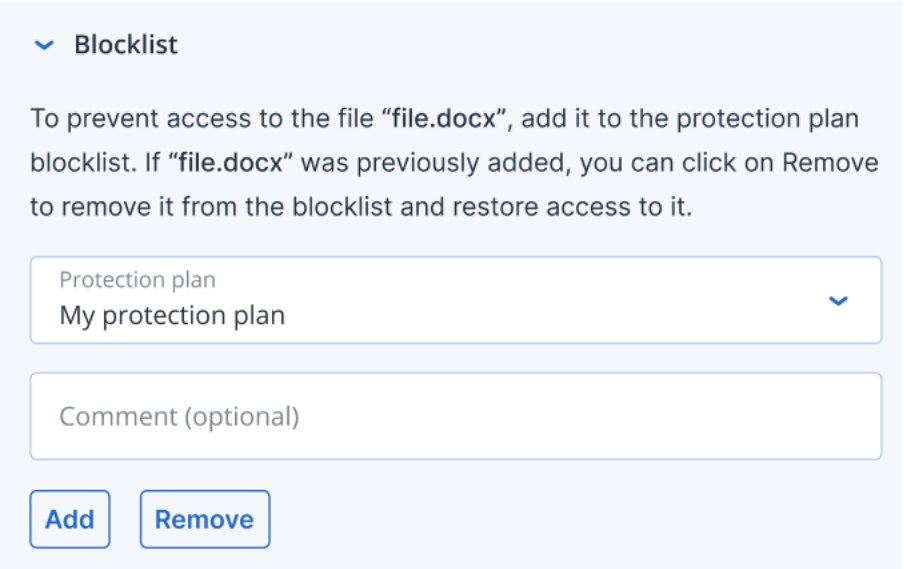
- Processus
- Fichier
- Réseau

Pour ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage du plan de protection

1. Dans la cyber kill chain, cliquez sur le processus, le fichier ou le nœud de réseau dont vous souhaitez résoudre les problèmes.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Prévention**, cliquez sur l'icône en forme de flèche située à côté de **Liste de blocage**.

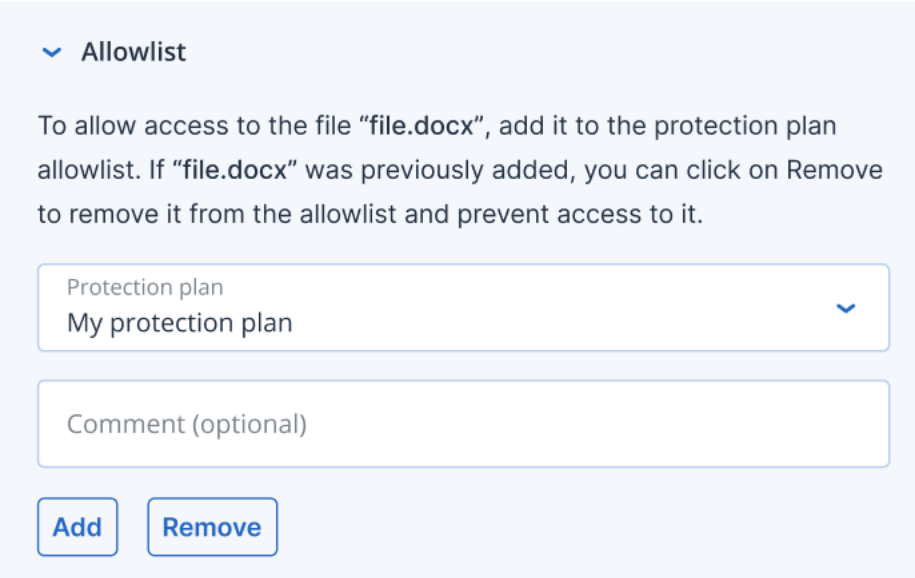


4. Sélectionnez le ou les plans de protection auxquels vous souhaitez appliquer cette mesure.
5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Ajouter**.
   L'action est implémentée, et le processus, le fichier ou le réseau ne pourra plus être lancé.
   Si le processus, le fichier ou le réseau a déjà été ajouté à la liste de blocage et que vous souhaitiez à présent le supprimer de cette liste, cliquez sur **Supprimer**. L'accès au nœud sera ainsi autorisé à l'avenir.
   L'action d'ajout ou de suppression peut également être visualisée dans les onglets **Activités** de chaque nœud et de l'incident dans son intégralité. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Pour ajouter ou supprimer un processus, un fichier ou un réseau dans la liste des autorisations du plan de protection

1. Dans la cyber kill chain, cliquez sur le processus, le fichier ou le nœud de réseau dont vous souhaitez résoudre les problèmes.
2. Dans l'encadré affiché, cliquez sur l'onglet **Mesures d'intervention**.
3. Dans la section **Prévention**, cliquez sur l'icône en forme de flèche à côté de **Liste d'autorisation**.

© Acronis International GmbH, 2003-2026



4. Sélectionnez le ou les plans de protection auxquels vous souhaitez appliquer cette mesure.
5. [Facultatif] Ajoutez un commentaire. Ce commentaire est visible dans l'onglet **Activités** (pour un seul nœud ou pour l'intégralité de l'incident) et pourra vous aider (ou vos collègues), lorsque vous réexaminerez l'incident, à vous souvenir des raisons pour lesquelles vous avez pris cette mesure.
6. Cliquez sur **Ajouter**.
   L'action est implémentée, et le processus, le fichier ou le réseau ne pourra plus être détecté.
   Si le processus, le fichier ou le réseau a déjà été ajouté à la liste d'autorisations et que vous souhaitiez à présent le supprimer de cette liste, cliquez sur **Supprimer**. Cela empêchera tout accès futur au nœud.
   L'action d'ajout ou de suppression peut également être visualisée dans les onglets **Activités** de chaque nœud et de l'incident dans son intégralité. Pour plus d'informations, voir "Comprendre les actions entreprises pour réduire un incident" (p. 1297).

Utilisation de workflows automatisés

Vous pouvez utiliser les workflows automatisés d'Acronis pour appliquer un ensemble d'actions prédéfinies qui peuvent remédier automatiquement aux incidents dans Endpoint Detection and Response (EDR) et Extended Detection and Response (XDR). Ces workflows, ou guides tactiques, vous permettent de rationaliser vos opérations de sécurité pour améliorer le temps de réponse tout en réduisant la charge opérationnelle de gestion et de réponse aux incidents de sécurité.

Six workflows EDR prédéfinis sont disponibles, chacun d'entre eux pouvant être configuré en fonction des besoins. Pour plus d'informations, voir "Workflows Endpoint Detection and Response (EDR)" (p. 1334).

Pour accéder aux workflows automatisés, accédez à **Gestion > Workflows**. La liste des workflows affichée indique les workflows activés ou désactivés, leur heure d'exécution et leur statut.

© Acronis International GmbH, 2003-2026

Workflows Endpoint Detection and Response (EDR)

Il existe six workflows EDR par défaut que vous pouvez configurer selon vos besoins :

- Menace en quarantaine (lorsqu'un incident EDR est créé)
- Menace en quarantaine (lorsqu'un incident EDR est mis à jour)
- Isoler la ressource (lorsqu'un incident EDR est créé)
- Isoler la ressource (lorsqu'un incident EDR est mis à jour)
- Incident de malware nécessitant une attention particulière
- Incident nécessitant une attention particulière

Le tableau suivant décrit les déclencheurs, conditions et actions par défaut applicables à chaque workflow. Pour plus d'informations sur la modification de ces conditions et actions, voir "Configuration d'un workflow automatisé EDR (Endpoint Detection and Response)" (p. 1336).

Étapes de la procédure	Déclencheur	Conditions	Actions
Menace en quarantaine	L'incident EDR est créé	État de la menace = Non atténuée ET État de l'incident = Non démarré ET Gravité = Élevée ET Type d'incident = Processus détecté OU Malware détecté	1. Arrêtez le processus. 2. Mettez le processus en quarantaine. 3. Ajoutez un commentaire. Le texte du commentaire par défaut est « <Workflow name> - Menace de gravité élevée placée en quarantaine. 4. Clôturez l'incident.
Menace en quarantaine	L'incident EDR est mis à jour		

© Acronis International GmbH, 2003-2026

Étapes de la procédure	Déclencheur	Conditions	Actions
Isoler la ressource	L'incident EDR est créé	État de la menace = Non atténuée ET État de l'incident = Non démarré ET Gravité = Critique ET Verdict = Malveillant ET Niveau de positivité > 9 ET Type d'incident = Processus détecté OU Malware détecté	1. Arrêtez le processus. 2. Mettez le processus en quarantaine. 3. Isolez la ressource. 4. Ajoutez un commentaire. Le texte du commentaire par défaut est <Workflow name> - La ressource <Workload name> a été isolée après la détection d'un malware critique. 5. Envoyez un e-mail aux utilisateurs de la console Cyber Protect sélectionnés.
Isoler la ressource	L'incident EDR est mis à jour		
Incident de malware nécessitant une attention particulière	L'incident EDR est créé	État de la menace = Non atténuée ET État de l'incident = Non démarré ET Ancienneté de l'incident > 8 heures ET Gravité = Élevée OU Critique ET Verdict = Malveillant	1. Arrêtez le processus. 2. Mettez le processus en quarantaine. 3. Ajoutez un commentaire. Le texte du commentaire par défaut est « <Workflow name> - Mise en quarantaine d'une menace de gravité élevée/critique en raison de

© Acronis International GmbH, 2003-2026

Étapes de la procédure	Déclencheur	Conditions	Actions
		ET Type d'incident = Détection de malware	l'absence d'enquête pendant 8 h ». 4. Envoyez un e-mail aux utilisateurs de la console Cyber Protect sélectionnés.
Incident nécessitant une attention particulière	L'incident EDR est créé	État de la menace = Non atténuée ET État de l'incident = Non démarré ET Âge de l'incident > 24 heures ET Gravité = Élevée OU Critique ET Verdict = Malveillant	1. Arrêtez le processus. 2. Mettez le processus en quarantaine. 3. Ajoutez un commentaire. Le texte du commentaire par défaut est « <Workflow name> - Mise en quarantaine d'une menace de gravité élevée/critique en raison de l'absence d'enquête pendant 24 h ». 4. Envoyez un e-mail aux utilisateurs de la console Cyber Protect sélectionnés.

Configuration d'un workflow automatisé EDR (Endpoint Detection and Response)

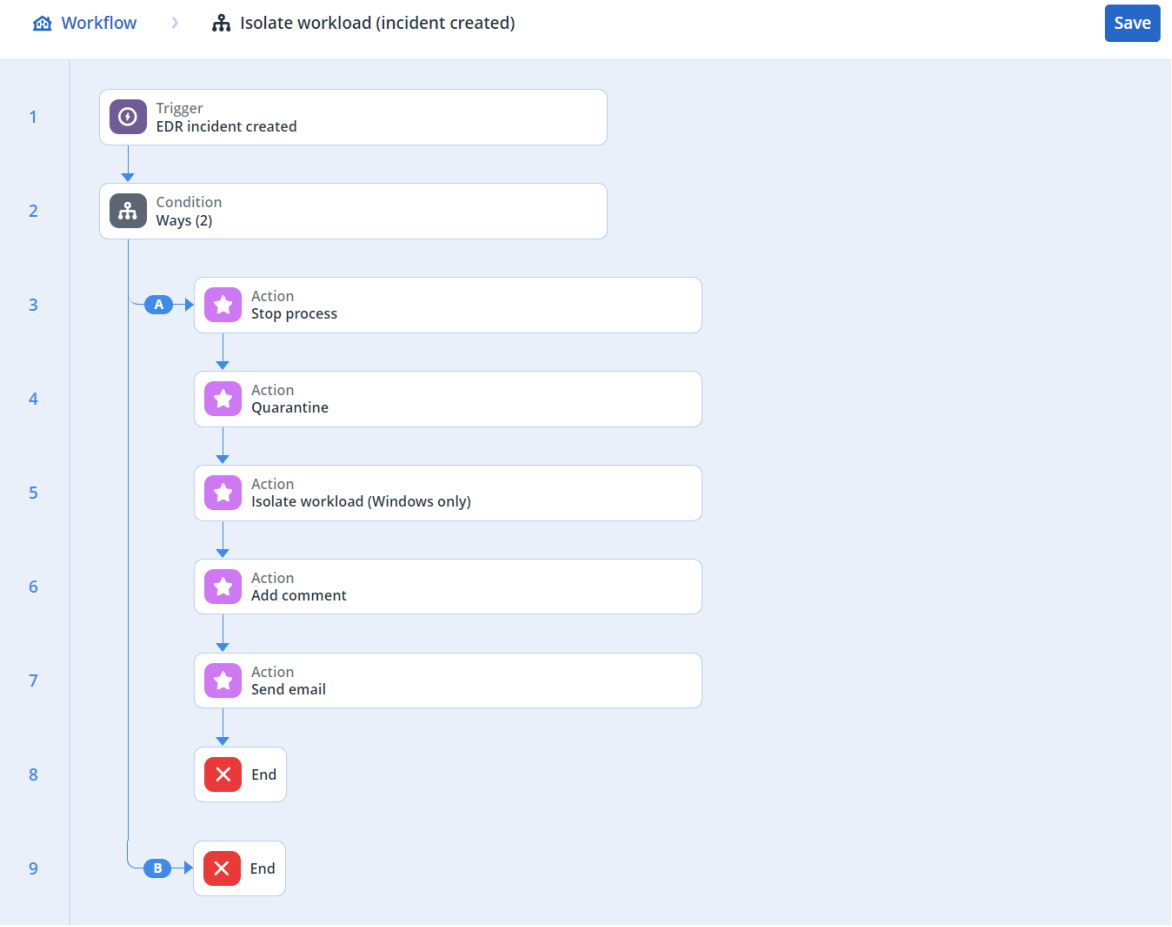
Vous pouvez configurer n'importe lequel des workflows EDR prédéfinis selon vos besoins.

Pour configurer un workflow EDR

1. Dans la console Cyber Protect, accédez à **Gestion > Workflows**.
2. Dans la colonne à l'extrême droite, cliquez sur l'icône représentant des points de suspension (...) dans la ligne du workflow que vous souhaitez configurer, puis sélectionnez **Ouvrir**.

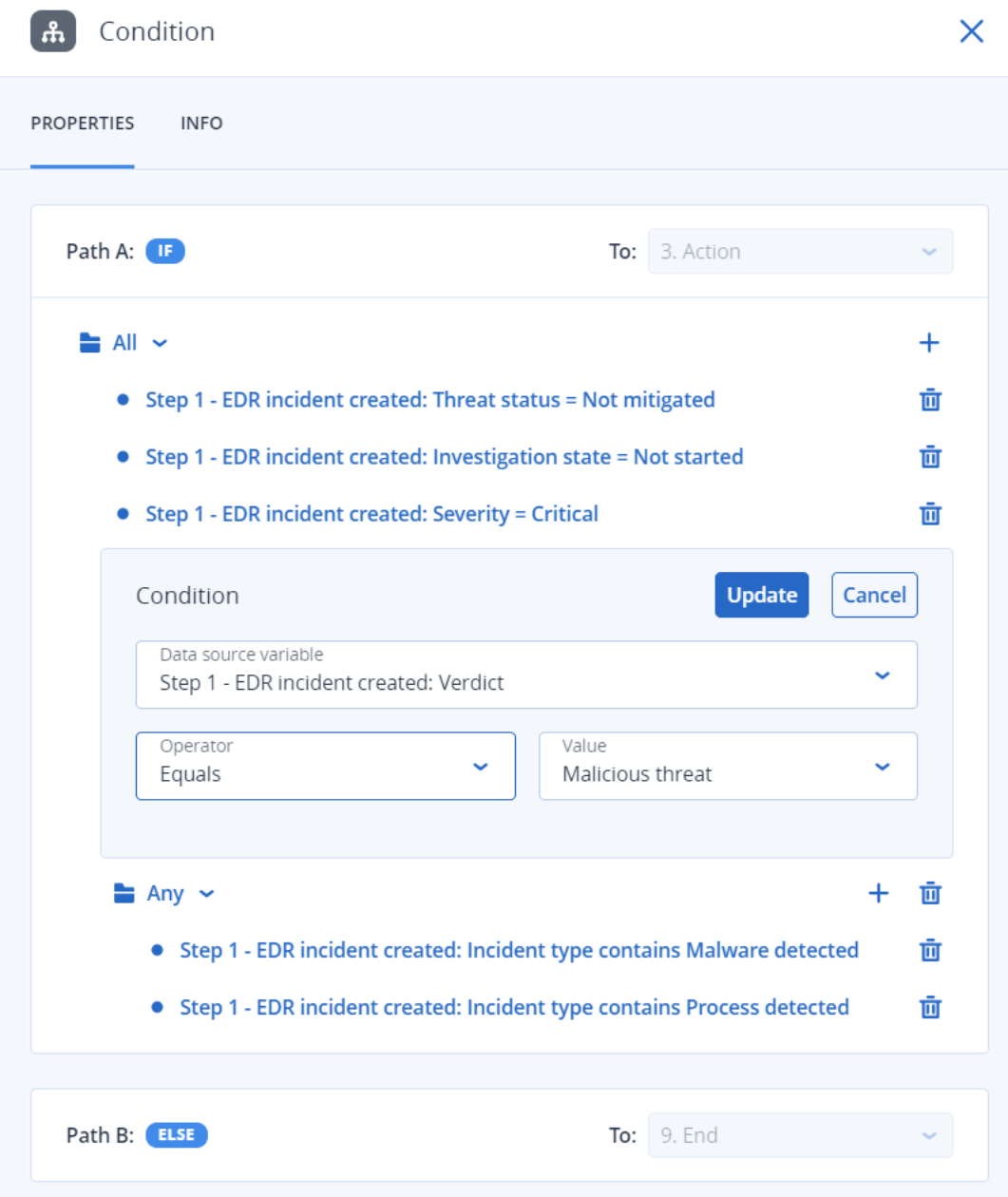
© Acronis International GmbH, 2003-2026

Vous pouvez également cliquer sur le workflow approprié, puis sur **Ouvrir** dans le volet affiché. Les conditions et les actions du workflow s'affichent.



3. Pour afficher et modifier l'une des conditions du workflow, cliquez sur le bloc **Condition**.

© Acronis International GmbH, 2003-2026



Le bloc de condition définit un ensemble de conditions qui doivent être exécutées dans le cadre du workflow, et se compose de deux types de bloc :

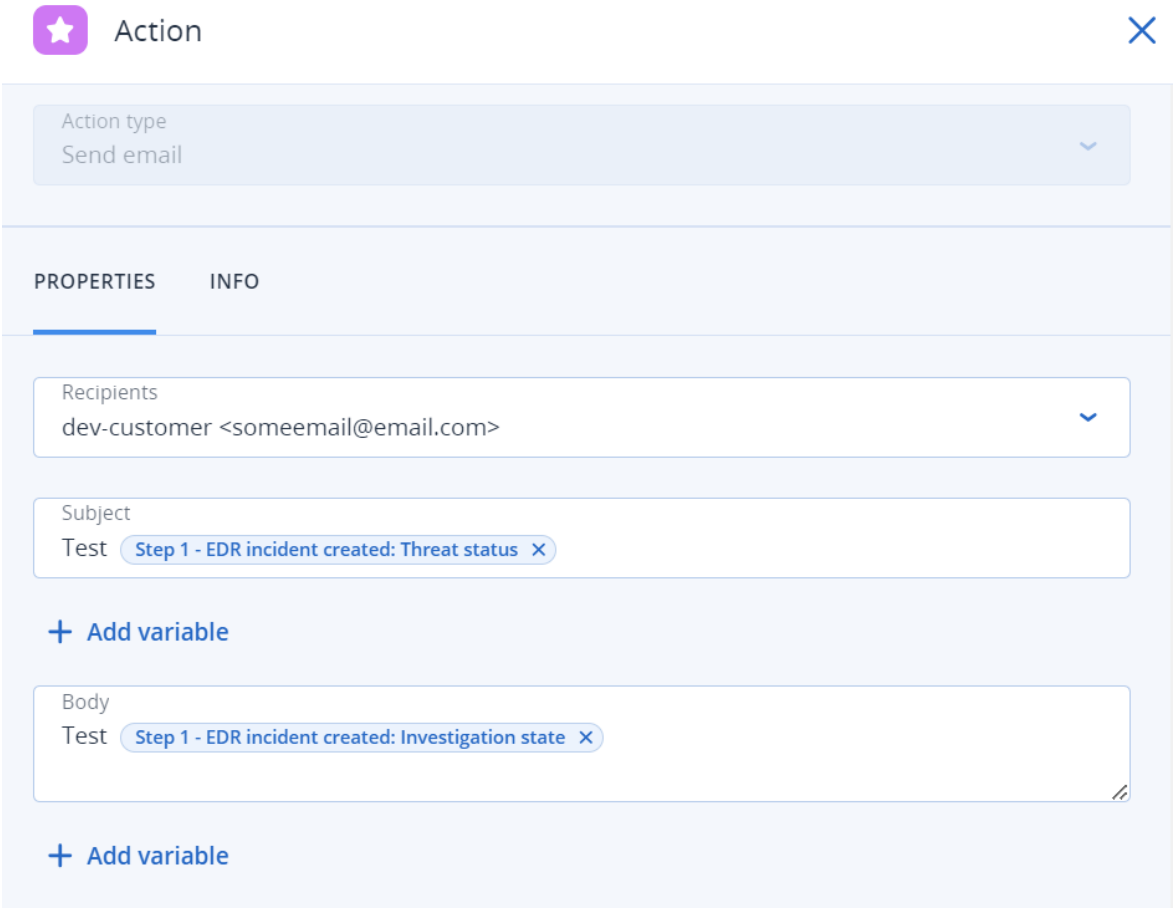
- **Tous** : toutes les conditions de ce bloc doivent être remplies pour que vous puissiez passer à l'étape suivante du workflow.
- **Tout** : au moins une des conditions de ce bloc doit être remplie pour que vous puissiez passer à l'étape suivante du workflow.

4. Pour modifier une condition, cliquez sur la condition et modifiez les valeurs pertinentes. Lorsque vous avez terminé, cliquez sur **Mettre à jour**.

   Notez que vous pouvez également supprimer une condition en cliquant sur l'icône de la corbeille située à côté.
5. Pour modifier une action, cliquez sur l'action que vous souhaitez modifier.
6. Dans le volet affiché, apportez les modifications nécessaires.

© Acronis International GmbH, 2003-2026

Par exemple, cliquez sur l'action **Envoyer un e-mail**, puis modifiez les destinataires, le corps et le sujet de l'e-mail envoyé dans le cadre de ce workflow.



7. [Facultatif] Modifiez les actions supplémentaires.
8. Cliquez sur **Enregistrer**.

   Si le workflow n'était pas activé et qu'il se trouve dans l'état **Brouillon**, cliquez sur **Enregistrer et activer** pour l'activer. Sinon, cliquez sur **Enregistrer** pour le laisser **Désactivé**.

   Vous pouvez activer et désactiver un workflow à partir de l'écran principal des workflows en cliquant sur le workflow pertinent et en sélectionnant **Activer** ou **Désactiver**, selon vos besoins.

Activation du mode de surveillance pour EDR (Endpoint Detection and Response)

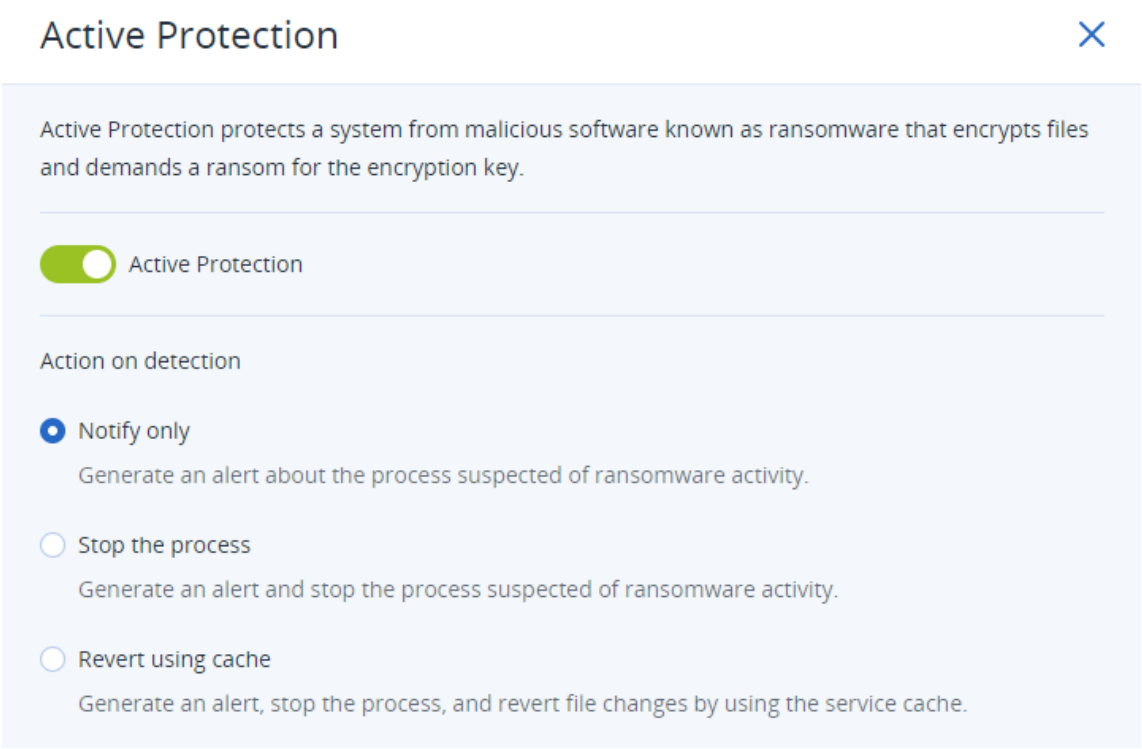
Le mode de surveillance dans Cyber Protection vous permet d'utiliser EDR dans un environnement de production. Cela vous permet de rechercher la présence de faux positifs et d'exclure les éléments nécessaires avant de déployer entièrement EDR.

En mode de surveillance, rien n'est bloqué ni arrêté. Des incidents sont créés, mais aucune réponse n'est initiée.

Pour activer le mode de surveillance pour EDR

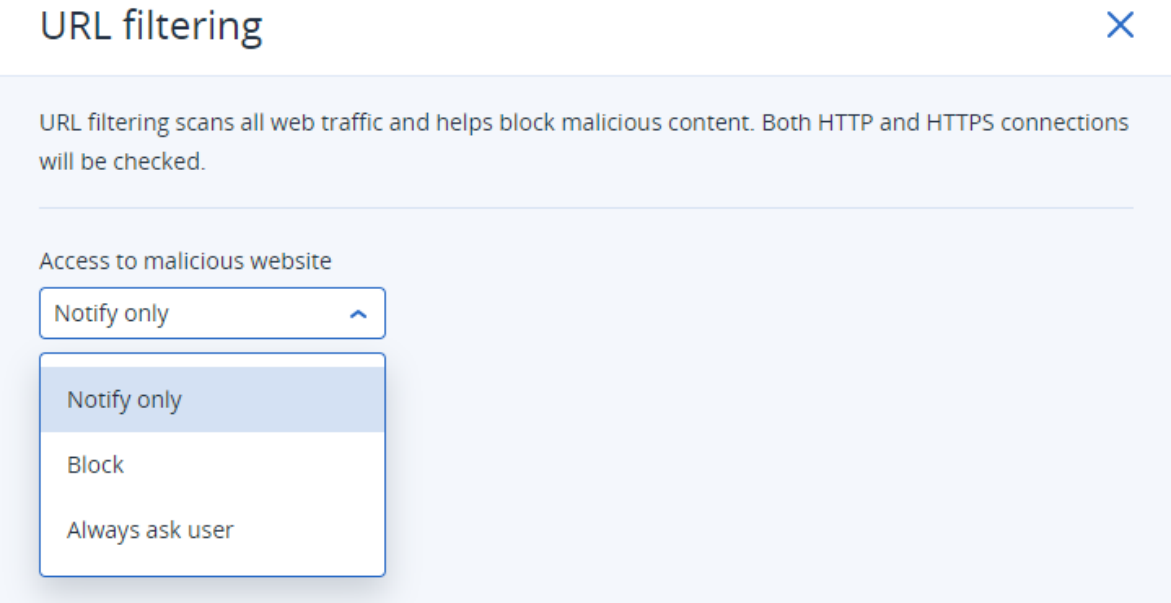
© Acronis International GmbH, 2003-2026

1. Dans le plan de protection pertinent, assurez-vous qu'EDR est activé. Pour plus d'informations, voir "Activation de la fonctionnalité EDR (Endpoint Detection and Response)" (p. 1255).
2. Développez le module **Protection antivirus et antimalware**, puis définissez ce qui suit :
   - Cliquez sur **Active Protection**, puis dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Active Protection" (p. 1170).



   - Cliquez sur **Moteur de comportement**, puis dans la section **Action lors de la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Moteur de comportement" (p. 1176).
   - Cliquez sur **Prévention des failles** et dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Ensuite, cliquez sur **Terminé**. Pour plus d'informations, voir "Prévention des failles" (p. 1176).
   - Cliquez sur **Protection en temps réel**, et dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Protection en temps réel" (p. 1178).
   - Cliquez sur **Planifier l'analyse**, et dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Planifier l'analyse" (p. 1179).
   - Cliquez sur **Application potentiellement indésirable** et, dans la section **Action sur la détection**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Application potentiellement indésirable" (p. 1187).
3. Développez le module **filtrage d'URL** et dans la liste déroulante **Accès à un site Web malveillant**, sélectionnez **Notifier uniquement**. Cliquez ensuite sur **Terminé**. Pour plus d'informations, voir "Filtrage d'URL" (p. 1197).

© Acronis International GmbH, 2003-2026



Test du fonctionnement de la fonctionnalité EDR (Endpoint Detection and Response)

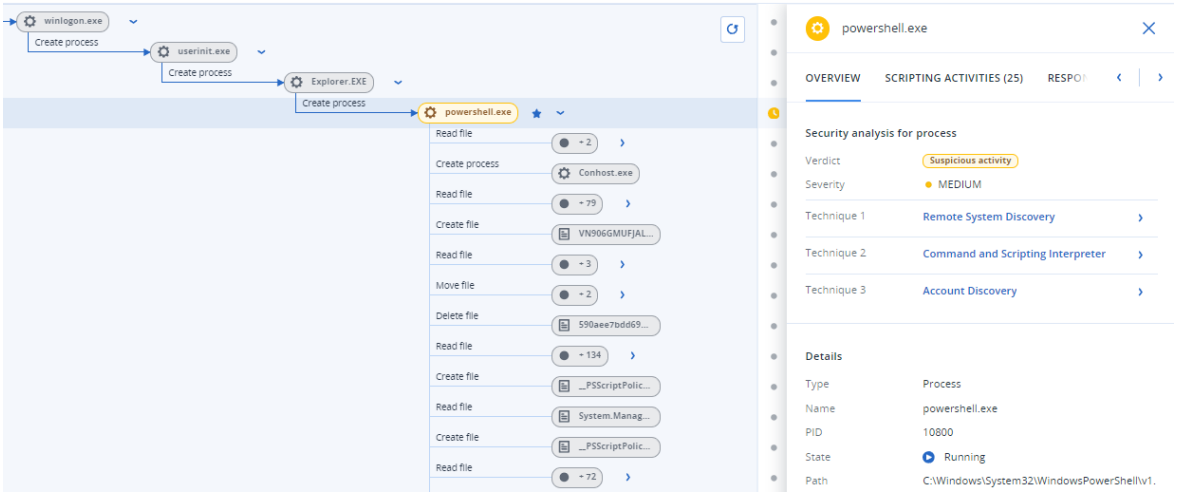
Pour vérifier si la fonctionnalité EDR est déployée et opérationnelle, vous pouvez exécuter un certain nombre de commandes qui déclenchent des détections EDR.

Remarque
Lorsque la fonctionnalité EDR est déployée, vous devriez constater des incidents immédiatement en cas d'activité suspecte. Les étapes ci-dessous vous permettent de vérifier si la fonctionnalité EDR est opérationnelle dans le cas où aucun nouvel incident n'a été déclenché pendant plusieurs jours.

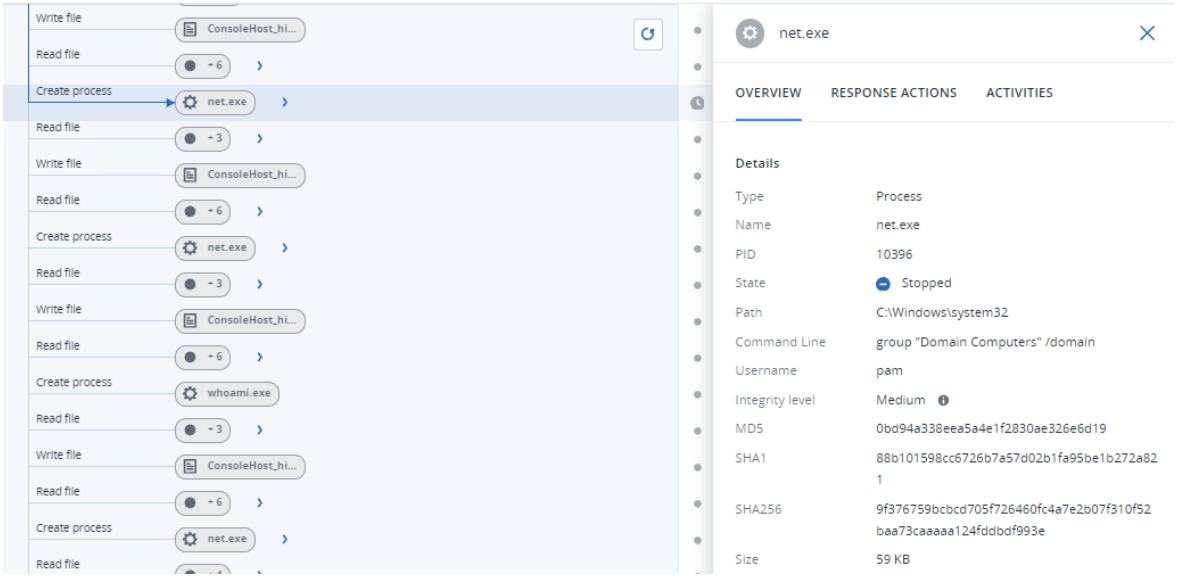
Pour tester si la fonctionnalité EDR est déployée et fonctionne correctement

1. Connectez-vous au compte utilisateur Active Directory associé au domaine pertinent.
2. Exécutez les deux commandes suivantes dans Windows PowerShell :
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Dans la console Cyber Protect, accédez à **Protection > Incidents** pour voir l'incident généré.
   Vous pouvez également cliquer sur l'incident déclenché dont la gravité est de type **Moyen** afin de l'afficher dans la cyber kill chain EDR et vérifier les commandes PowerShell que vous avez exécutées à l'étape précédente, comme l'indique l'exemple ci-dessous.

© Acronis International GmbH, 2003-2026



4. Exécutez les commandes suivantes dans Windows PowerShell :
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. Dans la cyber kill chain EDR, cliquez sur les nœuds d'exécutables (par exemple, **net.exe** ou **whoami.exe**) pour afficher les commandes PowerShell exactes qui sont exécutées dans la ligne de commande. Ces commandes sont affichées dans la section **Détails** de l'onglet **Vue d'ensemble** dans l'exemple ci-dessous.



6. Après avoir vérifié qu'un incident EDR a été généré, définissez manuellement l'option **Statut de la menace** de l'incident sur **Atténué** et l'option **État de l'enquête** sur **Fermé**. Pour plus d'informations, voir "Comment enquêter sur des incidents dans la cyber kill chain" (p. 1287). Vous pouvez également saisir un commentaire pour l'incident afin d'indiquer qu'il s'agissait d'un

© Acronis International GmbH, 2003-2026

incident test.

© Acronis International GmbH, 2003-2026

RMM

Le RMM est un ensemble de fonctionnalités offrant un niveau avancé de surveillance et de gestion pour les terminaux et les licences Microsoft 365. Vous pouvez en savoir plus, essayer ou demander une démonstration ici.

Pour vérifier les exigences logicielles de chaque fonctionnalité, consultez la section correspondante.

- Pour les terminaux, Acronis RMM offre les fonctionnalités suivantes :
  - **Inventaire du logiciel** : consultez la liste complète des logiciels utilisés par les clients, et gagnez du temps lors de la préparation, de la planification ou du suivi des mises à jour. Consultez "Gestion de votre inventaire de logiciels" (p. 1386).
  - **Déploiement de logiciels à l'aide de DeployPilot** – Déployer des logiciels à distance sur vos ressources gérées. Utilisez des plans de déploiement de logiciels pour automatiser le processus de déploiement et garantir une distribution uniforme des logiciels sur les ressources. Consultez "Gestion de logiciels" (p. 1385).
  - **Gestion automatisée des correctifs** - Résolvez les vulnérabilités avant qu'elles soient exploitées. Consultez "Gestion des correctifs" (p. 1401).
  - **Application de correctifs avec tolérance de pannes** - Restaurez les ressources rapidement et facilement à partir de correctifs défaillants en effectuant des sauvegardes système automatiques avant l'application des correctifs. Consultez "Paramètres de gestion des correctifs dans le plan de protection" (p. 1402).
  - **Surveillance et alertes intelligentes basées sur l'apprentissage automatique** - Limitez les risques opérationnels et optimisez la tâche de surveillance grâce à la surveillance prédictive et aux alertes. Consultez "Alertes de surveillance" (p. 1571).
  - **Création de cyberscripts prêts à l'emploi** - Automatisez et simplifiez les tâches de routine. Consultez "Création de cyber-scripts" (p. 489).
  - **Surveillance de l'intégrité des lecteurs** : utilisez la surveillance prédictive et les alertes, et limitez de manière proactive les interruptions d'activité provoquées par des défaillances de lecteur. Consultez "Surveillance de l'intégrité du disque" (p. 346).
  - **Bureau à distance et assistance à distance** - Accédez à des ressources distantes et résolvez rapidement les problèmes techniques. Gagnez du temps et fournissez un support fiable, avec d'excellentes performances, même avec une bande passante limitée. La fonctionnalité offre une meilleure couverture des plates-formes (Windows, macOS et Linux), ainsi que des fonctionnalités étendues pour les enregistrements de session, les actions distantes, les transferts de fichiers, la surveillance, le reporting et l'observation de ressources en vue multiple. Consultez "Connexion à des ressources de type Bureau ou assistance à distance" (p. 1459).
  - **Évaluation des vulnérabilités des applications Windows tierces** – Améliorez le niveau de sécurité des applications Windows tierces en détectant et en gérant les vulnérabilités de 314 applications critiques, prises en charge par une base de données gérée en interne par Acronis. Consultez "Solutions Microsoft et tiers prises en charge pour l'évaluation des vulnérabilités" (p. 1391).

© Acronis International GmbH, 2003-2026

  - **Suivi de la géolocalisation** - Affichez l'emplacement physique en temps réel de vos ressources gérées. Consultez "Suivi de la géolocalisation" (p. 1512).
  - **Chat d'assistance** - Utilisez l'outil de communication en temps réel entre les techniciens et les utilisateurs distants de ressources Windows et macOS gérées pour fournir une résolution des problèmes plus rapide et un meilleur service client. Consultez "Chat d'assistance" (p. 1515).
- Pour les postes Microsoft 365, Acronis RMM fournit un audit continu de la posture de sécurité Microsoft 365 avec des références de bonnes pratiques, une remédiation automatique des déviations de référence de posture de sécurité, ainsi que l'intégration et la sortie des utilisateurs.

Gestion et surveillance de l'environnement Microsoft 365

Important
Dans le cadre de la licence basée sur le service, cette fonctionnalité fait partie de l'offre payante RMM – postes Microsoft 365. La fonctionnalité inclut une surveillance continue de la posture de sécurité Microsoft 365 avec des références de bonnes pratiques, la remédiation des déviations de référence et des risques utilisateurs, ainsi que l'intégration et la sortie des utilisateurs. Si vous ne souhaitez pas utiliser le service de surveillance et de gestion de la sécurité Microsoft 365, contactez votre fournisseur de services pour désactiver l'intégration pour vous.

Dans le modèle de licence basé sur la solution, l'ensemble des fonctionnalités est inclus dans les licences Sécurité et RMM et Protection Ultime, dans le cadre de l'offre de postes Microsoft 365.

Des frais sont appliqués pour chaque utilisateur auquel une licence de boîte aux lettres Exchange Online est allouée.

Le service de surveillance et de gestion de la sécurité Microsoft 365 dans Cyber Protection vous permet d'effectuer les opérations suivantes :

- Intégration facile des tenants de clients Microsoft 365 à Cyber Protect Cloud.
- Vérification continue du niveau de sécurité des clients Microsoft 365.
- Surveillance des violations et les risques avec des modèles de référence de bonnes pratiques de Microsoft 365.
- Correction des écarts par rapport aux références (en un clic) et des erreurs de configuration des contrôles de sécurité.
- Surveillance et gestion des risques liés aux utilisateurs Microsoft 365.
- Intégration et exclusion d'utilisateurs Microsoft 365.

Configuration des connexions Microsoft 365

Remarque
Cette fonctionnalité est uniquement disponible pour les administrateurs partenaires.

© Acronis International GmbH, 2003-2026

Lorsque la surveillance et la gestion de la sécurité Microsoft 365 sont activées dans Cyber Protect, vous pouvez vous connecter aux clients Microsoft 365 associés à votre compte Microsoft (ou à celui de votre client).

Vous pouvez ensuite mapper les tenants Microsoft 365 aux clients pertinents dans Cyber Protect.

Connexion à un compte Microsoft

En tant qu'administrateur partenaire, vous pouvez vous connecter à votre compte Microsoft CSP ou à votre compte Microsoft classique.

Lorsque vous vous connectez à votre compte Microsoft CSP, le système récupère automatiquement tous les tenants clients associés à ce compte.

Lorsque vous vous connectez à un compte Microsoft classique, vous pouvez vous connecter aux comptes Microsoft de vos clients, l'un après l'autre, à condition de disposer des identifiants appropriés.

Important
Lorsque vous intégrez des tenants avec un grand nombre d'utilisateurs (par exemple, plus de 1 000), le système peut prendre un certain temps pour récupérer tous les détails pertinents. En effet, chaque utilisateur doit être vérifié, et certaines API Microsoft ne peuvent être déclenchées qu'une fois toutes les deux secondes. Ce problème concerne les comptes Microsoft CSP et les comptes classiques.

Pour se connecter à un compte Microsoft

Compte Microsoft CSP

1. Dans la console Cyber Protect, accédez à **Gestion M365** > **Configuration**.
2. Cliquez sur **Connecter un compte Microsoft**.
   Vous êtes redirigé vers la page de connexion Microsoft.
3. Connectez-vous au compte Microsoft avec vos identifiants CSP, puis acceptez les autorisations demandées par Acronis. Lorsque vous cliquez sur **Accepter**, vous êtes redirigé vers la console Cyber Protect.

   Remarque
   Les autorisations demandées lors de la connexion à un compte Microsoft sont celles de l'application d'entreprise **Octiga Multi-Tenant Security** enregistrée dans Entra ID. Cette application est connectée aux tenants Microsoft 365 des fournisseurs de services et leur permet de gérer les opérations de sécurité de leurs clients.

4. Dans l'onglet **Mappage de client** qui s'affiche, mappez les clients Microsoft 365 avec les clients pertinents dans Cyber Protect Cloud. Pour plus d'informations, voir "Mappage de client" (p. 1347).
   Le système répertorie automatiquement tous les tenants Microsoft 365 associés au compte Microsoft dans l'onglet **Mappage de client**, chacun avec le statut initial **Intégration du tenant**.

© Acronis International GmbH, 2003-2026

Compte Microsoft classique

1. Dans la console Cyber Protect, accédez à **Gestion M365 >Configuration**.
2. Cliquez sur **Connecter un compte Microsoft**.
   Vous êtes redirigé vers la page de connexion Microsoft.
3. Connectez-vous au compte Microsoft et acceptez les autorisations demandées par Acronis.
   Lorsque vous cliquez sur **Accepter**, vous êtes redirigé vers la console Cyber Protect.

   Remarque
   Les autorisations demandées concernent l'application d'entreprise **Octiga Multi-Tenant Security** enregistrée dans le compte Entra ID du tenant partenaire.

4. Cliquez sur **Ajouter le compte Microsoft du client**.
   Vous êtes invité à vous connecter avec les identifiants du compte client pertinent. Acceptez les autorisations demandées par Acronis. Lorsque vous cliquez sur **Accepter**, vous êtes à nouveau redirigé vers la console Cyber Protect.

   Remarque
   Les autorisations demandées concernent l'application d'entreprise **Octiga Cloud Security** enregistrée dans le compte Entra ID du tenant du client.

5. Dans l'onglet **Mappage de client** qui s'affiche, mappez les clients Microsoft 365 avec les clients pertinents dans Cyber Protect Cloud. Pour plus d'informations, voir "Mappage de client" (p. 1347).
6. [Facultatif] Pour répéter les étapes ci-dessus pour d'autres comptes Microsoft de clients, cliquez sur **Ajouter un compte Microsoft** dans l'onglet **Mappage de client**.

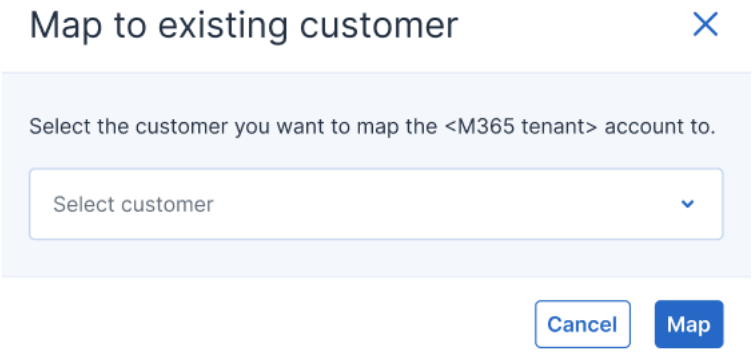
Mappage de client

Une fois l'intégration des tenants Microsoft 365 dans Cyber Protect Cloud terminée, vous pouvez mapper les tenants Microsoft 365 associés à ce compte aux clients dans Cyber Protect Cloud.

Pour associer des tenants Microsoft 365 à des clients

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Configuration**.
2. Dans l'onglet **Mappage de client**, sélectionnez le ou les tenants Microsoft 365 concernés, puis cliquez sur **Mapper au client existant**.
3. Sélectionnez le client pertinent dans la liste déroulante, puis cliquez sur **Associer**.

© Acronis International GmbH, 2003-2026



Lorsque le mappage du client réussit :

- Mapped s'affiche dans la colonne **État du mappage** dans l'onglet **Mappage de client**.
- Le système applique au tenant client les références de tenant prédéfinies. Pour plus d'informations, voir "Travail avec les références" (p. 1351).
- La surveillance du niveau de sécurité démarre et s'exécute pour le tenant client. Pour plus d'informations, voir "Examen du niveau de sécurité" (p. 1349).

Pour supprimer le mappage entre les clients et les tenants Microsoft 365

1. Dans l'onglet **Mappage de client** , sélectionnez le ou les tenants Microsoft 365 concernés, puis cliquez sur **Supprimer le mappage**.
2. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.
   Si vous êtes connecté à un compte Microsoft CSP, le mappage entre le tenant sélectionné et le client Cyber Protect Cloud est supprimé. Le tenant reste répertorié dans l'onglet **Mappage de client**, avec le statut **Non mappé**.
   Si vous êtes connecté à un compte Microsoft classique, le mappage entre le tenant sélectionné et le client Cyber Protect Cloud est supprimé, et l'application Acronis est également supprimée du répertoire **Inscriptions de l'application** dans le compte Microsoft Entra ID du client. Le tenant est supprimé de l'onglet **Mappage de client**.

Remarque
Lorsque le mappage est supprimé, le service de surveillance et de gestion de la sécurité Microsoft 365 est automatiquement désactivé pour le ou les clients sélectionnés.

Désactivation du service de gestion de Microsoft 365

Vous pouvez désactiver le service de gestion de Microsoft 365 pour les clients précédemment intégrés (voir "Connexion à un compte Microsoft" (p. 1346)) dans Cyber Protect Cloud.

Pour désactiver le service de gestion de Microsoft 365

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Configuration**.
2. Cliquez sur l'onglet **Paramètres**, puis sur **Désactiver le service**.
3. Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **Désactiver**.
   La désactivation du service supprimera :

© Acronis International GmbH, 2003-2026

- L'application Acronis connectée à partir du répertoire **Enregistrements d'applications** dans Microsoft Entra ID de votre tenant.
- Toutes les données relatives aux clients stockées dans Cyber Protect Cloud, y compris le mappage des clients aux tenants Microsoft 365.

Examen du niveau de sécurité

Les administrateurs partenaires peuvent examiner le niveau de sécurité de nombreux tenants Microsoft 365 dans un tableau de bord.

Pour accéder à la fonctionnalité de sécurité, accédez à **Gestion de Microsoft 365** > **Niveau de sécurité** .

L'écran **Niveau de sécurité** fournit une vue d'ensemble de la sécurité et affiche les données suivantes pour chaque tenant Microsoft 365 :

- Nom du tenant
- Références des tenants (le cas échéant, le nombre d'écarts par rapport à ces références est affiché)
- Utilisateurs (nombre)
- Boîtes aux lettres (nombre)

En haut de l'écran, vous pouvez voir des icônes qui indiquent les informations suivantes :

- Le nombre total de tenants Microsoft 365 avec des écarts par rapport aux références.
- Le nombre total d'écarts par rapport aux références dans les tenants affectés.

Remarque
Vous pouvez afficher des données de niveau de sécurité supplémentaires en cliquant sur la ligne du tenant pour afficher le tableau de bord Risque du tenant sélectionné. Pour plus d'informations, voir "Examen du tableau de bord Risque" (p. 1349).

Examen du tableau de bord Risque

Le tableau de bord Risque met en évidence les risques (ou écarts) par rapport aux références, catégories de références et comptes utilisateur d'un tenant Microsoft 365.

Vous pouvez accéder au tableau de bord Risque pour un tenant spécifique en cliquant sur la ligne du tenant pertinente dans l'écran Niveau de sécurité (voir "Examen du niveau de sécurité" (p. 1349)).

Pour afficher le tableau de bord Risque pour le ou les tenants Microsoft 365 mappés à un client spécifique, vous pouvez également sélectionner le client dans la liste déroulante **Tous les clients** (au-dessus du menu de navigation).

© Acronis International GmbH, 2003-2026

Baselines

Tenant baselines	3 passed	11 deviated

Baseline categories

Audit	1 passed	0 deviated
Authentication & Authorisation	0 passed	6 deviated
Email Security	0 passed	4 deviated
Remote Access	2 passed	0 deviated
Sharing	0 passed	1 deviated

User account risks

MFA	6 affected user accounts
Admin mailboxes	No affected user accounts
Anonymous admins	1 affected user account
Shared mailboxes	No affected user accounts
Dormant accounts	No affected user accounts
Dormant admins	No affected user accounts
Guests	18 affected user accounts

© Acronis International GmbH, 2003-2026

Le tableau de bord Risque inclut les informations suivantes :

- **Références**
  - Références des tenants (avec le nombre de références respectées et non respectées)
- **Catégories de référence**(chacune des catégories suivantes inclut le nombre de références respectées et non respectées)
  - Sécurité de la messagerie électronique
  - Authentification et autorisation
  - Partage
  - Audit
  - Accès à distance
- **Risques du compte utilisateur**
  - Authentification multifacteur (avec le nombre de comptes utilisateur affectés et pour lesquels l'authentificateur multifacteur est désactivée ou qui ne sont pas inscrits)
  - Boîtes aux lettres d'administrateur (avec le nombre de comptes utilisateur qui sont des comptes administrateur global avec une boîte aux lettres)
  - Administrateurs anonymes (avec le nombre de comptes utilisateur qui pourraient être des comptes administrateur partagés)
  - Boîtes aux lettres partagées (avec le nombre de comptes utilisateur qui ont des boîtes aux lettres partagées)
  - Comptes inactifs (avec le nombre de comptes utilisateur qui ne se sont pas connectés depuis trois mois)
  - Administrateurs inactifs (avec le nombre de comptes utilisateur qui sont des comptes administrateur, mais qui n'ont pas été utilisés depuis six mois)
  - Invités (avec le nombre de comptes utilisateur qui sont des comptes invités)

Travail avec les références

La gestion de Microsoft 365 vous permet de surveiller le statut de toutes les références de tenants appliquées.

Pour accéder à la fonctionnalité de références, accédez à **Gestion de Microsoft 365** > **Références**.

Surveillance des références des tenants

Vous pouvez surveiller les références de tous les tenants Microsoft 365 intégrés.

Pour surveiller les références de tenants

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Références**.
2. [Facultatif] Sélectionnez un tenant dans la liste déroulante **Tenant**. Vous pouvez également filtrer la liste selon le nom de la catégorie.
3. Dans la liste des références, vous pouvez effectuer les opérations suivantes :

© Acronis International GmbH, 2003-2026

- Consulter le statut de toutes les références (**respectées** ou **non respectées**) appliquées au tenant sélectionné.
- Vérifier si l'option de correction automatique est activée.
- Afficher plus de détails sur une référence. Cliquez sur la référence pertinente pour :
  - Voir la description de la référence. Pour plus d'informations sur chacune des références disponibles, voir "Références de tenant" (p. 1352).
  - Afficher les valeurs actuelles et requises de la configuration de référence.
  - Définissez la correction automatique de la référence. Cliquez sur **Activer la correction automatique** ou **Désactiver la correction automatique**, selon les besoins.
  - Remédiez à la déviation de la référence. Pour plus d'informations, voir "Correction manuelle des références des tenants" (p. 1366).

Références de tenant

Le tableau suivant répertorie les références de tenant Microsoft 365 actuellement prises en charge.

Catégorie	Référence	Description
Audit	Journal d'audit de la boîte aux lettres	Activer les journaux d'audit des boîtes aux lettres pour l'ensemble de l'organisation. Pour plus d'informations, voir la documentation Microsoft.
Audit	Journal d'audit unifié	Activer ou désactiver le journal d'audit pour l'ensemble de l'organisation. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Workflow de consentement de l'administrateur	Le workflow de consentement de l'administrateur dans Microsoft Entra ID permet aux utilisateurs de demander l'approbation pour les applis qui

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		nécessitent des autorisations de niveau administrateur. Lorsqu'il est activé, les utilisateurs peuvent soumettre des demandes, et les réviseurs désignés sont notifiés pour les approuver ou les refuser. Cela aide à contrôler l'accès aux données sensibles et garantit une gestion des autorisations sécurisée et traçable. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie de méthode d'authentification - OTP par e-mail	L'OTP par e-mail envoie un code au compte e-mail d'un utilisateur qui est ensuite utilisé pour l'authentification. Pour les membres d'un tenant, l'OTP par e-mail est utilisable uniquement pour la restauration de mot de passe en libre-service. Il peut également être configuré pour être utilisé pour l'ouverture de session par des utilisateurs invités. Pour plus d'informations, voir la documentation Microsoft.

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
Authentification et autorisation	Stratégie de méthode d'authentification - Microsoft Authenticator	L'appli Microsoft Authenticator est une méthode d'authentification phare, utilisable en modes sans mot de passe ou simple approbation par notification push. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – application des restrictions imposées pour les terminaux non gérés	Bloquer ou limiter l'accès au contenu SharePoint, OneDrive et Exchange à partir de terminaux non gérés. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – blocage de l'authentification héritée	Bloquer l'accès via des méthodes d'authentification héritées non sécurisées. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel - Bloquer l'accès aux terminaux inconnus ou non pris en charge	Les utilisateurs seront bloqués pour accéder aux ressources de l'entreprise lorsque le type de terminal est inconnu ou non pris en charge. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – application de l'authentification multifacteur (MFA)	Appliquer

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		l'authentification multifacteur. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – aucune session de navigateur persistante	Empêcher les sessions de navigateur persistantes. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – exiger des applis client approuvées	Exiger une application client approuvée ou une stratégie de protection des applications lors de l'utilisation de terminaux mobiles. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – exiger un terminal conforme ou hybride joint à Azure AD	Exiger des utilisateurs administrateurs qu'ils effectuent des actions à partir d'un terminal conforme ou hybride joint à Azure AD. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel - Restreindre l'accès au portail Azure	Exiger l'authentification multifactorielle pour la gestion Azure. Pour plus d'informations, voir la documentation

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel - Restreindre l'accès au portail d'administration Microsoft	Exiger l'authentification multifactorielle pour les administrateurs accédant aux portails d'administration Microsoft. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – sécurisation de l'inscription des informations de sécurité	Veiller à ce que tous les utilisateurs s'enregistrent de manière sécurisée pour l'authentification multifacteur (MFA) et la réinitialisation de mot de passe en libre-service (SSPR) via des terminaux conformes ou des conditions spécifiques lors de l'enregistrement. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie d'accès conditionnel – authentification multifacteur basée sur le risque de connexion	Protéger les utilisateurs lors de la connexion via l'authentification multifacteur dans les sessions à risque. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Customer Lockbox	Exiger des ingénieurs de support Microsoft

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		qu'ils obtiennent l'approbation du client avant d'accéder à ses données lors des cas de support. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Stratégie de mot de passe	Cette stratégie définit la durée de validité d'un mot de passe avant que l'utilisateur ne doive le changer, et combien de jours à l'avance l'utilisateur est informé de l'expiration à venir. Utilisez-la pour vous assurer que les identifiants utilisateur sont régulièrement renouvelés (ou définis pour ne jamais expirer, si approprié) en accord avec vos exigences de sécurité et opérationnelles. Pour plus d'informations, voir la documentation Microsoft.
Authentification et autorisation	Authentification moderne SharePoint appliquée	Appliquer l'utilisation de protocoles d'authentification modernes uniquement pour l'accès global à SharePoint en désactivant les protocoles d'authentification hérités. Pour plus

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		d'informations, voir la documentation Microsoft.
Authentification et autorisation	Paramètres de consentement des utilisateurs	Contrôlez quand les utilisateurs finaux et les propriétaires de groupe sont autorisés à accorder leur consentement aux applications, et quand ils devront demander un examen et une approbation de l'administrateur. Permettre aux utilisateurs d'accorder aux applis l'accès aux données les aide à acquérir des applications utiles et à être productifs, mais cela peut représenter un risque dans certaines situations si ce n'est pas surveillé et contrôlé avec soin.
Sécurité de la messagerie électronique	Transfert automatique – blocage	Règle de transport pour bloquer le transfert automatique. Pour plus d'informations, voir la documentation Microsoft.
Sécurité de la messagerie électronique	Stratégie par défaut du filtre anti-spam sortant hébergé	Une stratégie par défaut de filtre anti-spam sortant Exchange Online Protection (EOP) qui assure la surveillance et le blocage des e-

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		mails sortants suspects, aidant les MSP à détecter et à prévenir les comptes compromis d'envoyer du spam ou du contenu malveillant.
Sécurité de la messagerie électronique	Signature DKIM pour le domaine par défaut	Assurez-vous que la signature DomainKeys Identified Mail (DKIM) est activée pour le domaine par défaut.
Sécurité de la messagerie électronique	Transfert automatique des e-mails	Désactiver le transfert automatique vers des domaines externes par défaut pour l'ensemble de l'organisation (les attaquants ou les acteurs malveillants peuvent transférer automatiquement tous les e-mails vers une autre boîte aux lettres et enfreindre la conformité si le transfert automatique est effectué vers un domaine externe). Pour plus d'informations, voir la documentation Microsoft.
Sécurité de la messagerie électronique	Stratégie de filtrage des types de fichiers malware	Une stratégie qui bloque les types de fichiers malveillants connus ou personnalisés d'être attachés aux e-mails, aidant à prévenir les

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		infections par malware. Les administrateurs peuvent ajouter ou supprimer des extensions de fichiers spécifiques pour adapter la protection pour chaque tenant. Pour plus d'informations, voir la documentation Microsoft.
Sécurité de la messagerie électronique	Stratégie de notification de filtre d'expéditeur interne de malware	Une configuration au sein d'Exchange Online Protection (EOP) qui alerte les administrateurs lorsqu'un expéditeur interne est bloqué pour avoir tenté d'envoyer du malware, aidant les MSP à détecter et à répondre rapidement à une compromission potentielle de compte.
Sécurité de la messagerie électronique	Stratégie EOP prédéfinie (Standard)	Une stratégie Exchange Online Protection (EOP) gérée par Microsoft qui applique une référence standard en matière de sécurité des e-mails à l'échelle du tenant. Créée à partir d'un modèle dans la console d'administration Defender, cette stratégie est entièrement gérée et

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		maintenue par Microsoft une fois déployée.
Sécurité de la messagerie électronique	Stratégie EOP prédéfinie (Stricte)	Une stratégie prédéfinie stricte Exchange Online Protection est une stratégie prédéfinie créée à partir d'un modèle dans la console d'administration Office 365 Defender. Elles sont contrôlées par Microsoft une fois créées.
Sécurité de la messagerie électronique	Stratégie anti-phishing standard par défaut	Stratégie anti-phishing par défaut pour les boîtes aux lettres Exchange, couvrant également l'intelligence anti-usurpation d'identité. Pour plus d'informations, voir la documentation Microsoft.
Général	Stratégie de sécurité par défaut	Les paramètres de sécurité par défaut sont un ensemble de mécanismes de sécurité d'identité de base recommandés par Microsoft. Lorsqu'elles sont activées, ces recommandations seront automatiquement appliquées dans votre organisation. Les administrateurs et les utilisateurs

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		seront mieux protégés contre les attaques courantes liées à l'identité. **Remarque** Cela remplacera certains paramètres, tels que les stratégies d'accès conditionnel.
Intune	Android Enterprise - Stratégie de conformité	Stratégie de conformité pour les terminaux Android gérés. Pour plus d'informations, voir la documentation Microsoft.
Intune	iOS/iPadOS - Stratégie de conformité	Stratégie de conformité pour les terminaux iOS/iPadOS gérés. Pour plus d'informations, voir la documentation Microsoft.
Intune	MAC OS - Stratégie de conformité	Stratégie de conformité pour les terminaux macOS gérés. Pour plus d'informations, voir la documentation Microsoft.
Intune	Stratégie de conformité pour Windows 10 ou version ultérieure	Une stratégie de conformité qui impose des normes de sécurité pour les terminaux Windows 10 et versions ultérieures gérés via Intune. Elle valide le chiffrement, le démarrage sécurisé,

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		le statut de Defender, la version du système d'exploitation et l'intégrité du terminal pour s'assurer que les terminaux répondent aux exigences de sécurité organisationnelles et réglementaires dans tous les environnements clients. Pour plus d'informations, voir la documentation Microsoft.
Intune	Stratégie de configuration Windows 10 ou ultérieure - Bloquer l'enregistrement des mots de passe dans Google Chrome	Stratégie de configuration pour bloquer l'enregistrement des mots de passe dans Google Chrome.
Intune	Stratégie de configuration Windows 10 ou ultérieure - Blocage de l'enregistrement des mots de passe dans Microsoft Edge	Stratégie de configuration pour bloquer l'enregistrement des mots de passe dans Microsoft Edge.
Accès mobile	Stratégie par défaut de boîte aux lettres de terminal mobile	Définissez la stratégie par défaut de boîte aux lettres de terminal mobile pour gérer de nombreux paramètres de sécurité différents des boîtes aux lettres sur les terminaux mobiles
Accès à distance	Authentification moderne	Activer l'authentification moderne pour l'ensemble de

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		l'organisation. Pour plus d'informations, voir la documentation Microsoft.
Accès à distance	Accès SMTP	Désactiver l'accès SMTP pour l'ensemble de l'organisation. SMTP est considéré comme un ancien protocole de messagerie non sécurisé. Pour plus d'informations, voir la documentation Microsoft.
Partage	Expiration des liens anonymes	S'assurer que les liens anonymes expirent après un certain nombre de jours. Pour plus d'informations, voir la documentation Microsoft.
Partage	Partage de nouveau par des utilisateurs externes (invités)	Empêcher les utilisateurs invités qui ont un accès partagé à un élément (où l'élément a été partagé à l'aide du partage invité, et non via un lien anonyme) de partager à nouveau l'élément avec d'autres. Le paramètre Empêcher le partage par les utilisateurs externes garantit un accès limité aux éléments partagés. Pour plus d'informations, voir la documentation

© Acronis International GmbH, 2003-2026

Catégorie	Référence	Description
		Microsoft.
Partage	Stratégie de partage par défaut globale	Contrôlez le partage au niveau de l'organisation dans SharePoint et OneDrive.
Partage	Blocage du téléchargement des fichiers infectés sur SharePoint	Bloquer le téléchargement de fichiers infectés sur SharePoint. Pour plus d'informations, voir la documentation Microsoft.
Partage	Avertissement de stockage SharePoint	Utilisez cette référence pour définir un seuil d'avertissement pour les sites SharePoint approchant de la limite de stockage. Si l'un des sites dépasse le seuil de stockage défini par la référence, alors la référence déviera, ce qui déclenchera une alerte.

Modification des références des tenants

Vous pouvez modifier les références qui ne sont pas gérées par un modèle pour changer la configuration de la référence sur le tenant où la référence est appliquée.

Pour modifier une référence

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Références**.
2. Cliquez sur l'icône de crayon à la fin de la référence concernée.
   La boîte de dialogue de modification de la référence s'ouvre.
3. Appliquez les modifications nécessaires et cliquez sur **Enregistrer**.

Un contrôle de déviation commence pour évaluer si l'état de la référence est différent de l'état souhaité.

© Acronis International GmbH, 2003-2026

Remarque
Enregistrer la référence ne change pas la valeur dans Microsoft 365. Cela enregistre simplement une cible de configuration pour la référence.

Correction manuelle des références des tenants

Vous pouvez corriger les écarts dans les références de tenant en appliquant la configuration de référence requise dans le tenant.

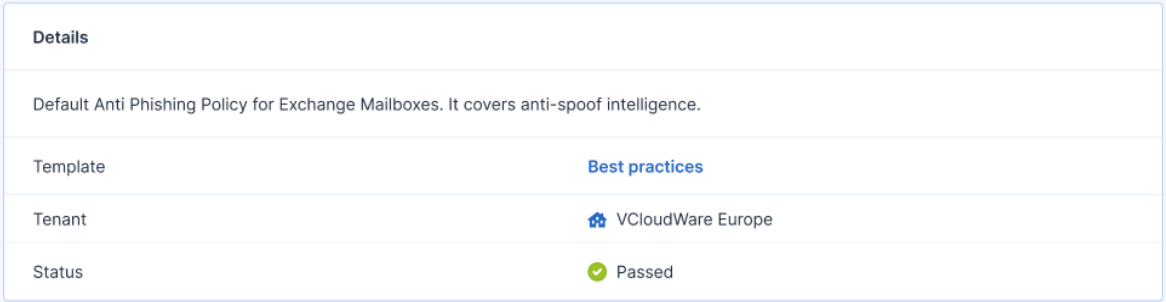
Remarque
Dans le cadre d'une licence basée sur le service, cette fonctionnalité nécessite que le quota de service **RMM** > **Postes Microsoft 365** soit appliqué à tous les sièges Microsoft 365 du client.

Dans le cadre d'une licence basée sur la solution, la fonctionnalité est activée avec soit la licence **Sécurité et RMM**, soit la licence **Protection Ultime**.

Important
L'option Correction automatique doit être activée pour que les écarts par rapport à la référence du tenant soient corrigés automatiquement. Toutefois, elle n'est pas requise pour la correction manuelle. Pour plus d'informations, voir "Activation ou désactivation de la correction automatique des écarts par rapport aux références" (p. 1367).

Pour corriger les écarts par rapport à la référence du tenant

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Références**.
2. Sélectionnez la ligne de tenant concernée.
   Le volet des détails de la référence s'affiche.
3. Cliquez sur **Réparer**.
   Le processus de correction démarre.
   Lorsque la correction est terminée, le statut de la référence change et indique **Réussi**, comme illustré ci-dessous.



© Acronis International GmbH, 2003-2026

Activation ou désactivation de la correction automatique des écarts par rapport aux références

Vous pouvez configurer la correction automatique des écarts par rapport aux références pour les tenants Microsoft 365 sélectionnés.

Remarque
Dans le cadre d'une licence basée sur le service, cette fonctionnalité nécessite que le quota de service **RMM** > **Postes Microsoft 365** soit appliqué à tous les sièges Microsoft 365 du client.

Dans le cadre d'une licence basée sur la solution, la fonctionnalité est activée avec soit la licence **Sécurité et RMM**, soit la licence **Protection Ultime**.

Pour activer ou désactiver la correction automatique des écarts par rapport aux références

1. Dans la console Cyber Protect, accédez à **Gestion M365** > **Références**.
2. Dans la liste déroulante **Tenant**, sélectionnez le tenant concerné.
   Vous pouvez également sélectionner le client pertinent dans la liste déroulante **Tous les clients** (au-dessus du menu de navigation).
3. Activez ou désactivez les options de correction automatique en fonction des besoins :
   - Cliquez sur **Activer la correction automatique** pour appliquer la correction automatique des écarts à toutes les références.
   - Cliquez sur **Désactiver la correction automatique** pour désactiver la correction automatique des écarts pour toutes les références.
4. [Facultatif] Cliquez sur une ligne de référence pour modifier son paramètre de correction automatique.
   Par exemple, vous pouvez activer la correction automatique pour toutes les références, mais la désactiver pour une ou plusieurs références spécifiques.

   Remarque
   Le système vérifie l'état de la ou des références trois fois par jour (toutes les huit heures) et corrige automatiquement tout écart (si la correction automatique est activée).

Suppression des références des tenants

Vous pouvez supprimer les références qui ne sont pas gérées par des modèles de référence.

Pour supprimer des références

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Références**.
2. Sélectionnez la case à cocher dans la ligne des références que vous souhaitez supprimer.

© Acronis International GmbH, 2003-2026

3. Cliquez sur **Supprimer** au-dessus de la liste.
4. Dans la boîte de dialogue **Supprimer des références**, cliquez sur **Confirmer**, puis sur **Fermer**.

   Les références qui ne sont pas gérées par des modèles sont supprimées. Les références qui font partie de modèles de référence ne seront pas supprimées.

Gestion des modèles de référence du tenant

Les modèles de référence vous permettent de créer un ensemble réutilisable de références. Ils sont particulièrement utiles lorsque vous travaillez avec plusieurs tenants, car un modèle peut être géré de manière centralisée et alloué aux tenants concernés, selon les besoins.

Modèles intégrés et personnalisés

Par défaut, le service fournit quelques modèles intégrés. Vous ne pouvez pas modifier ou supprimer ces modèles intégrés, mais vous pouvez les utiliser pour créer vos propres modèles personnalisés et gérer ces modèles personnalisés selon vos besoins. Un modèle personnalisé peut contenir n'importe quel mélange de références.

Remarque
Vous devez créer un modèle personnalisé si vous avez besoin de la gestion multitenant des références.

Le modèle par défaut

Par défaut, le modèle intégré Bonnes pratiques est défini comme modèle de référence par défaut. Le modèle par défaut est utilisé lors de l'intégration de nouveaux tenants. Un administrateur partenaire peut modifier le modèle par défaut selon les besoins.

Avec la gestion de Microsoft 365, vous pouvez gérer les modèles de référence de votre organisation Microsoft 365 comme suit :

- Créer des modèles de référence
- Supprimer des modèles de référence
- Spécifier un modèle de référence par défaut
- Ajouter des références dans les modèles
- Importer des références dans les modèles
- Configurer les paramètres de la référence
- Supprimer des références les modèles
- Déployer des modèles de référence
- Révoquer des modèles de référence

Pour accéder aux modèles de référence, allez à **Gestion de Microsoft 365** > **Modèles de référence**.

© Acronis International GmbH, 2003-2026

Révision des modèles de référence

En utilisant le service de surveillance et de gestion de la sécurité Microsoft 365, vous pouvez examiner les détails de tous les modèles de référence actuels du tenant, y compris les tenants attachés à chaque modèle. Vous pouvez également activer la remédiation automatique pour les références sélectionnées.

Pour examiner les modèles de référence

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Cliquez sur un modèle dans la liste pour ouvrir ses détails.
   - Dans l'onglet **Détails**, vous pouvez modifier le nom du modèle et vérifier si le modèle est défini par défaut.
   - Dans l'onglet **Références**, vous pouvez voir les détails des références dans le modèle, y compris si une référence nécessite une saisie utilisateur, et tous les plans de service Microsoft associés.

     Remarque
     La saisie utilisateur indique que certaines valeurs pour la référence doivent être définies par l'utilisateur avant d'appliquer le modèle au tenant.

     Certaines références nécessitent également des plans de service Microsoft spécifiques pour être appliquées, tels que AAD_PREMIUM et AAD_PREMIUM_P2. Si un tenant n'a pas ces plans, la référence est omise pour ce tenant.

     Pour activer la remédiation automatique pour une référence, sélectionnez la référence dans la liste, puis cliquez sur **Activer la remédiation automatique**.
   - Dans l'onglet **Clients**, visualisez les clients auxquels un modèle de référence est appliqué et révoquez le modèle pour des clients spécifiques.

Définir un modèle de référence par défaut

Le modèle par défaut est utilisé lors de l'intégration de nouveaux tenants. Initialement, le modèle intégré Bonnes pratiques est défini par défaut. En tant qu'administrateur partenaire, vous pouvez modifier le modèle par défaut selon les besoins, ou retirer le drapeau par défaut d'un modèle.

Remarque
Un seul modèle peut être défini par défaut pour tous les clients sous le service de gestion de la posture de sécurité Microsoft 365.

Pour définir un modèle de référence par défaut

Rôle requis : administrateur partenaire.

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cochez la case à cocher de celui que vous souhaitez définir par défaut.
3. Cliquez sur **Définir par défaut** au-dessus de la liste.

La colonne **Modèle par défaut** indique le modèle par défaut avec **Oui**.

Pour retirer le drapeau par défaut d'un modèle de référence

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, sélectionnez la case à cocher de la référence par défaut.
3. Cliquez sur **Effacer la valeur par défaut** au-dessus de la liste.

Créer et modifier des modèles de référence

Vous devez créer un modèle personnalisé si vous avez besoin de la gestion multitenant des références, mais les modèles sont également utiles dans les environnements de tenant unique, en tant qu'ensembles de références réutilisables.

Le processus allant de la création à l'utilisation réelle d'un modèle de référence personnalisé comprend plusieurs étapes :

1. Créer un modèle de référence.
   À cette étape, vous créez un conteneur pour les références.
2. Remplissez le modèle avec des références.
   À cette étape, vous pouvez ajouter des références à partir de la bibliothèque de références.
3. [Facultatif] Configurer les paramètres de certaines références dans le modèle.
4. Déployer le modèle de référence.

Pour créer un modèle de référence

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Au-dessus de la liste des modèles de référence, cliquez sur **Créer un modèle**.
3. Dans la boîte de dialogue **Créer un modèle de référence**, entrez un nom pour le modèle, puis cliquez sur **Créer**.

Le nouveau modèle de référence vide apparaît dans la liste. Vous devez maintenant l'éditer pour ajouter des références. Voir "Ajouter des références aux modèles" (p. 1371).

Modifier un modèle de référence

Rôle requis : administrateur partenaire.

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur celui que vous souhaitez modifier.
   Les détails du modèle apparaissent à droite.
3. Cliquez sur les onglets pour afficher ou éditer les propriétés dont vous avez besoin.
   - **Détails** - nom du modèle et statut par défaut du modèle.
   - **Références** - références dans le modèle.
   - **Clients** - clients auxquels le modèle est déployé.

Ajouter des références aux modèles

Dans un modèle de référence, vous pouvez ajouter des références à partir de la bibliothèque de références.

Pour ajouter des références à un modèle

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur celui auquel vous souhaitez ajouter une référence.
   Les détails du modèle apparaissent à droite.
3. Cliquez sur **Ajouter des références**.
4. Dans la boîte de dialogue **Ajouter des références**, sélectionnez les références que vous souhaitez ajouter et cliquez sur **Ajouter**.
   Vous pouvez rechercher des noms de référence ou filtrer les références par catégorie.
5. Dans la boîte de dialogue **Confirmer le changement de modèle**, examinez les modifications que vous avez appliquées et cliquez sur **Confirmer**.

Importer des références dans des modèles

Dans un modèle de référence, vous pouvez importer des références déjà gérées par un autre modèle. Si vous souhaitez ajouter des références qui ne sont pas gérées par un autre modèle, voir "Ajouter des références aux modèles" (p. 1371).

Importer des références dans un modèle

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur celui auquel vous souhaitez ajouter une référence.
   Les détails du modèle apparaissent à droite.
3. Cliquez sur **Importer des références**.

© Acronis International GmbH, 2003-2026

4. Dans la boîte de dialogue **Ajouter des références**, sélectionnez le nom du modèle qui contient les références que vous souhaitez importer.
5. Sélectionnez les références que vous souhaitez importer, puis cliquez sur **Importer**.
   Vous pouvez rechercher dans la liste par nom de référence ou catégorie.
6. Dans la boîte de dialogue **Confirmer le changement de modèle**, examinez les modifications que vous avez appliquées et cliquez sur **Confirmer**.

Édition des références dans les modèles

Vous pouvez éditer les références qui sont gérées par des modèles personnalisés pour modifier leurs paramètres selon les besoins.

Pour éditer une référence dans un modèle

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur celui qui contient la référence à modifier.
   Les détails du modèle apparaissent à droite, et la liste des références est affichée dans l'onglet **Références**.
3. Cliquez sur le menu contextuel à l'extrémité de la ligne de la référence et sélectionnez **Modifier**.
   La boîte de dialogue **Modifier la référence** s'ouvre.
4. Appliquez les modifications nécessaires et cliquez sur **Enregistrer** en haut à droite.

Suppression des références d'un modèle

Vous pouvez supprimer des références des modèles de référence personnalisés.

Pour supprimer une référence d'un modèle

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur celui qui contient la référence à supprimer.
   Les détails du modèle apparaissent à droite, et la liste des références est affichée dans l'onglet **Références**.
3. Cliquez sur le menu contextuel à l'extrémité de la ligne de la référence et sélectionnez **Supprimer**.
   La boîte de dialogue **Supprimer la référence** s'ouvre.
4. Cliquez sur **Supprimer** pour confirmer.

Exporter des bases de référence vers un fichier CSV

Vous pouvez exporter des bases de référence vers un fichier CSV à des fins de reporting.

Pour exporter des bases de référence vers un fichier CSV

Rôles requis : Administrateur partenaire ; Administrateur client

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Références**.
2. Dans la liste des références, cochez les cases à cocher des références que vous souhaitez exporter, puis cliquez sur **Exporter un fichier CSV** au-dessus de la liste.
3. Dans la boîte de dialogue **Exporter les références**, sélectionnez si vous souhaitez exporter tous les champs ou uniquement les champs avec des valeurs déviantes, puis cliquez sur **Exporter**.

Le fichier CSV se télécharge à l'emplacement de téléchargement par défaut configuré dans votre navigateur.

Déploiement des modèles de référence

Déployer un modèle déploie automatiquement et analyse toutes les références constituantes au client sur lequel le modèle est déployé. Cela écrasera toutes les références existantes du même type.

Remarque
Dans le cadre d'une licence basée sur le service, cette fonctionnalité nécessite que le quota de service **RMM** > **Postes Microsoft 365** soit appliqué à tous les sièges Microsoft 365 du client.

Dans le cadre d'une licence basée sur la solution, la fonctionnalité est activée avec soit la licence **Sécurité et RMM**, soit la licence **Protection Ultime**.

Déployer un modèle de référence

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur le modèle que vous souhaitez déployer. Les détails du modèle apparaissent à droite.
3. Cliquez sur **Déployer le modèle**.
4. Dans la boîte de dialogue **Déployer le modèle**, sélectionnez un client pour déployer le modèle.
5. [Si un autre modèle est déjà déployé chez le client] Parce qu'un client ne peut être géré que par un seul modèle à la fois, sélectionnez ce qu'il faut faire avec les paramètres du modèle actuel :
   - **Remplacer les références du modèle actuel**
     Les références du modèle actuel seront supprimées, et les références du nouveau modèle seront appliquées.
   - **Conserver les références du modèle actuel**
     Conservez les références du modèle actuel mais arrêtez de les gérer avec ce modèle. Le nouveau modèle sera appliqué et toutes les références chevauchantes seront remplacées par les références du modèle nouvellement déployé.
6. Cliquez sur **Déployer**.

© Acronis International GmbH, 2003-2026

Remarque
Déployer une référence n'est pas la même opération que remédier à une référence. Aucun changement ne sera apporté au client tant que vous ne choisissez pas de remédier.

Révocation des modèles de référence

Vous pouvez révoquer un modèle d'un ou plusieurs clients sur lesquels il est déployé.

Pour révoquer un modèle auprès d'un client

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, cliquez sur celui que vous souhaitez révoquer.
   Les détails du modèle apparaissent à droite.
3. Cliquez sur l'onglet **Clients**.
4. Dans la liste des clients, cliquez sur la poubelle pour révoquer le modèle du client correspondant.
5. Cliquez sur **Confirmer**.

Suppression des modèles de référence

Vous pouvez supprimer des modèles de référence si vous n'en avez plus besoin. Comme les modèles ne sont que des conteneurs pour les références, les références ne seront pas affectées et vous pouvez continuer à les utiliser selon vos besoins.

Pour supprimer un modèle de référence

Rôle requis : administrateur partenaire.

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Modèles de référence**.
2. Dans la liste des modèles de référence, sélectionnez la case à cocher du modèle que vous souhaitez supprimer.
3. Cliquez sur **Supprimer le modèle** au-dessus de la liste.
4. [Si le modèle est déployé aux clients] Dans la boîte de dialogue **Supprimer le modèle**, examinez la liste des clients affectés et décidez comment gérer les références qui sont gérées par le modèle :
   - **Conserver les références comme ne plus gérées**
     Si vous sélectionnez cette option, les références resteront affectées aux clients mais ne seront plus gérées par le modèle.
   - **Supprimer les références des clients ci-dessus**
     Les références seront retirées des clients, mais ne seront pas supprimées, vous pourrez donc les utiliser plus tard selon vos besoins.
5. Cliquez sur **Confirmer**.

© Acronis International GmbH, 2003-2026

Gestion des utilisateurs Microsoft 365

En tant qu'administrateur partenaire, vous pouvez parcourir et gérer la liste des utilisateurs du tenant Microsoft 365.

Pour parcourir la liste des utilisateurs intégrés dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Utilisateurs**. Vous pouvez filtrer la liste selon le tenant, le risque utilisateur, le type d'utilisateur, le rôle de l'utilisateur et la licence de produit.

Remarque
Après l'intégration du tenant du client, la liste des utilisateurs du tenant Microsoft 365 prendra généralement quelques minutes pour être importée depuis Microsoft 365.

Dans l'écran Utilisateurs, vous pouvez procéder à l'intégration de nouveaux utilisateurs (voir "Intégration d'utilisateurs" (p. 1375)).

Pour effectuer des actions spécifiques sur un seul utilisateur, cliquez sur la ligne de l'utilisateur concerné. Vous pouvez alors :

- Réinitialiser son mot de passe (voir "Réinitialisation des mots de passe des utilisateurs" (p. 1378)).
- Corrigez les risques liés à l'utilisateur (voir "Correction des risques liés aux utilisateurs" (p. 1376)).
- Excluez l'utilisateur (voir "Exclusion d'utilisateurs" (p. 1379)).

Remarque
Vous pouvez actuellement modifier les détails de l'utilisateur et gérer les applications et licences uniquement dans Microsoft 365. Pour plus d'informations, consultez la documentation Microsoft.

Intégration d'utilisateurs

Vous pouvez intégrer de nouveaux utilisateurs à un tenant Microsoft 365 via le service de gestion de Microsoft 365.

Pour intégrer un nouvel utilisateur

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Utilisateurs**.
2. Cliquez sur **Intégrer un utilisateur** .
3. Dans la boîte de dialogue, définissez les détails de l'utilisateur suivants :
   - [Facultatif] **Prénom** : prénom de l'utilisateur.
   - [Facultatif] **Nom** : nom de famille de l'utilisateur.
   - **Nom affiché** : nom visible par les destinataires des e-mails.
   - **Nom d'utilisateur** : nom d'utilisateur lors de la connexion.
   - [Facultatif] **Domaine** : sélectionnez le domaine Microsoft 365 pertinent dans la liste déroulante.
   - **Emplacement** : sélectionnez le pays pertinent dans la liste déroulante.

© Acronis International GmbH, 2003-2026

- **Mot de passe** : saisissez le mot de passe requis pour vous connecter.
- [Facultatif] Dans la section **Informations de contact**, entrez les informations pertinentes.

4. [Facultatif] Cochez la case **Demander à l'utilisateur de changer de mot de passe à la première connexion** si vous souhaitez que les utilisateurs changent de mot de passe lors de leur première connexion.
5. Cliquez sur **Créer**.

Correction des risques liés aux utilisateurs

Vous pouvez corriger un certain nombre de risques de sécurité liés au compte Microsoft 365 d'un utilisateur spécifique. Notez que vous ne pouvez corriger qu'un risque utilisateur à la fois.

Les risques que vous pouvez corriger sont notamment les suivants :

- Comptes administrateur avec boîte aux lettres : supprimez les privilèges d'administrateur des comptes pour lesquels la boîte aux lettres est requise, puis créez un nouveau compte administrateur distinct pour l'utilisateur.
- Comptes inactifs d'invités, d'utilisateurs et d'administrateurs : identifiez les anciens employés ou les autres comptes inutilisés, puis supprimez les comptes administrateur et les autres comptes qui ne sont plus nécessaires.
- Comptes avec l'authentification multifacteur désactivée ou non inscrits : évaluez les comptes utilisateur qui sont à risque en fonction des références et des paramètres requis de l'authentification multifacteur.
- Comptes administrateur anonymes : déterminez si les utilisateurs qui requièrent des privilèges d'administrateur doivent se voir attribuer un compte administrateur distinct (sans boîte aux lettres).
- Comptes avec boîtes aux lettres partagées mal configurées : identifiez les utilisateurs concernés qui ont besoin de l'option Envoyer en tant que ou qui doivent bénéficier d'un Accès total au compte partagé.

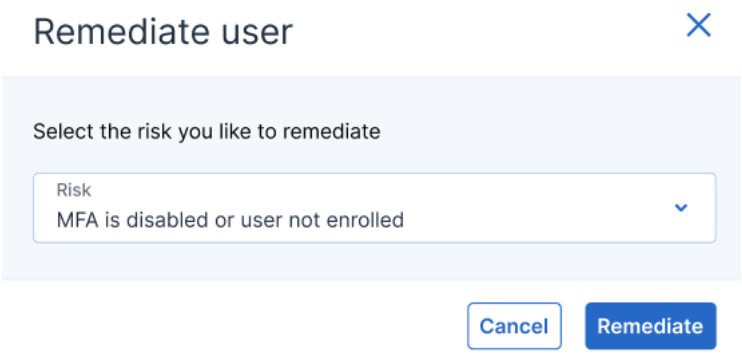
Remarque
Dans le cadre d'une licence basée sur le service, cette fonctionnalité nécessite que le quota de service **RMM** > **Postes Microsoft 365** soit appliqué à tous les sièges Microsoft 365 du client.

Dans le cadre d'une licence basée sur la solution, la fonctionnalité est activée avec soit la licence **Sécurité et RMM**, soit la licence **Protection Ultime**.

Pour corriger les risques liés aux utilisateurs

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Utilisateurs**.
2. Cochez la case dans la ligne de l'utilisateur concerné, puis cliquez sur **Corriger l'utilisateur**.
3. Dans la liste déroulante **Risque**, sélectionnez le risque à corriger, puis cliquez sur **Réparer**.

© Acronis International GmbH, 2003-2026



Le tableau suivant répertorie les risques et les étapes de correction qui sont appliquées lorsque vous cliquez sur **Réparer**.

Risque	Étapes de correction
L'authentification multifacteur est désactivée ou l'utilisateur n'est pas inscrit	L'authentification multifacteur est activée pour l'utilisateur.
Comptes inactifs	Interdit toute nouvelle connexion pour le compte utilisateur ou administrateur inactif sélectionné. Si l'utilisateur ou l'administrateur est connecté, il est automatiquement déconnecté de tous les services Microsoft dans un délai de 60 minutes.
Administrateurs inactifs	
Boîtes aux lettres d'administrateur	Supprime les privilèges d'administrateur du compte sélectionné et crée un nouveau compte administrateur distinct (sans licence) pour l'utilisateur. Le système génère

© Acronis International GmbH, 2003-2026

Risque	Étapes de correction
	également automatiquement un fichier CSV qui répertorie les comptes administrateur créés et leurs mots de passe à usage unique.
Administrateurs anonymes	Supprime le compte administrateur anonyme.
Boîtes aux lettres partagées	Convertit le compte utilisateur en boîte aux lettres partagée. Vous pouvez ensuite déléguer les options Envoyer en tant que ou Accès total aux utilisateurs concernés.
Invités	Supprime le compte utilisateur invité inactif.

4. Dans la boîte de dialogue de confirmation, cliquez sur **Confirmer**, puis sur **Fermer**.

Réinitialisation des mots de passe des utilisateurs

Vous pouvez réinitialiser le mot de passe Microsoft 365 d'un utilisateur spécifique.

Pour réinitialiser le mot de passe Microsoft 365 d'un utilisateur

1. Dans l'écran principal Utilisateurs, cliquez sur la ligne de l'utilisateur concerné.
2. Cliquez sur **Réinitialiser le mot de passe**.
3. Dans la boîte de dialogue affichée, entrez le nouveau mot de passe de l'utilisateur.
4. Si vous souhaitez obliger l'utilisateur à changer de mot de passe, sélectionnez **Exiger que cet utilisateur change de mot de passe à la première connexion**.
5. Cliquez sur **Enregistrer**.
6. Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **Fermer**.

© Acronis International GmbH, 2003-2026

Exclusion d'utilisateurs

Vous pouvez exclure des utilisateurs d'un tenant Microsoft 365 via le service de gestion de Microsoft 365.

Remarque
Dans le cadre d'une licence basée sur le service, cette fonctionnalité nécessite que le quota de service **RMM** > **Postes Microsoft 365** soit appliqué à tous les sièges Microsoft 365 du client.

Dans le cadre d'une licence basée sur la solution, la fonctionnalité est activée avec soit la licence **Sécurité et RMM**, soit la licence **Protection Ultime**.

Pour exclure des utilisateurs

1. Dans la console Cyber Protect, accédez à **Gestion de Microsoft 365** > **Utilisateurs**.
2. Cochez la case dans la colonne à l'extrême gauche de l'utilisateur que vous souhaitez exclure, puis cliquez sur **Exclure l'utilisateur**.
3. Modifiez les paramètres Microsoft 365 de l'utilisateur dans les sections suivantes, si nécessaire :
   - **Configurations de l'utilisateur**
   - **Attribuer des délégués de boîte aux lettres**
   - **Mesure d'intervention automatique**
   - **Blocage pour cause de litige**
4. Cliquez sur **Enregistrer**.
5. Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **Fermer**.
   L'utilisateur est exclu du tenant Microsoft 365 concerné.

Gestion de votre inventaire matériel

Lorsque vous activez la fonctionnalité d'inventaire matériel, vous pouvez afficher tous les composants matériels disponibles sur :

- les terminaux Windows ou macOS physiques qui possèdent une licence prenant en charge la fonctionnalité « Inventaire du matériel ».
- les machines Windows et macOS fonctionnant sur les plates-formes de virtualisation suivantes : VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo et Virtuozzo Hybrid Infrastructure.
  Pour en savoir plus sur les versions des plates-formes de virtualisation prises en charge, consultez "Plates-formes de virtualisation prises en charge" (p. 526).

  Remarque
  La fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.

© Acronis International GmbH, 2003-2026

La fonctionnalité d'inventaire du matériel n'est prise en charge que pour les terminaux sur lesquels un agent de protection est installé.

Pour obtenir les données d'inventaire du matériel, vous pouvez exécuter des analyses automatiques ou manuelles sur le terminal.

Vous pouvez utiliser les données d'inventaire du matériel pour :

- Découvrez toutes les ressources matérielles de l'organisation.
- Parcourez l'inventaire du matériel de tous les terminaux de votre organisation.
- Comparer les composants matériels sur plusieurs terminaux.
- Affichez les informations détaillées concernant un composant matériel.

Activation ou désactivation de l'analyse de l'inventaire matériel

Lorsque l'analyse de l'inventaire du matériel est activée sur les terminaux physiques et les machines virtuelles, le système collecte automatiquement les données du matériel toutes les 12 heures.

La fonctionnalité d'analyse de l'inventaire du matériel est activée par défaut, mais vous pouvez modifier le paramètre si nécessaire.

Remarque
Les tenants du client peuvent activer ou désactiver l'analyse de l'inventaire du matériel. Les tenants d'unités peuvent consulter les paramètres d'analyse de l'inventaire du matériel, mais ils ne peuvent pas les modifier.

Activer

Pour activer l'analyse de l'inventaire du matériel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Gestion**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Activez le module **Analyse de l'inventaire du matériel** en cliquant sur le commutateur à côté du nom du module.

Désactiver

Pour désactiver l'analyse de l'inventaire du matériel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Gestion**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Désactivez le module **Analyse de l'inventaire du matériel** en cliquant sur le commutateur à côté du nom du module.

© Acronis International GmbH, 2003-2026

Démarrage manuel d'une analyse de l'inventaire matériel

Vous pouvez démarrer manuellement une analyse de l'inventaire matériel pour un terminal unique et afficher les données actuelles des composants matériels du terminal.

Remarque
L'analyse de l'inventaire du matériel des machines virtuelles n'est prise en charge que lorsque la date et l'heure actuelles de la machine virtuelle correspondent à la date et l'heure actuelle en UTC. Afin de vérifier que la machine virtuelle utilise les paramètres de date et d'heure corrects, désactivez l'option **Synchronisation date/heure** de la machine virtuelle, définissez la date, l'heure et le fuseau horaire actuels, puis redémarrez **Acronis Agent Core Service** et **Acronis Managed Machine Service**.

Prérequis

- Le terminal utilise un système d'exploitation Windows ou macOS.
- Les terminaux possèdent une licence qui prend en charge la fonctionnalité Inventaire du matériel.

  Remarque
  Notez que la fonctionnalité Inventaire du matériel pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.

- Un agent de protection est installé sur le terminal.
- [Si le terminal est une machine virtuelle] La machine utilise l'une des plates-formes de virtualisation prises en charge. Pour plus d'informations, voir "Gestion de votre inventaire matériel" (p. 1379).

Pour démarrer une analyse de l'inventaire matériel sur un terminal unique

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Cliquez sur le terminal que vous souhaitez analyser, puis cliquez sur **Inventaire**.
3. Dans l'onglet **Matériel**, cliquez sur **Analyser maintenant**.

Navigation dans l'inventaire du matériel

Vous pouvez afficher et parcourir les données de tous les composants matériels disponibles sur tous les terminaux de votre organisation.

Prérequis

- Les terminaux utilisent le système d'exploitation Windows ou macOS.
- Les terminaux possèdent une licence qui prend en charge la fonctionnalité Inventaire du matériel.

© Acronis International GmbH, 2003-2026

Remarque
La fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.

- Un agent de protection est installé sur le terminal.
- L'analyse de l'inventaire du matériel sur les terminaux s'est déroulée correctement.
- [Si le terminal est une machine virtuelle] La machine utilise l'une des plates-formes de virtualisation prises en charge. Pour plus d'informations, voir "Gestion de votre inventaire matériel" (p. 1379).

Pour afficher tous les composants matériels disponibles sur les terminaux Windows et macOS

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Dans le champ à liste déroulante **Affichage :**, sélectionnez **Matériel**.

Remarque
La vue est un ensemble de colonnes qui détermine les données visibles à l'écran. Les vues prédéfinies sont **Standard** et **Matériel**. Vous pouvez créer et enregistrer des vues personnalisées qui incluent différents ensembles de colonnes, plus adaptés à vos besoins.

Le tableau suivant décrit les données visibles dans la vue **Matériel**.

Colonne	Description
Nom	Nom du terminal.
État de l'analyse du matériel	Statut de l'analyse du matériel. • **Terminée**. • **Non démarrée**. • **Non pris en charge**. Ce statut est affiché pour les ressources pour lesquelles la fonctionnalité d'inventaire matériel n'est pas prise en charge. Par exemple, les machines virtuelles, les terminaux mobiles et les terminaux Linux. • **Mise à jour de l'agent**. Ce statut est affiché lorsqu'une version obsolète de l'agent est installée sur le terminal. En cliquant sur cette action, vous serez redirigé vers la page **Paramètres** > **Agents**, où les administrateurs peuvent mettre à jour l'agent. • **Licence de mise à niveau**. En cliquant sur ce statut, une boîte de dialogue s'ouvre où les administrateurs peuvent changer la licence actuelle pour une autre licences disponibles pour le tenant.

© Acronis International GmbH, 2003-2026

Colonne	Description
Processeur	Modèles de tous les processeurs du terminal.
Cœurs de processeur	Nombre de cœurs de tous les processeurs du terminal.
Espace de stockage disque	Stockage utilisé et stockage total de tous les disques du terminal.
Mémoire	Capacité totale de la mémoire RAM du terminal.
Date de l'analyse	Date et heure de la dernière analyse de l'inventaire du matériel.
Carte mère	Carte mère du terminal.
Numéro de série de la carte mère	Numéro de série de la carte mère.
Numéro de série	Numéro de série du système du terminal.
Version du BIOS	Version du BIOS du système.
Organisation	Organisation à laquelle appartient le terminal.
Propriétaire	Propriétaire du terminal.
Domaine	Domaine du terminal.
Système d'exploitation	Système d'exploitation du terminal.
Version du système d'exploitation	Version du système d'exploitation du terminal.

3. [Facultatif] Pour ajouter des colonnes au tableau, cliquez sur l'icône en forme d'engrenage, puis sélectionnez les colonnes qui doivent être visibles dans le tableau.
4. [Facultatif] Pour réduire la quantité d'informations affichées, utilisez un ou plusieurs filtres.
   a. Cliquez sur **Rechercher**.
   b. Cliquez sur la flèche, puis sur **Matériel**.
   c. Sélectionnez un ou plusieurs filtres.
   Le tableau suivant décrit les filtres **Matériel**.

Filtre	Description
Modèle de processeur	Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant du modèle de processeur spécifié.
Cœurs de processeur	Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant du nombre de cœurs de processeur spécifié.
Taille totale	Utilisez ce filtre si vous souhaitez afficher les données sur le matériel

© Acronis International GmbH, 2003-2026

Filtre	Description
du disque	des terminaux disposant de la taille totale de stockage spécifiée.
Capacité mémoire	Utilisez ce filtre si vous souhaitez afficher les données sur le matériel des terminaux disposant de la capacité de mémoire RAM spécifiée.

d. Cliquez sur **Appliquer**.

5. [Facultatif] Pour trier les données dans l'ordre croissant, cliquez sur un nom de colonne.

Affichage du matériel d'un seul terminal

Vous pouvez afficher des informations détaillées sur la carte mère, les processeurs, la mémoire, la carte graphique, les lecteurs de stockage, le réseau et le système d'un terminal spécifique.

Prérequis

- Le terminal utilise le système d'exploitation Windows ou macOS.
- Le terminal dispose d'une licence qui prend en charge la fonctionnalité Inventaire du matériel.

> **Remarque**
> La fonctionnalité « Inventaire du matériel » pour les machines virtuelles n'est pas prise en charge dans les anciennes éditions de Cyber Protect.

- Un agent de protection est installé sur le terminal.
- L'analyse de l'inventaire matériel sur le terminal s'est déroulée correctement.
- [Si le terminal est une machine virtuelle] La machine utilise l'une des plates-formes de virtualisation prises en charge. Pour plus d'informations, voir "Gestion de votre inventaire matériel" (p. 1379).

Pour afficher les informations détaillées sur le matériel d'un terminal spécifique

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Dans le champ à liste déroulante **Affichage :**, sélectionnez **Matériel**.
3. Recherchez le terminal que vous souhaitez inspecter à l'aide de l'une des méthodes décrites ci-dessous.
   - Recherchez le terminal à l'aide de l'option **Filtre** :
     a. Cliquez sur **Filtre**.
     b. Sélectionnez un ou plusieurs des paramètres de filtre pour rechercher le terminal.
     c. Cliquez sur **Appliquer**.
   - Recherchez le terminal à l'aide de l'option **Recherche** :
     a. Cliquez sur **Rechercher**.
     b. Saisissez une partie ou l'intégralité du nom du terminal, puis appuyez sur la touche **Entrée**.

© Acronis International GmbH, 2003-2026

4. Cliquez sur la ligne qui indique le terminal, puis cliquez sur **Inventaire**.
5. Cliquez sur l'onglet **Matériel**.

   Les données suivantes sur le matériel sont disponibles.

Composant matériel	Informations affichées
Carte mère	Nom, fabricant, modèle et numéro de série de la carte mère du terminal.
Processeurs	Fabricant, modèle, vitesse maximale de l'horloge et nombre de cœurs de chaque processeur du terminal.
Mémoire	Capacité, fabricant et numéro de série de la mémoire du terminal.
Graphiques	Fabricant et modèle des processeurs graphiques du terminal.
Lecteurs de stockage	Modèle, type de support, espace disponible et taille des lecteurs de stockage du terminal.
Réseau	Adresse MAC, adresse IP et type des cartes réseau du terminal.
Système	Identifiant de solution, date d'installation d'origine, heure de démarrage du système, fabricant et modèle du système, numéro de série, version du BIOS, périphérique de démarrage, paramètres régionaux du système et fuseau horaire du système.

Gestion de logiciels

Remarque
Pour accéder à cette fonctionnalité, vous devez disposer de l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise, cyberadministrateur ou administrateur en lecture seule.

Les fonctionnalités de gestion de logiciels de Cyber Protection couvrent l'intégralité du cycle de vie des logiciels.

- Déploiement de logiciels à l'aide de DeployPilot : ajoutez des packages logiciels au référentiel de logiciels et déployez rapidement des logiciels sur des ressources distantes.
- Analyse de l'inventaire : exécutez des analyses d'inventaire automatiques ou manuelles sur les terminaux et obtenez une visibilité complète sur les logiciels installés sur ces terminaux.
- Évaluation des vulnérabilités : exécutez des analyses de vulnérabilités pour identifier les vulnérabilités des systèmes d'exploitation et des logiciels installés sur les terminaux.

© Acronis International GmbH, 2003-2026

- Gestion des correctifs : gérez les correctifs (mises à jour) des systèmes d'exploitation et des logiciels installés sur vos terminaux, et maintenez vos systèmes à jour.

Gestion de votre inventaire de logiciels

La disponibilité de cette fonctionnalité dépend de la licence qui est affectée à votre ressource.

Cette fonctionnalité vous permet d'afficher toutes les applications logicielles installées sur tous les terminaux Windows et macOS.

Pour obtenir les données d'inventaire du logiciel, vous pouvez exécuter des analyses automatiques ou manuelles sur les terminaux.

Vous pouvez utiliser les données d'inventaire du logiciel pour :

- rechercher et comparer les informations concernant toutes les applications installées sur les terminaux de l'entreprise ;
- déterminer si une application doit être mise à jour ;
- déterminer si une application inutilisée doit être supprimée ;
- vérifier que la version du logiciel est la même sur différents terminaux de l'entreprise ;
- surveiller les modifications du statut du logiciel entre des analyses consécutives.

Activation ou désactivation de l'analyse de l'inventaire logiciel

Lorsque l'analyse de l'inventaire logiciel est activée sur les terminaux, le système collecte automatiquement les données logicielles toutes les 12 heures.

La fonctionnalité d'analyse de l'inventaire du logiciel est activée par défaut pour tous les terminaux qui possèdent la licence requise, mais vous pouvez modifier le paramètre si nécessaire.

Remarque
Les tenants du client peuvent activer ou désactiver l'analyse de l'inventaire du logiciel. Les tenants d'unités peuvent consulter les paramètres d'analyse de l'inventaire du logiciel, mais ils ne peuvent pas les modifier.

Activer

Pour activer l'analyse de l'inventaire logiciel

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Gestion**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Activez le module **Analyse de l'inventaire du logiciel** en cliquant sur le commutateur à côté du nom du module.

Désactiver

Pour désactiver l'analyse de l'inventaire logiciel

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Paramètres**.
2. Cliquez sur **Gestion**.
3. Cliquez sur **Analyse de l'inventaire**.
4. Désactivez le module **Analyse de l'inventaire du logiciel** en cliquant sur le commutateur à côté du nom du module.

Démarrage manuel d'une analyse de l'inventaire logiciel

Vous pouvez démarrer manuellement une analyse de l'inventaire logiciel à partir de l'écran **Inventaire logiciel** ou de l'onglet **Logiciel** sur l'écran **Inventaire**.

Prérequis

- Le terminal utilise le système d'exploitation Windows ou macOS.
- Le terminal dispose de la licence requise.

À partir de l'inventaire logiciel

Pour démarrer une analyse de l'inventaire logiciel à partir de l'écran Inventaire logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel**.
2. Cliquez sur **Inventaire du logiciel**.
3. Dans le menu déroulant **Grouper par :**, sélectionnez **Terminaux**.
4. Trouvez le terminal que vous souhaitez analyser, puis cliquez sur **Analyser maintenant**.

À partir de Logiciel

Pour démarrer une analyse de l'inventaire logiciel à partir de l'onglet Logiciel sur l'écran Inventaire

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Cliquez sur le terminal que vous souhaitez analyser, puis cliquez sur **Inventaire**.
3. Dans l'onglet **Logiciel**, cliquez sur **Analyser maintenant**.

Navigation dans l'inventaire du logiciel

Vous pouvez afficher et parcourir les données de toutes les applications logicielles disponibles sur tous les terminaux de votre organisation.

Prérequis

- Les terminaux utilisent le système d'exploitation Windows ou macOS.
- Les terminaux disposent de la licence requise.
- Au moins un scan d'inventaire des logiciels sur les terminaux a été terminé avec succès.

Pour afficher toutes les applications logicielles disponibles sur tous les terminaux Windows et macOS

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel**.
2. Cliquez sur **Inventaire du logiciel**.

   Par défaut, les données sont regroupées par terminal. Le tableau suivant décrit les données visibles dans l'écran **Inventaire du logiciel**.

Colonne	Description
Nom	Nom de l'application.
Version	Version de l'application.
Statut	Statut de l'application. • **Nouvelle**. • **Mise à jour**. • **Supprimée**. • **Aucun changement**.
Fournisseur	Fournisseur de l'application.
Date d'installation	Date et heure d'installation de l'application.
Dernière exécution	Réservé aux terminaux macOS. Date et heure de la dernière activité de l'application.
Emplacement	Répertoire d'installation de l'application.
Utilisateur	Utilisateur pour lequel l'application a été installée.
Type de système	Réservé aux terminaux Windows. Type binaire de l'application. • **X86** pour les applications 32 bits. • **X64** pour les applications 64 bits.

3. Pour regrouper les données par application, sélectionnez dans le champ à liste déroulante **Regrouper par :** l'option **Applications**.
4. Pour réduire la quantité d'informations affichées, utilisez un ou plusieurs filtres.
   a. Cliquez sur **Filtre**.
   b. Sélectionnez un ou plusieurs filtres.

      Le tableau suivant décrit les filtres de l'écran **Inventaire du logiciel**.

Filtre	Description
Nom du terminal	Nom du terminal. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez comparer le logiciel de terminaux spécifiques.
Application	Nom de l'application. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez comparer les données d'une application spécifique sur

© Acronis International GmbH, 2003-2026

Filtre	Description
	des terminaux spécifiques ou sur tous les terminaux.
Fournisseur	Fournisseur de l'application. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez afficher toutes les applications d'un fournisseur spécifique sur des terminaux spécifiques ou sur tous les terminaux.
Statut	Statut de l'application. Il est possible de sélectionner plusieurs éléments. Utilisez ce filtre si vous souhaitez afficher toutes les applications ayant le statut sélectionné sur des terminaux spécifiques ou sur tous les terminaux.
Date d'installation	Date d'installation de l'application. Utilisez ce filtre si vous souhaitez afficher toutes les applications installées à une date spécifique sur des terminaux spécifiques ou sur tous les terminaux.
Date de l'analyse	Date d'analyse de l'inventaire du logiciel. Utilisez ce filtre si vous souhaitez afficher les informations concernant le logiciel sur des terminaux spécifiques ou sur tous les terminaux analysés à cette date.

c. Cliquez sur **Appliquer**.

5. Pour parcourir toute la liste d'inventaire du logiciel, utilisez la pagination en bas à gauche de l'écran.

- Cliquez sur le numéro de la page que vous souhaitez ouvrir.
- Dans la liste déroulante, sélectionnez le numéro de la page que vous souhaitez ouvrir.

Remarque
La liste peut contenir des informations sur les ordinateurs supprimés. La stratégie de rétention actuelle est de conserver les données des ordinateurs supprimés jusqu'à 35 jours après leur suppression.

Affichage de l'inventaire du logiciel d'un seul terminal

Vous pouvez afficher une liste de toutes les applications logicielles qui sont installées sur un terminal unique, et des informations détaillées sur les applications, telles que l'état, la version, le fournisseur, la date d'installation, la dernière exécution et l'emplacement.

Prérequis

- Le terminal utilise le système d'exploitation Windows ou macOS.
- Le terminal dispose de la licence requise.

© Acronis International GmbH, 2003-2026

- Au moins un scan d'inventaire logiciel sur le terminal a été terminé avec succès.

À partir de l'inventaire logiciel

Pour afficher l'inventaire logiciel d'un terminal unique à partir de l'écran Inventaire logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel**.
2. Cliquez sur **Inventaire du logiciel**.
3. Dans le menu déroulant **Grouper par :**, sélectionnez **Terminaux**.
4. Trouvez le terminal que vous souhaitez inspecter, en utilisant l'une des options suivantes.
   - Utilisez **Filtrer** :
     a. Cliquez sur **Filtre**.
     b. Dans le champ **Nom du terminal**, sélectionnez le nom du terminal que vous souhaitez afficher.
     c. Cliquez sur **Appliquer**.
   - Utilisez **Rechercher** :
     a. Cliquez sur **Rechercher**.
     b. Saisissez une partie ou l'intégralité du nom du terminal.

À partir de terminaux

Pour afficher l'inventaire du logiciel d'un seul terminal depuis l'écran Terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux**.
2. Cliquez sur le terminal que vous souhaitez afficher, puis cliquez sur **Inventaire**.
3. Cliquez sur l'onglet **Logiciel**.

Évaluation des vulnérabilités et gestion des correctifs

L'**évaluation des vulnérabilités** est un processus consistant à identifier, quantifier et classer par ordre de priorité les vulnérabilités identifiées dans le système. Dans le module d'évaluation des vulnérabilités, vous pouvez analyser vos ordinateurs à la recherche de vulnérabilités, et vérifier si les systèmes d'exploitation et les applications installées sont à jour et fonctionnent correctement.

L'analyse d'évaluation des vulnérabilités est prise en charge pour les machines exécutant les systèmes d'exploitation suivants :

- Windows. Pour plus d'informations, voir "Solutions Microsoft et tiers prises en charge pour l’évaluation des vulnérabilités" (p. 1391).
- macOS. Pour plus d'informations, voir "Solutions Apple et tiers prises en charge pour l’évaluation des vulnérabilités" (p. 1393).
- Ordinateurs Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Pour plus d'informations, voir "Solutions Linux prises en charge pour l'évaluation des vulnérabilités" (p. 1394).

© Acronis International GmbH, 2003-2026

Utilisez la fonctionnalité Gestion des correctifs pour gérer les correctifs (mises à jour) des applications et des systèmes d'exploitation installés sur vos terminaux, et tenir vos systèmes à jour. Dans le module Gestion des correctifs, vous pouvez approuver automatiquement ou manuellement l'installation de mises à jour sur vos terminaux.

La gestion des correctifs est prise en charge pour les machines exécutant les systèmes d'exploitation Windows. Pour plus d'informations, voir "Solutions Microsoft et tiers prises en charge pour l'évaluation des vulnérabilités" (p. 1391).

Évaluation des vulnérabilités

Le processus d'évaluation des vulnérabilités se compose des étapes suivantes :

1. Vous créez un plan de protection avec le module d'évaluation des vulnérabilités activé, spécifiez les paramètres d'évaluation des vulnérabilités, et assignez le plan à des machines.
2. Le système, de façon planifiée ou à la demande, envoie une commande pour exécuter l'analyse d'évaluation des vulnérabilités aux agents de protection installés sur les machines.
3. Les agents reçoivent la commande, commencent à analyser les machines à la recherche de vulnérabilités, puis génèrent l'activité d'analyse.
4. Une fois l'analyse d'évaluation des vulnérabilités terminée, les agents génèrent les résultats et les envoient au service de surveillance.
5. Le service de surveillance traite les données reçues des agents et affiche les résultats dans les widgets d'évaluation des vulnérabilités et dans la liste des vulnérabilités trouvées.
6. Lorsque vous obteniez une liste des vulnérabilités trouvées, vous pouvez la traiter et décider des vulnérabilités trouvées à corriger.

Vous pouvez surveiller les résultats de l'analyse d'évaluation des vulnérabilités dans les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Solutions Microsoft et tiers prises en charge pour l'évaluation des vulnérabilités

Les produits Microsoft et les produits tiers suivants pour les systèmes d'exploitation Windows sont pris en charge pour l'évaluation des vulnérabilités et la gestion des correctifs.

Produits Microsoft pris en charge

Systèmes d'exploitation de bureau

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 (Enterprise, Professional, Ultimate)

Systèmes d'exploitation des serveurs

© Acronis International GmbH, 2003-2026

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office et composants connexes

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Composants en lien avec Windows

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio et applications
- Composants du système d'exploitation

Applications serveur

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2016

© Acronis International GmbH, 2003-2026

Produits tiers pris en charge pour Windows

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Cyber Protect prend en charge l'évaluation des vulnérabilités et l'application de correctifs sur un large éventail d'applications tierces, notamment les outils de collaboration et les clients VPN, qui ont une importance vitale dans les contextes de travail à distance :

- Microsoft Teams
- Zoom
- Slack
- Webex
- NordVPN
- TeamViewer

Pour obtenir la liste complète des produits tiers pris en charge pour Windows, consultez la Liste des produits tiers pris en charge par la Gestion des correctifs (62853).

Solutions Apple et tiers prises en charge pour l'évaluation des vulnérabilités

Les produits Apple suivants et les produits tiers pour macOS sont pris en charge pour l'évaluation des vulnérabilités :

Produits Apple pris en charge

macOS

- macOS 10.13.x et versions ultérieures

Applications macOS intégrées

- Safari, iTunes et autres.

Produits tiers pour macOS pris en charge

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Thunderbird
- VLC media player

© Acronis International GmbH, 2003-2026

Pour la liste complète des solutions tiers prises en charge pour macOS, consultez la Liste des solutions tiers prises en charge par la Gestion des correctifs (62853).

Solutions Linux prises en charge pour l'évaluation des vulnérabilités

Les distributions Linux suivantes sont prises en charge pour l'évaluation des vulnérabilités :

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Paramètres d'évaluation des vulnérabilités

Pour savoir comment créer un plan de protection avec le module **Évaluation des vulnérabilités**, voir « Création d'un plan de protection ». Vous pouvez effectuer une analyse d'évaluation des vulnérabilités par planification ou à la demande (en utilisant l'action **Exécuter maintenant** dans un plan de protection).

Vous pouvez spécifier les paramètres suivants dans le module **Évaluation des vulnérabilités**.

Éléments à analyser

Définir les produits logiciels que vous souhaitez analyser à la recherche de vulnérabilités :

- Ordinateurs Windows :
  - **Produits Microsoft** : cette option fait partie du plan de protection standard.
  - **Produits Windows tiers** – la disponibilité de cette option dépend de la licence. Pour plus d'informations sur les produits Windows tiers pris en charge par Patch Management, voir Liste des produits Windows tiers pris en charge par Patch Management.
- Ordinateurs macOS :
  - **Produits Apple**
  - **Produits macOS tiers**
- Ordinateurs Linux :
  - **Analyser les packages Linux**

Planification

Définissez le planning selon lequel l'analyse d'évaluation des vulnérabilités sera effectuée sur les machines sélectionnées :

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié.

© Acronis International GmbH, 2003-2026

Champs	Description
suivants	• **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte utilisateur dont	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**.

© Acronis International GmbH, 2003-2026

Champs	Description
la connexion au système d'exploitation lancera une tâche	Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

© Acronis International GmbH, 2003-2026

Évaluation des vulnérabilités pour les machines Windows

Vous pouvez analyser les machines Windows et les produits tiers pour Windows à la recherche de vulnérabilités.

Remarque
La disponibilité de cette fonctionnalité dépend de la licence qui est affectée à votre ressource et peut entraîner des coûts supplémentaires.

Pour configurer l'évaluation des vulnérabilités pour les machines Windows

1. Dans la console Cyber Protect, créez un plan de protection et activez le module **Évaluation des vulnérabilités**.
2. Spécifiez les paramètres d'évaluation des vulnérabilités :
   - **Éléments à analyser** : sélectionnez une option ou les deux.
     - **Produits Microsoft** : cette option fait partie des fonctionnalités de protection standard.
     - **Produits Windows tiers** - cette option fait partie de RMM (mode de licence basé sur le service) ou de Sécurité et RMM (mode de licence basé sur la solution).
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.

   Pour en savoir plus sur les options de **Planification**, consultez "Paramètres d'évaluation des vulnérabilités" (p. 1394).
3. Assignez le plan aux ordinateurs Windows.

Après une analyse de l'évaluation de la vulnérabilité, vous pouvez consulter une liste des vulnérabilités trouvées. Vous pouvez traiter les informations et décider des vulnérabilités trouvées à corriger.

Pour surveiller les résultats de l'évaluation des vulnérabilités, consultez les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Évaluation des vulnérabilités pour les machines sous Linux

Vous pouvez analyser les machines sous Linux à la recherche de vulnérabilités au niveau des applications et des noyaux.

Pour configurer l'évaluation des vulnérabilités pour les machines sous Linux

1. Dans la console Cyber Protect, créez un plan de protection et activez le module **Évaluation des vulnérabilités**.
2. Spécifiez les paramètres d'évaluation des vulnérabilités :
   - **Éléments à analyser :** sélectionner **Analyser les packages Linux**.
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.

   Pour en savoir plus sur les options de **Planification**, consultez "Paramètres d'évaluation des vulnérabilités" (p. 1394).
3. Appliquez le plan aux machines Linux.

© Acronis International GmbH, 2003-2026

Après une analyse de l'évaluation de la vulnérabilité, vous pouvez consulter une liste des vulnérabilités trouvées. Vous pouvez traiter les informations et décider des vulnérabilités trouvées à corriger.

Pour surveiller les résultats de l'évaluation des vulnérabilités, consultez les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Évaluation des vulnérabilités pour les terminaux macOS

Vous pouvez analyser les terminaux macOS à la recherche de vulnérabilités au niveau du système d'exploitation et de l'application.

Pour configurer l'évaluation des vulnérabilités pour les terminaux macOS

1. Dans la console Cyber Protect, créez un plan de protection et activez le module **Évaluation des vulnérabilités**.
2. Spécifiez les paramètres d'évaluation des vulnérabilités :
   - **Éléments à analyser** : sélectionnez les **produits Apple**, les **produits macOS tiers**, ou les deux.
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.

   Pour en savoir plus sur les options de **Planification**, consultez "Paramètres d'évaluation des vulnérabilités" (p. 1394).
3. Appliquez le plan aux terminaux macOS.

Après une analyse de l'évaluation de la vulnérabilité, vous pouvez consulter une liste des vulnérabilités trouvées. Vous pouvez traiter les informations et décider des vulnérabilités trouvées à corriger.

Pour surveiller les résultats de l'évaluation des vulnérabilités, consultez les widgets **Surveillance** > **Vue d'ensemble** > **Vulnérabilités/Vulnérabilités existantes**.

Gestion des vulnérabilités trouvées

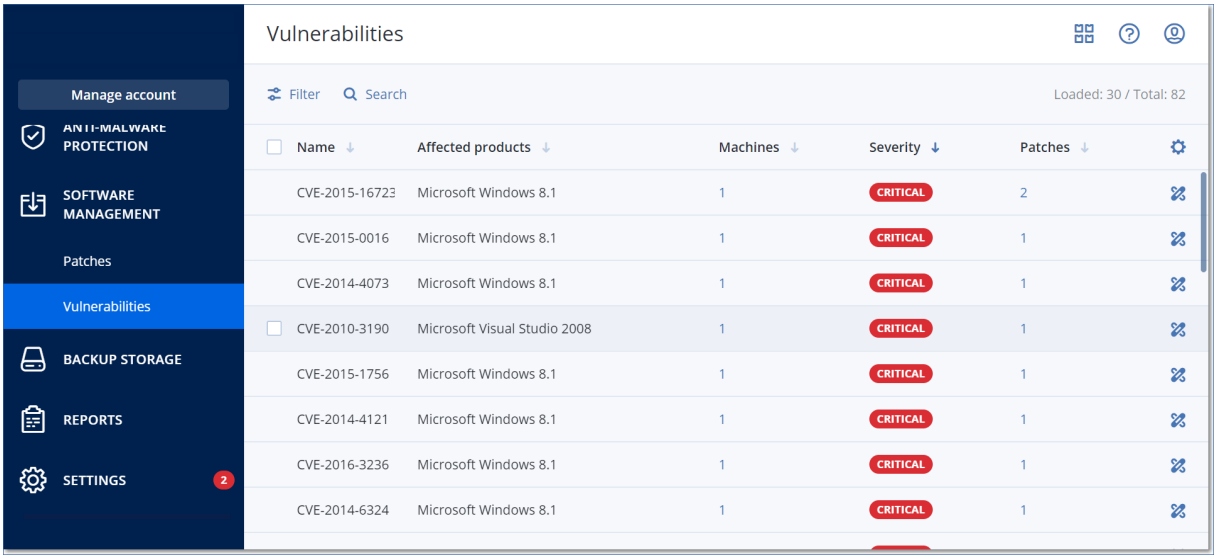
Si l'évaluation des vulnérabilités a été effectuée au moins une fois et que des vulnérabilités ont été identifiées, vous pouvez les afficher dans **Gestion de logiciel** > **Vulnérabilités**. La liste des vulnérabilités affiche à la fois les vulnérabilités qui disposent de correctifs à installer et celles pour lesquelles aucun correctif n'est suggéré. Vous pouvez vous servir du filtre pour afficher uniquement les vulnérabilités qui disposent d'un correctif.

Nom	Description
Nom	Le nom de la vulnérabilité.
Produits affectés	Produits logiciels pour lesquels les vulnérabilités ont été trouvées.
Machines	Le nombre de machines affectées.
La gravité	La gravité de la vulnérabilité trouvée. Les niveaux de gravité suivants peuvent être

© Acronis International GmbH, 2003-2026

	attribués, d'après le système d'évaluation des vulnérabilités (CVSS) : • **Critique** : 9 à 10 CVSS • **Élevée** : 7 à 9 CVSS • **Moyenne** : 3 à 7 CVSS • **Basse** : 0 à 3 CVSS • **Aucune**
Correctifs	Le nombre de correctifs appropriés.
Publié	La date et l'heure auxquelles la vulnérabilité a été publiée dans Vulnérabilités et expositions courantes (CVE).
Détecté	La date à laquelle une vulnérabilité existante a été détectée pour la première fois sur des machines.

Vous pouvez afficher la description de la vulnérabilité trouvée en cliquant sur son nom dans la liste.



Démarrer le processus de réparation des vulnérabilités

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Vulnérabilités**.
2. Sélectionnez la vulnérabilité dans la liste, puis cliquez sur **Installer les correctifs**. L'assistant de réparation des vulnérabilités apparaît.
3. Sélectionnez les correctifs à installer sur les ordinateurs sélectionnés, puis cliquez sur **Suivant**.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez installer les correctifs.
5. Sélectionnez les options de redémarrage.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel

© Acronis International GmbH, 2003-2026

Option	Description
	uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.

© Acronis International GmbH, 2003-2026

Option	Description
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

6. Cliquez sur **Installer les correctifs**.

Les correctifs choisis sont alors installés sur les machines sélectionnées.

Gestion des correctifs

Remarque

- La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.
- Pour que le module **Gestion des correctifs** puisse être activé dans le plan de protection, le module **Évaluation des vulnérabilités** doit être activé.

Pour plus d'informations sur les solutions tierces prises en charge pour les systèmes d'exploitation Windows, reportez-vous à l'article Liste des solutions tierces prises en charge par la gestion des correctifs (62853).

Utilisez la fonctionnalité de gestion des correctifs pour :

- installer les mises à jour du système d'exploitation ou des applications
- approuver manuellement ou automatiquement les correctifs
- installer les correctifs à la demande ou de façon planifiée
- définir précisément quels correctifs installer selon différents critères : gravité, catégorie et statut d'approbation
- effectuer une sauvegarde pré mise à jour pour prévenir les éventuelles mises à jour ratées
- définir l'action de redémarrage après l'installation des correctifs

Remarque

Pour travailler avec les mises à jour Windows, la fonctionnalité de gestion des correctifs nécessite que les mises à jour Windows soient activées sur la ressource. La fonctionnalité de gestion des correctifs repose sur le service de mise à jour Windows, qui détecte les mises à jour manquantes et les propose en fonction de la version du système d'exploitation en cours d'exécution.

Important

La fonctionnalité de gestion des correctifs prend en charge les mises à niveau vers Windows 11. Toutefois, vous devez vérifier que les ressources Windows 10 que vous prévoyez de mettre à niveau sont correctement préparées à cette fin. Voir cet article Microsoft pour plus de détails.

© Acronis International GmbH, 2003-2026

Pour la mise à jour de produits tiers pour Windows, Cyber Protection utilise une technologie de pair à pair pour réduire le trafic sur la bande passante. Vous pouvez choisir un ou plusieurs agents dédiés qui téléchargeront les mises à jour via Internet et les redistribueront à d'autres agents du réseau. Tous les agents partageront aussi leurs mises à jour avec les autres, en tant qu'agents de pair à pair.

Workflow Gestion des correctifs

Le workflow Gestion des correctifs comprend les étapes de configuration et d'application d'un plan de protection, l'exécution d'une analyse de l'évaluation des vulnérabilités, la configuration des paramètres de correctifs, l'approbation des correctifs et, enfin, l'installation de correctifs approuvés. Les étapes exactes du workflow sont les suivantes.

1. Configurez un plan de protection dont les modules **Évaluation des vulnérabilités** et **Gestion des correctifs** sont activés.
2. Configurez les paramètres d'évaluation des vulnérabilités. Pour plus d'informations sur ces paramètres, voir "Paramètres d'évaluation des vulnérabilités" (p. 1394).
3. Configurez les paramètres de gestion des correctifs. Pour plus d'informations sur ces paramètres, voir "Paramètres de gestion des correctifs dans le plan de protection" (p. 1402)
4. Appliquez le plan de protection à un ou plusieurs ordinateurs.
5. En attente de l'achèvement de l'analyse de l'évaluation des vulnérabilités. L'analyse démarre automatiquement en fonction de la planification configurée dans le plan de protection. Vous pouvez également démarrer l'analyse à la demande manuellement en cliquant sur l'icône **Exécuter maintenant** dans le module **Évaluation des vulnérabilités** dans le plan de protection.
6. Approuvez les correctifs. Vous pouvez définir les paramètres d'approbation automatique des correctifs, notamment l'installation automatique des correctifs sur les ordinateurs de test. Pour plus d'informations, voir "Approbation automatique des correctifs" (p. 1412). Vous pouvez également approuver les correctifs manuellement en définissant leur statut d'approbation sur **Approuvé**. Pour plus d'informations, voir "Approbation manuelle des correctifs" (p. 1417).
7. Installez les correctifs. Les correctifs approuvés peuvent être installés automatiquement en fonction de la planification configurée dans le plan de protection. Vous pouvez également installer les correctifs manuellement, à la demande. Pour plus d'informations, voir "Installation de correctifs à la demande" (p. 1418).

Vous pouvez surveiller les résultats de l'installation des correctifs dans le widget **Surveillance** > **Vue d'ensemble** > **Historique d'installation des correctifs**.

Paramètres de gestion des correctifs dans le plan de protection

Dans le module **Gestion des correctifs** du plan de protection, vous pouvez configurer les paramètres de gestion des correctifs suivants :

- Mises à jour à installer pour les produits Microsoft et tiers pour le système d'exploitation Windows.

© Acronis International GmbH, 2003-2026

- Moment d'exécution de l'installation automatique des correctifs.
- Exécution ou non d'une sauvegarde pré-mise à jour.

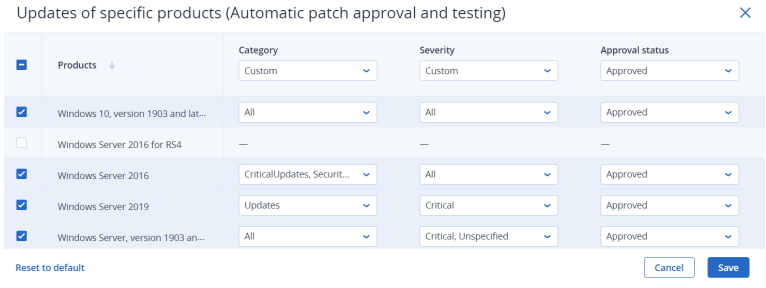
Pour plus d'informations sur la création d'un plan de protection et l'activation du module **Gestion des correctifs**, voir "Création d'un plan de protection" (p. 244).

Remarque
La disponibilité de cette fonctionnalité dépend des quotas de service activés pour votre compte.

Produits Microsoft

Pour installer les mises à jour Microsoft sur les ordinateurs sélectionnés

1. Activez l'option **Mettre les produits Microsoft à jour** dans le plan de protection.
2. Sélectionnez l'option d'installation :

Option	Description
Toutes les mises à jour	Utilisez cette option si vous souhaitez installer toutes les mises à jour approuvées.
Uniquement les mises à jour critiques et de sécurité	Utilisez cette option si vous souhaitez installer toutes les mises à jour de sécurité et critiques approuvées.
Mises à jour de produits spécifiques (approbation et test automatiques des correctifs)	Utilisez cette option si vous souhaitez définir des paramètres personnalisés pour différents produits. Si vous souhaitez mettre à jour des produits spécifiques, vous pouvez définir, pour chaque produit, les mises à jour à installer en fonction de la catégorie, de la sévérité ou du statut d'approbation. Si vous souhaitez configurer l'approbation du test automatique et le test des correctifs, sélectionnez cette option. **Important** La fonctionnalité de gestion des correctifs prend en charge les mises à niveau vers Windows 11. Toutefois, vous devez vérifier que les ressources Windows 10 que vous prévoyez de mettre à niveau sont correctement préparées à cette fin. Voir cet article Microsoft pour plus de détails. 

© Acronis International GmbH, 2003-2026

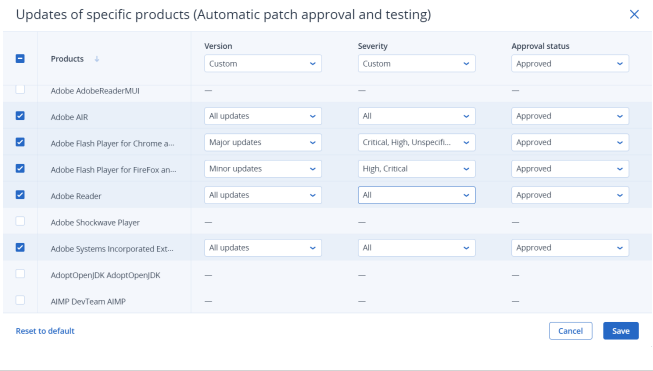
Pour les produits Microsoft, la distribution des correctifs utilise le service API Windows. Les correctifs et les mises à jour ne sont ni téléchargées ni stockées en interne ou sur des agents de distribution. Ils sont téléchargés depuis Microsoft CDN. Par conséquent, même si le rôle Responsable de la mise à jour lui est affecté, l'agent ne peut ni télécharger ni distribuer les correctifs.

Produits Windows tiers

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Pour installer les mises à jour de tiers pour le système d'exploitation Windows sur les ordinateurs sélectionnés

1. Activez l'option **Produits Windows tiers** dans le plan de protection.
2. Sélectionnez les options d'installation :

Option	Description
Toutes les mises à jour	Utilisez cette option si vous souhaitez installer toutes les mises à jour approuvées. *
Mises à jour principales uniquement	Utilisez cette option si vous souhaitez installer toutes les mises à jour majeures approuvées.
Seulement des mises à jour mineures	Utilisez cette option si vous souhaitez installer des mises à jour mineures approuvées.
Mises à jour de produits spécifiques (approbation et test automatiques des correctifs)	Utilisez cette option si vous souhaitez définir des paramètres personnalisés pour différents produits. Si vous souhaitez mettre à jour des solutions spécifiques, vous pouvez définir, pour chaque solution, les mises à jour à installer en fonction de la catégorie, de la sévérité ou du statut d'approbation. Si vous souhaitez configurer l'approbation du test automatique et le test des correctifs, sélectionnez cette option. 

© Acronis International GmbH, 2003-2026

Option	Description
N'installez les dernières versions que pour les applications dont les vulnérabilités ont été détectées	Cochez cette case à cocher si vous souhaitez installer uniquement les dernières mises à jour pour les applications qui ont détecté des vulnérabilités.

Pour les produits tiers Windows, les correctifs sont distribués directement aux ressources gérées lorsque l'accès à Internet est disponible. Si l'accès à Internet n'est pas disponible pour toutes les ressources, le rôle de responsable de la mise à jour doit être affecté à un agent disposant d'un accès à Internet. Cet agent téléchargera alors les correctifs et les distribuera aux autres agents sur le réseau.

Planification

Définissez la planification selon laquelle les mises à jour seront installées sur les ordinateurs sélectionnés.

Champs	Description
Planifiez l'exécution de la tâche à l'aide des événements suivants	Ce paramètre définit le moment où la tâche sera exécutée. Les valeurs suivantes sont disponibles : • **Planifier selon l'horaire** : il s'agit du paramètre par défaut. La tâche sera exécutée selon l'horaire spécifié. • **Lorsque l'utilisateur se connecte au système** : par défaut, la connexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. • **Lorsqu'un utilisateur se déconnecte du système** : par défaut, la déconnexion de n'importe quel utilisateur lancera la tâche. Vous pouvez modifier ce paramètre pour que seul un compte utilisateur spécifique déclenche la tâche. **Remarque** La tâche ne sera pas lancée lors d'un arrêt du système. Dans la configuration de planification, un arrêt est différent d'une déconnexion. • **Au démarrage du système** : la tâche sera exécutée au démarrage du système d'exploitation. • **À l'arrêt du système** : la tâche sera exécutée à l'arrêt du système d'exploitation.
Type de planification	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**.

© Acronis International GmbH, 2003-2026

Champs	Description
	Les valeurs suivantes sont disponibles : • **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée. • **Quotidienne** : il s'agit du paramètre par défaut. Sélectionnez les jours de la semaine au cours desquels la tâche sera exécutée. • **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.
Débuter à	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants** Sélectionnez l'heure exacte à laquelle la tâche sera exécutée.
Configurer la fenêtre de maintenance des correctifs	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Sélectionnez ce paramètre si vous souhaitez que l'installation des correctifs ne s'exécute que pendant l'intervalle de temps que vous allez indiquer. Si le processus d'installation des correctifs n'est pas terminé à l'heure de fin définie par la fenêtre de maintenance des correctifs, il est arrêté automatiquement.
Exécuter sur une plage de date	Ce champ apparaît si vous avez sélectionné l'option **Planifier selon l'horaire** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Configurez une plage pendant laquelle la planification configurée sera effective.
Précisez un compte utilisateur dont la connexion au système d'exploitation lancera une tâche	Ce champ apparaît si vous avez sélectionné l'option **Lorsque l'utilisateur se connecte au système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la connexion de n'importe quel utilisateur déclenche la tâche. • **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la connexion d'un compte utilisateur spécifique déclenche la tâche.
Précisez un compte utilisateur dont la déconnexion du système d'exploitation lancera une	Ce champ apparaît si vous avez sélectionné l'option **Lorsqu'un utilisateur se déconnecte du système** dans **Planifiez l'exécution de la tâche à l'aide des événements suivants**. Les valeurs suivantes sont disponibles : • **Tout utilisateur** : utilisez cette option si vous souhaitez que la déconnexion de n'importe quel utilisateur déclenche la tâche.

© Acronis International GmbH, 2003-2026

Champs	Description
tâche	• **L'utilisateur suivant** : utilisez cette option si vous souhaitez que la déconnexion d'un compte utilisateur spécifique déclenche la tâche.
Conditions de démarrage	Définit toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée. Les conditions de démarrage des analyses antimalware sont semblables aux conditions de démarrage du module **Sauvegarde** qui sont décrites dans la section Conditions de démarrage. Vous pouvez définir les conditions de démarrage suivantes : • **Répartir les heures de démarrage de tâche dans une fenêtre de temps :** cette option vous permet de définir le délai pour la tâche afin d'éviter les goulots d'étranglement au niveau du réseau. Vous pouvez indiquer le délai en heures ou minutes. Par exemple, si l'heure de démarrage par défaut est 10 h et que le délai est 60 minutes, la tâche démarrera entre 10 h et 11 h. • **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** • **Empêcher l'activation du mode veille ou veille prolongée lors de l'exécution de la tâche** : cette option fonctionne uniquement pour les machines sous Windows. • **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche au bout de :** spécifiez la période après laquelle la tâche sera lancée, quelles que soient les autres conditions de démarrage. **Remarque** Les conditions de démarrage ne sont pas prises en charge sous Linux.

Options de redémarrage

Indiquez si vous souhaitez que les ressources soient redémarrées après l'installation des correctifs.

Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.

© Acronis International GmbH, 2003-2026

Option	Description
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

© Acronis International GmbH, 2003-2026

Sauvegarde pré-mise à jour

Exécutez la sauvegarde avant d'installer les mises à jour du logiciel : le système créera une sauvegarde incrémentielle de la machine avant d'y installer des mises à jour. Si aucune sauvegarde n'avait été créée avant, une sauvegarde complète de la machine sera alors créée. Cela vous permet de prévenir les situations dans lesquelles l'installation des mises à jour a échoué et où vous devez revenir à un état précédent. Pour que l'option **Sauvegarde pré-mise à jour** fonctionne, le module de gestion des correctifs et le module de sauvegarde doivent tous les deux être activés sur les machines correspondantes au sein d'un plan de protection, et les éléments à sauvegarder doivent être la machine entière ou les volumes systèmes et les volumes de démarrage. Si vous sélectionnez des éléments inappropriés à sauvegarder, le système ne vous autorisera alors pas à activer l'option **Sauvegarde pré-mise à jour**.

Affichage de la liste des correctifs disponibles

Une fois l'analyse de l'évaluation des vulnérabilités effectuée, vous trouverez les informations sur les correctifs disponibles dans **Gestion de logiciel** > **Correctifs**.

Pour afficher les détails d'un correctif spécifique, cliquez dans la liste sur le correctif correspondant.

Le tableau suivant décrit les informations concernant le correctif affiché à l'écran.

Colonne	Description
Statut d'approbation	Le statut d'approbation est principalement nécessaire pour les scénarios d'approbation automatique. Vous pouvez définir l'un des statuts suivants pour un correctif : • **Approuvé :** le correctif a été installé sur au moins une machine et a été validé. • **Refusé :** le correctif n'est pas sûr et peut corrompre le système d'une machine. • **En attente d'approbation** : le statut du correctif n'est pas clair et doit être validé
Contrat de licence	• Accepté • Refusé. Si vous refusez le contrat de licence, le statut du correctif devient **Refusé** et le correctif ne sera pas installé.
La gravité	La gravité du correctif : • **Critique** • **Élevée** • **Moyenne** • **Basse** • **Aucune**
Fournisseur	Le fournisseur du correctif.
Produit affecté	Le produit auquel s'applique le correctif.
Versions	Les versions du produit qui sont déjà installées.

© Acronis International GmbH, 2003-2026

installées	
Version	La version du correctif.
Stabilité	Le score de stabilité du correctif qui indique s'il est sûr d'installer le correctif. Vous pouvez utiliser ces informations pour estimer l'impact potentiel d'un correctif avant son installation, et savoir si un correctif est stable ou peut exposer l'organisation à des vulnérabilités. Un correctif peut avoir l'un des scores de stabilité suivants : • **Stable** - Indique que le correctif n'a aucun problème ou préoccupation signalé(e) sur la base de l'analyse des sentiments et d'autres sources de données, et que le correctif est connu (il y a suffisamment de données sur ce correctif particulier). Vous pouvez installer ce correctif en toute confiance sans risque significatif. • **Problèmes mineurs** - Indique que le correctif présente des problèmes signalés, tels que des problèmes de fonctionnalité ou d'interface utilisateur, mais qu'ils sont mineurs, non critiques ou qu'il existe des solutions de contournement claires. En général, vous pouvez procéder à l'installation du correctif dans la plupart des environnements, mais vous devez d'abord examiner les problèmes. • **Attention** - Temps forts indiquant que le correctif présente des problèmes importants ou répandus, tels que l'instabilité du système, la rupture de la fonctionnalité ou l'introduction de vulnérabilités de sécurité. Dans ce cas, vous devez retarder l'installation du correctif, le tester en profondeur dans un environnement contrôlé ou attendre les mises à jour du fournisseur. • **Problèmes critiques** - Indique que le correctif présente des problèmes graves et à fort impact qui pourraient entraîner des perturbations majeures, telles que des plantages système, une perte de données ou des défaillances d'application critiques. Vous devez éviter d'installer ce correctif jusqu'à ce que le fournisseur publie un correctif ou des conseils. Lorsque vous cliquez sur les valeurs de cette colonne, vous pouvez voir les informations supplémentaires suivantes sur le correctif : aperçu du correctif, risques potentiels, statistiques et indicateurs, configurations spécifiques, informations et recommandations, et expérience utilisateur. Les informations sur la **Stabilité** sont collectées à partir de diverses sources externes à l'aide de moteurs de recherche d'intelligence artificielle.
Catégorie	La catégorie à laquelle le correctif appartient : • **Mise à jour critique :** correctifs largement diffusés pour des problèmes spécifiques, afin de régler des problèmes critiques et non liés à la sécurité. • **Mise à jour de sécurité :** correctifs largement diffusés pour des produits spécifiques, pour régler des problèmes en lien avec la sécurité. • **Mise à jour de définition :** mise à jour des fichiers de définition de virus ou d'autres fichiers de définition. • **Mise à jour cumulative :** ensemble cumulatif de correctifs, de mises à jour de sécurité, de mises à jour critiques et de mises à jour, rassemblés pour un déploiement aisé. Une mise à jour cumulative cible généralement un domaine spécifique, comme la sécurité, ou un composant spécifique, comme

© Acronis International GmbH, 2003-2026

	Internet Information Services (IIS). • **Service pack** ensemble cumulatif de tous les correctifs et de toutes les mises à jour de sécurité, mises à jour critiques et mises à jour créées depuis la sortie du produit. Les Service Pack peuvent aussi contenir un nombre limité de fonctionnalités ou de changements de conception demandés par les clients. • **Outil :** utilitaires ou fonctionnalités aidant à accomplir une tâche ou un ensemble de tâches. • **Feature pack :** nouvelles fonctionnalités, généralement intégrées aux produits dans leur prochaine version. • **Mise à jour :** correctifs largement diffusés pour des produits spécifiques, pour régler des problèmes non critiques et non liés à la sécurité. • **Application** : correctifs pour une application.
Date de publication	La date à laquelle le correctif a été publié.
Date du dernier rapport	La date du dernier signalement du correctif
Date de la première installation	La date de la première installation réussie du correctif sur un ordinateur
Base de connaissances Microsoft	Si le correctif concerne un produit Microsoft, le champ indique l'identifiant de l'article de la base de connaissances
Machines	Le nombre de machines affectées.
Vulnérabilités	Le nombre de vulnérabilités. Si vous cliquez dessus, vous serez redirigé vers la liste des vulnérabilités.
Taille	La taille moyenne du correctif
Langue	La langue prise en charge par le correctif.
Site du fournisseur	Le site officiel du correctif.

Configuration de la durée de vie des correctifs dans la liste

Vous pouvez tenir à jour la liste des correctifs en configurant la durée de vie des correctifs dans la liste disponible dans l'écran **Correctifs**. Ce paramètre définit la durée pendant laquelle le correctif disponible détecté sera visible dans la liste des correctifs. Le correctif sera supprimé de la liste une fois qu'il sera correctement installé sur tous les ordinateurs sur lesquels il a été indiqué comme manquant ou une fois la durée de vie dans la liste écoulée.

Pour configurer la durée de vie des correctifs dans la liste

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Cliquez sur **Paramètres**.
3. Dans **Durée de vie dans la liste** sélectionnez l'option appropriée.

Option	Description
Toujours	Le correctif reste toujours dans la liste.
7 jours	Le correctif sera supprimé de la liste sept jours après sa première installation. Par exemple, considérons que vous disposez de deux ordinateurs sur lesquels des correctifs doivent être installés. L'un d'eux est en ligne, et l'autre est hors ligne. Le correctif a d'abord été installé sur la première machine. Après 7 jours, le correctif sera retiré de la liste des correctifs, même s'il n'a pas été installé sur le deuxième ordinateur (car il était hors ligne).
30 jours	Le correctif est supprimé de la liste 30 jours après sa première installation.

Approbation automatique des correctifs

L'approbation automatique des correctifs facilite le processus d'installation des mises à jour sur les ordinateurs. Grâce à l'approbation automatique des correctifs, l'installation des correctifs n'est pas retardée par le processus d'approbation manuelle des correctifs. Les mises à jour et correctifs importants sont installés plus rapidement, ce qui améliore la fiabilité de votre système.

Vous pouvez utiliser l'approbation automatique des correctifs dans les scénarios test pour l'installation automatique des correctifs. Si les correctifs sont installés avec succès sur les ordinateurs de test, les correctifs seront installés automatiquement sur les ordinateurs de production également. Pour plus d'informations sur ce scénario, voir "Cas d'utilisation de l'approbation et du test automatiques des correctifs" (p. 1413).

Vous pouvez également utiliser l'approbation automatique des correctifs dans les scénarios d'installation automatique de correctifs dans votre environnement de production, et ignorer la phase de test. Pour plus d'informations sur ce scénario, voir "Cas d'utilisation d'approbation automatique des correctifs sans test" (p. 1417).

Important
La fonctionnalité de gestion des correctifs prend en charge les mises à niveau vers Windows 11. Toutefois, vous devez vérifier que les ressources Windows 10 que vous prévoyez de mettre à niveau sont correctement préparées à cette fin. Voir cet article Microsoft pour plus de détails.

Configuration de l'approbation automatique des correctifs

Vous pouvez configurer l'approbation automatique des correctifs et vous assurer que l'installation des correctifs n'est pas retardée par le processus d'approbation manuelle des correctifs.

© Acronis International GmbH, 2003-2026

Remarque
Vous pourriez ne pas être autorisé à modifier les paramètres que votre administrateur partenaire a configurés au niveau du partenaire.

Configurer l'approbation automatique des correctifs

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Cliquez sur **Paramètres**.
3. Activez **Approbation automatique des correctifs**.
4. Configurez les paramètres d'approbation automatique des correctifs.
   a. Sélectionnez l'option Approbation automatique des correctifs.

Option	Description
Approbation et test automatiques des correctifs	Le statut d'approbation du correctif passera à **Approuvé** lorsque le nombre de jours sélectionnés sera écoulé après l'installation réussie du correctif. Nous vous recommandons d'utiliser ce paramètre si vous souhaitez tester les correctifs en les installant d'abord sur un ordinateur de test, de vérifier que tout fonctionne comme prévu, puis d'installer les correctifs dans votre environnement de production.
Approbation automatique des correctifs sans test	Le statut d'approbation du correctif passera à **Approuvé** lorsque le nombre de jours sélectionnés sera écoulé après la détection du correctif.

   b. Sélectionnez le nombre de jours qui doivent s'écouler une fois que la condition de l'option Approbation automatique des correctifs est satisfaite. Après cette période, le statut d'approbation des correctifs passe automatiquement de **En attente d'approbation** à **Approuvé**.
5. Sélectionnez **Acceptez automatiquement les contrats de licence**.
6. Cliquez sur **Appliquer**.

Cas d'utilisation de l'approbation et du test automatiques des correctifs

Si vous souhaitez tester les derniers correctifs sur un ordinateur de test avant de les installer sur vos ordinateurs de production, vous pouvez configurer deux plans de protection : un plan pour l'installation de correctifs à des fins de test et un plan pour l'installation de correctifs testés sur les ordinateurs de production. Par conséquent, vous vous assurerez que les correctifs que vous installez dans votre environnement de production sont sécurisés et que vos ordinateurs de production fonctionnent correctement après l'installation de ces correctifs.

Le cas d'utilisation est constitué des étapes suivantes :

© Acronis International GmbH, 2003-2026

1. Configurez les paramètres d'approbation automatique des correctifs. Sélectionnez l'option **Approbation et test automatiques des correctifs**. Pour plus d'informations, voir "Configuration de l'approbation automatique des correctifs" (p. 1412).
2. Configurez un plan de protection à des fins de test (par exemple, Correctifs Test) avec le module **Gestion des correctifs** activé, puis appliquez-le aux ordinateurs dans l'environnement de test. Spécifiez la condition d'installation de correctif suivante : le statut d'approbation du correctif doit être **En attente d'approbation**. Cette étape est nécessaire pour valider les correctifs et vérifier si les machines fonctionnent correctement après l'installation des correctifs. Pour plus d'informations, voir "Configuration du plan de protection Correctifs Test" (p. 1415).
3. Configurez un plan de protection pour l'environnement de production (par exemple, Correctifs Production) avec le module **Gestion des correctifs** activé, puis appliquez-le aux ordinateurs dans l'environnement de production. Spécifiez la condition d'installation de correctif suivante : le statut d'approbation du correctif doit être **Approuvé**. Pour plus d'informations, voir "Configuration du plan de protection Correctifs Production" (p. 1416).
4. Exécutez le plan « Correctifs Test » et vérifiez les résultats. Conservez le statut d'approbation **En attente d'approbation** des ordinateurs ne présentant aucun problème, mais modifier en **Refusé** celui des ordinateurs qui ne fonctionnent pas correctement. En fonction du nombre de jours défini dans le paramètre **Approbation automatique des correctifs**, le statut d'approbation des correctifs passe automatiquement de **En attente d'approbation** à **Approuvé**. Lorsque vous exécutez le plan Correctifs Production, seuls les correctifs ayant le statut **Approuvé** seront installés sur les ordinateurs de production. Pour plus d'informations, voir "Exécution du plan de protection Correctifs Test et refus des correctifs non sécurisés" (p. 1417).
5. Exécutez le plan Correctifs Production.

© Acronis International GmbH, 2003-2026

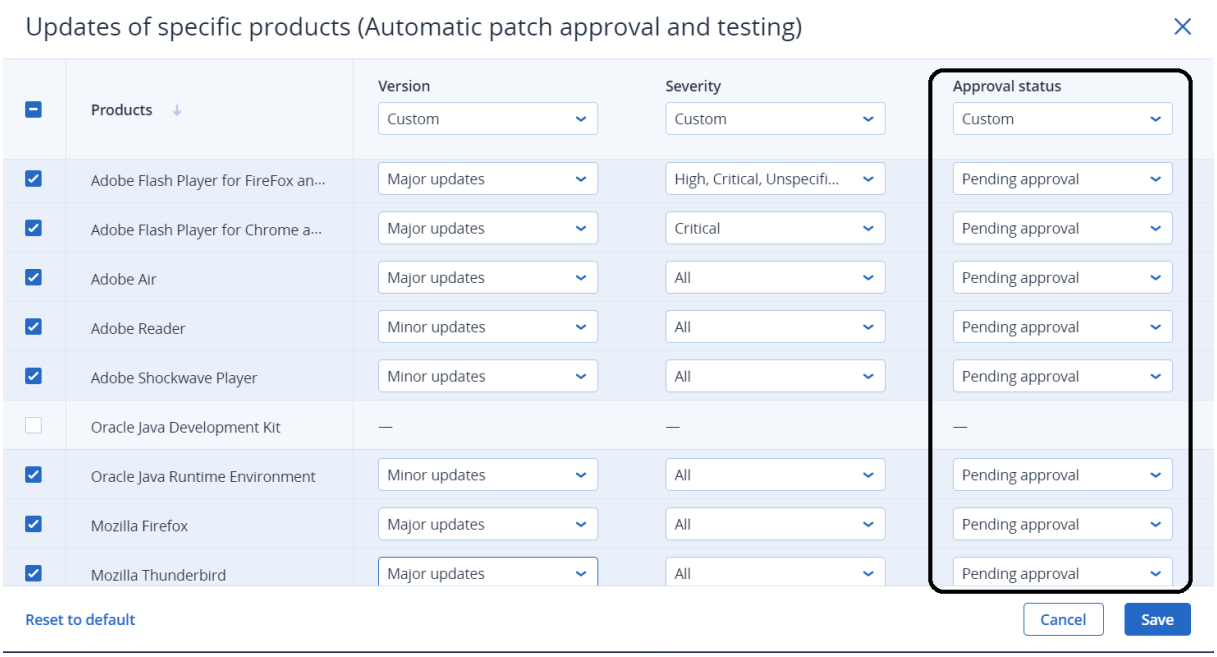
Configuration du plan de protection Correctifs Test

Vous pouvez configurer un plan de protection avec les paramètres d'installation des correctifs de vos ordinateurs dans l'environnement de test.

Pour configurer le plan de protection Correctifs Test

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Activez le module **Gestion des correctifs**.
4. Définissez les mises à jour à installer pour les produits Microsoft et tiers, le planning, et la sauvegarde pré mise à jour. Pour plus d'informations sur ces paramètres, voir "Paramètres de gestion des correctifs dans le plan de protection" (p. 1402).

Important
Pour tous les produits à mettre à jour, sélectionnez le statut d'approbation sur **En attente d'approbation**. Ainsi, l'agent installera uniquement les correctifs dont le statut est **En attente d'approbation** sur les ordinateurs sélectionnés dans l'environnement de test.



© Acronis International GmbH, 2003-2026

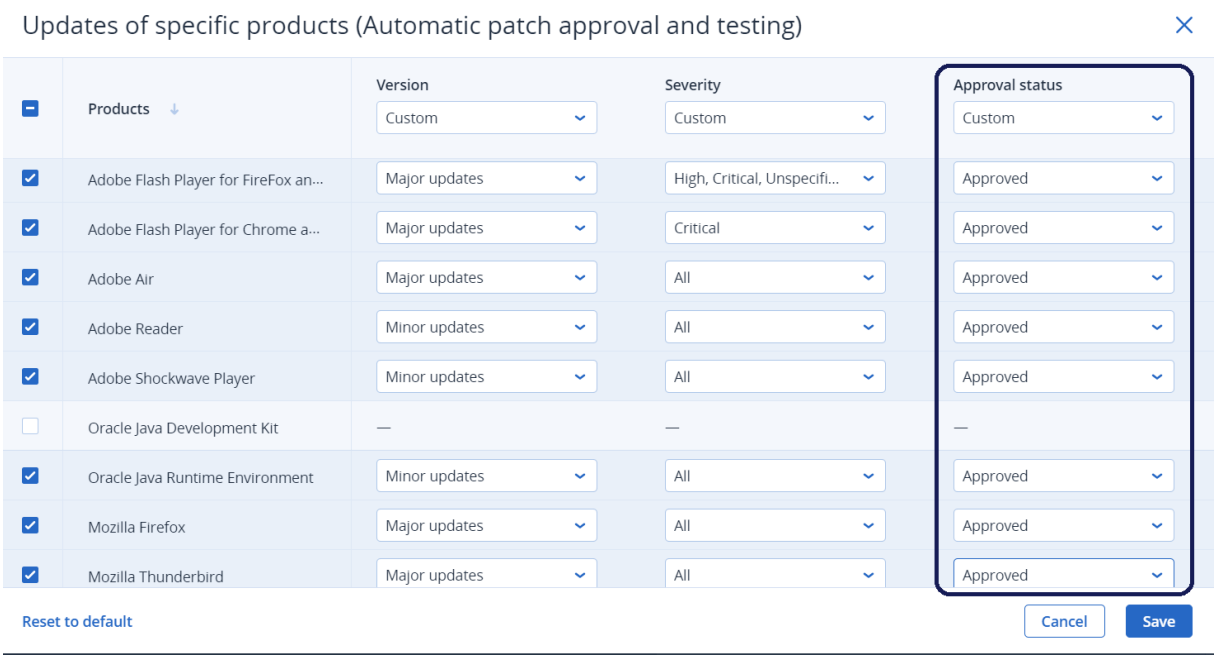
Configuration du plan de protection Correctifs Production

Vous pouvez configurer un plan de protection avec les paramètres d'installation des correctifs de votre ordinateur dans l'environnement de production.

Pour configurer le plan de protection Correctifs Production

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Activez le module **Gestion des correctifs**.
4. Définissez les mises à jour à installer pour les produits Microsoft et tiers, le planning, et la sauvegarde pré mise à jour. Pour plus d'informations sur ces paramètres, voir "Paramètres de gestion des correctifs dans le plan de protection" (p. 1402).

Important
Pour tous les produits à mettre à jour, définissez le **statut d'approbation** sur **Approuvé**. Ainsi, l'agent installera uniquement les correctifs dont le statut est **Approuvé** sur les ordinateurs sélectionnés dans l'environnement de production.



© Acronis International GmbH, 2003-2026

Exécution du plan de protection Correctifs Test et refus des correctifs non sécurisés

Après l'installation des correctifs sur les ordinateurs de votre environnement de test, vous pouvez vérifier si tout fonctionne correctement. Vous pouvez conserver le statut d'approbation **En attente d'approbation** des ordinateurs ne présentant aucun problème, mais modifier en **Refusé** celui des ordinateurs qui ne fonctionnent pas correctement.

Pour exécuter le plan de protection Correctifs Test et refuser les correctifs non sécurisés

1. Exécutez le plan de protection Correctifs Test (de façon planifiée ou manuellement).
2. Selon le résultat, déterminez les correctifs installés qui sont sûrs.
3. Accédez à **Gestion de logiciel** > **Correctifs** et définissez le **statut d'approbation** sur **Refusé** pour les correctifs qui ne sont pas sûrs.

Cas d'utilisation d'approbation automatique des correctifs sans test

Si vous souhaitez installer automatiquement de nouveaux correctifs sur vos ordinateurs de production dans les meilleurs délais, sans les installer d'abord sur les ordinateurs de test, vous pouvez configurer un seul plan de protection.

Le cas d'utilisation est constitué des étapes suivantes :

1. Configurez les paramètres d'approbation automatique des correctifs. Sélectionnez l'option **Approbation automatique des correctifs sans test**. Pour plus d'informations, voir "Configuration de l'approbation automatique des correctifs" (p. 1412).
2. Configurez un plan de protection pour l'environnement de production (par exemple, Correctifs Production) avec le module **Gestion des correctifs** activé, puis appliquez-le aux ordinateurs dans l'environnement de production. Spécifiez la condition d'installation de correctif suivante : le statut d'approbation du correctif doit être **Approuvé**. Pour plus d'informations, voir "Configuration du plan de protection Correctifs Production" (p. 1416).
3. Exécutez le plan Correctifs Production.

Approbation manuelle des correctifs

Vous pouvez approuver un correctif manuellement et accélérer son installation en ignorant la phase de test.

Prérequis

- Un plan de protection dont le module **Gestion des correctifs** est activé est appliqué à un ordinateur Windows au moins.
- Des correctifs ne sont pas encore installés sur le ou les ordinateurs sur lesquels le plan de protection est appliqué.

Pour approuver manuellement des correctifs

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Sélectionnez les correctifs que vous souhaitez installer, puis acceptez les contrats de licence.
3. Définissez le **statut d'approbation** des correctifs sur **Approuvé**.
   Le statut d'approbation des correctifs est défini sur **Approuvé**. Les correctifs seront installés automatiquement sur les ordinateurs en fonction de la planification définie dans le plan de protection. Si vous souhaitez installer les correctifs immédiatement, suivez the procédure décrite dans "Installation de correctifs à la demande" (p. 1418).

Installation de correctifs à la demande

Vous pouvez installer les correctifs manuellement, à la demande, si vous ne souhaitez pas attendre l'heure d'installation planifiée.

Vous pouvez démarrer l'installation manuelle des correctifs à partir de trois écrans : **Correctifs**, **Vulnérabilités** et **Tous les terminaux**.

Important
La fonctionnalité de gestion des correctifs prend en charge les mises à niveau vers Windows 11. Toutefois, vous devez vérifier que les ressources Windows 10 que vous prévoyez de mettre à niveau sont correctement préparées à cette fin. Voir cet article Microsoft pour plus de détails.

Pour installer manuellement un correctif

À partir de correctifs

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Acceptez le contrat de licence des correctifs que vous souhaitez installer.
3. Dans l'assistant **Installer les correctifs**, sélectionnez les correctifs que vous souhaitez installer, puis cliquez sur **Installer**.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez installer les correctifs.
5. Sélectionnez les options de redémarrage.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.

© Acronis International GmbH, 2003-2026

Option	Description
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

6. Cliquez sur **Installer les correctifs**.

À partir de vulnérabilités

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Vulnérabilités**.
2. Effectuez le processus de réparation tel que décrit dans "Gestion des vulnérabilités trouvées" (p. 1398).

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez l'ordinateur sur lequel vous souhaitez installer les correctifs.
3. Cliquez sur **Correctif**.
4. Sélectionnez les correctifs que vous souhaitez installer, puis cliquez sur **Suivant**.
5. Sélectionnez les options de redémarrage.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du

© Acronis International GmbH, 2003-2026

Option	Description
	redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

6. Cliquez sur **Installer les correctifs**.

Évaluation des vulnérabilités et gestion des correctifs au niveau partenaire

Au niveau partenaire (**Tous les clients**), vous pouvez définir, modifier et appliquer les paramètres d'évaluation des vulnérabilités et de gestion des correctifs de manière centralisée, en appliquant des plans de protection aux terminaux de tous les tenants clients simultanément. Vous pouvez également configurer et propager à vos clients les paramètres pour l'acceptation automatique des contrats de licence et l'approbation automatique des correctifs. Pour plus d'informations, voir "Configuration des paramètres de correctif au niveau du partenaire" (p. 1427).

Le système introduit des règles intelligentes pour gérer les conflits qui surviennent si un plan de protection au niveau du partenaire a des paramètres qui contredisent un plan de protection au niveau du client. Lorsque vous créez un nouveau plan au niveau du partenaire et essayez de l'appliquer à un terminal qui a déjà des stratégies d'évaluation des vulnérabilités et de gestion des correctifs appliquées au niveau du client, vous verrez l'indication de conflit et ne pourrez pas enregistrer le plan tant que vous n'aurez pas résolu le conflit. Il y a quatre options pour cela : désactiver les modules en conflit dans le plan appliqué au niveau du client, désactiver le plan appliqué au niveau du client, retirer des ressources du plan que vous créez, ou annuler la création du plan. Pour plus d'informations sur la résolution des problèmes de compatibilité, voir "Résolution des problèmes de compatibilité" (p. 253).

© Acronis International GmbH, 2003-2026

Ces fonctionnalités vous permettent de :

- Appliquez une planification et une stratégie d'approbation à tous les clients, pour maintenir des environnements uniformément protégés.
- Déployez immédiatement les correctifs critiques sur les terminaux des clients.
- Autorisez des exceptions au niveau du client pour des terminaux spécifiques ou des besoins de conformité.

Affichage des vulnérabilités au niveau du partenaire

Sur l'écran **Vulnérabilités**, vous pouvez voir une liste de toutes les vulnérabilités qui ont été trouvées sur les terminaux de vos clients, si une évaluation des vulnérabilités a été effectuée au moins une fois et que des vulnérabilités ont été trouvées.

Pour afficher les détails d'une vulnérabilité

1. Connectez-vous à la console Cyber Protect au niveau du partenaire (**Tous les clients**), puis accédez à **Gestion des logiciels** > **Vulnérabilités**.
   La liste des vulnérabilités montre à la fois les vulnérabilités pour lesquelles des correctifs doivent être installés, et celles pour lesquelles aucun correctif n'est suggéré. Vous pouvez utiliser le filtre pour n'afficher que les vulnérabilités avec correctifs.

Champs	Description
Nom	Nom de la vulnérabilité
La gravité	Gravité de la vulnérabilité détectée. Les niveaux suivants peuvent être affectés conformément au Common Vulnerability Scoring System (CVSS) : • **Critique** : 9 à 10 CVSS • **Élevée** : 7 à 9 CVSS • **Moyenne** : 3 à 7 CVSS • **Basse** : 0 à 3 CVSS • **Aucune**
Produits affectés	Nom de la solution affectée par la vulnérabilité
Clients	Nombre de clients ayant des terminaux sur lesquels la vulnérabilité a été trouvée. Si vous cliquez sur le nombre, l'onglet **Tenants affectés** s'ouvre, où vous pouvez voir une liste des clients affectés.
Terminaux	Nombre de terminaux sur lesquels la vulnérabilité a été trouvée. Si vous cliquez sur le nombre, l'onglet **Terminaux affectés** s'ouvre, où vous pouvez voir plus d'informations sur les terminaux affectés, tels que le nom, le compte client sous lequel le terminal est enregistré, et l'adresse MAC.
Correctifs	Nombre de correctifs disponibles pour résoudre la vulnérabilité. La valeur affichée est un lien vers l'écran **Correctifs**, où les résultats sont filtrés pour montrer uniquement les informations pertinentes à ce correctif spécifique.

© Acronis International GmbH, 2003-2026

Champs	Description
Publié	Date et heure auxquelles la vulnérabilité a été publiée dans Common Vulnerabilities and Exposures (CVE)
Détecté	Date à laquelle une vulnérabilité existante a été détectée pour la première fois sur des terminaux

2. Cliquez sur une vulnérabilité de la liste.

   Un volet supplémentaire s'ouvre. Vous pouvez voir plus de détails liés à la vulnérabilité sur trois onglets : **Détails & Correctifs**, **Tenants affectés**, et **Terminaux affectés**.

Affichage des correctifs au niveau du partenaire

Après qu'une analyse d'évaluation des vulnérabilités est terminée, vous pouvez voir des informations sur les correctifs disponibles pour les vulnérabilités trouvées sur les terminaux de vos clients.

Pour afficher les détails d'un correctif

1. Connectez-vous à la console Cyber Protect au niveau du partenaire (**Tous les clients**), puis allez à **Gestion des logiciels** > **Correctifs**.

   Le tableau suivant décrit les informations concernant les correctifs que vous pouvez afficher à l'écran.

Colonne	Description
Nom	Nom du correctif
La gravité	Gravité du correctif : **Critique**, **Élevée**, **Moyenne**, **Faible**, ou **Aucune**.
Stabilité	Le score de stabilité du correctif qui indique s'il est sûr d'installer le correctif. Vous pouvez utiliser ces informations pour estimer l'impact potentiel d'un correctif avant son installation, et savoir si un correctif est stable ou peut exposer l'organisation à des vulnérabilités. Un correctif peut avoir l'un des scores de stabilité suivants : • **Stable** - Indique que le correctif n'a aucun problème ou préoccupation signalé(e) sur la base de l'analyse des sentiments et d'autres sources de données, et que le correctif est connu (il y a suffisamment de données sur ce correctif particulier). Vous pouvez installer ce correctif en toute confiance sans risque significatif. • **Problèmes mineurs** - Indique que le correctif présente des problèmes signalés, tels que des

© Acronis International GmbH, 2003-2026

	problèmes de fonctionnalité ou d'interface utilisateur, mais qu'ils sont mineurs, non critiques ou qu'il existe des solutions de contournement claires. En général, vous pouvez procéder à l'installation du correctif dans la plupart des environnements, mais vous devez d'abord examiner les problèmes. • **Attention** - Temps forts indiquant que le correctif présente des problèmes importants ou répandus, tels que l'instabilité du système, la rupture de la fonctionnalité ou l'introduction de vulnérabilités de sécurité. Dans ce cas, vous devez retarder l'installation du correctif, le tester en profondeur dans un environnement contrôlé ou attendre les mises à jour du fournisseur. • **Problèmes critiques** - Indique que le correctif présente des problèmes graves et à fort impact qui pourraient entraîner des perturbations majeures, telles que des plantages système, une perte de données ou des défaillances d'application critiques. Vous devez éviter d'installer ce correctif jusqu'à ce que le fournisseur publie un correctif ou des conseils. Lorsque vous cliquez sur les valeurs de cette colonne, vous pouvez voir les informations supplémentaires suivantes sur le correctif : aperçu du correctif, risques potentiels, statistiques et indicateurs, configurations spécifiques, informations et recommandations, et expérience utilisateur. Les informations sur la **Stabilité** sont collectées à partir de diverses sources externes à l'aide de moteurs de recherche d'intelligence artificielle.
Produit affecté	Le produit auquel s'applique le correctif.
Clients	Nombre de clients ayant des terminaux sur lesquels le correctif peut être installé. Si vous cliquez sur le nombre, l'onglet **Tenants affectés** s'ouvre, où vous pouvez voir une liste des clients affectés.
Terminaux	Nombre de terminaux sur lesquels le correctif peut être installé. Si vous cliquez sur le nombre, l'onglet **Terminaux pouvant être corrigés** s'ouvre, où vous pouvez voir plus d'informations sur les terminaux, telles que le nom, le compte client sous lequel le terminal est enregistré, et l'adresse MAC.
Statut d'approbation	Statut d'approbation du correctif - principalement nécessaire pour les scénarios d'approbation

© Acronis International GmbH, 2003-2026

	automatique. • **Approuvé** – le correctif a été installé sur au moins un ordinateur et validé comme OK. • **Refusé** – le correctif n'est pas sûr et peut corrompre le système d'un ordinateur. • **Approbation en attente** – le statut du correctif n'est pas clair et doit être validé. **Remarque** Si vous avez configuré les paramètres d'approbation automatique des correctifs avec propagation à vos clients, mais qu'un client a modifié manuellement le statut d'approbation d'un correctif à une autre valeur, vous verrez un avertissement de conflit. Pour voir une liste des tenants et le statut d'approbation pour chaque tenant, cliquez sur l'icône d'avertissement de conflit. Pour plus d'informations sur la configuration des paramètres de correctif au niveau du partenaire, voir "Configuration des paramètres de correctif au niveau du partenaire" (p. 1427).
Statistiques d'approbation	Barre de couleur qui visualise le statut d'approbation des correctifs. Les couleurs représentent les statuts suivants : • Rouge - **Refusé** • Vert - **Approuvé** • Bleu – **Approbation en attente**
Versions installées	Les versions du produit qui sont déjà installées.
Version du correctif	La version du correctif.
Date du dernier rapport	Date à laquelle le correctif a été signalé pour la dernière fois
Fournisseur	Fournisseur du correctif
Catégorie	Catégorie à laquelle le correctif appartient : • **Mise à jour critique :** correctifs largement diffusés pour des problèmes spécifiques, afin de régler des problèmes critiques et non liés à la sécurité. • **Mise à jour de sécurité :** correctifs largement diffusés pour des produits spécifiques, pour régler des problèmes en lien avec la sécurité. • **Mise à jour de définition :** mise à jour des fichiers de définition de virus ou d'autres fichiers de

© Acronis International GmbH, 2003-2026

	définition. • **Mise à jour cumulative :** ensemble cumulatif de correctifs, de mises à jour de sécurité, de mises à jour critiques et de mises à jour, rassemblés pour un déploiement aisé. Une mise à jour cumulative cible généralement un domaine spécifique, comme la sécurité, ou un composant spécifique, comme Internet Information Services (IIS). • **Service pack** ensemble cumulatif de tous les correctifs et de toutes les mises à jour de sécurité, mises à jour critiques et mises à jour créées depuis la sortie du produit. Les Service Pack peuvent aussi contenir un nombre limité de fonctionnalités ou de changements de conception demandés par les clients. • **Outil :** utilitaires ou fonctionnalités aidant à accomplir une tâche ou un ensemble de tâches. • **Feature pack :** nouvelles fonctionnalités, généralement intégrées aux produits dans leur prochaine version. • **Mise à jour :** correctifs largement diffusés pour des produits spécifiques, pour régler des problèmes non critiques et non liés à la sécurité. • **Application** : correctifs pour une application.
Base de connaissances Microsoft	Si le correctif concerne un produit Microsoft, le champ indique l'identifiant de l'article de la base de connaissances
Date de publication	Date à laquelle le correctif a été publié
Date de la première installation	Date de la première installation réussie du correctif sur un ordinateur
Identifiant du correctif	Identifiant du correctif
Contrat de licence	Statut d'acceptation du contrat de licence du correctif. Le contrat de licence peut être dans l'un des statuts suivants : • **Accepté** - le contrat de licence est accepté. • **En attente** - état initial du contrat de licence, lorsqu'aucune décision n'a encore été prise. • **Refusé** – si vous refusez le contrat de licence, le statut du correctif devient **Refusé** et il ne sera pas installé.

2. Pour afficher les détails d'un correctif spécifique dans la liste des correctifs, cliquez sur le correctif correspondant.

© Acronis International GmbH, 2003-2026

Un nouveau volet s'ouvre avec des informations sur le correctif spécifique. Vous pouvez voir les détails supplémentaires suivants concernant le correctif.

Onglet	Description
Détails	Sur cet onglet, vous pouvez consulter les détails du correctif, tels que le contrat de licence, la taille, la langue, le fournisseur, ainsi que le nombre de terminaux pouvant être corrigés et de tenants affectés.
Tenants affectés	Sur cet onglet, vous pouvez voir une liste de tous les clients et unités qui ont des terminaux pouvant être corrigés (terminaux sur lesquels le correctif peut être installé) et le nombre de terminaux pouvant être corrigés par tenant.
Terminaux pouvant être corrigés	Sur cet onglet, vous pouvez voir une liste de tous les terminaux de vos clients sur lesquels le correctif peut être installé.

Configuration des paramètres de correctif au niveau du partenaire

Au niveau du partenaire (**Tous les clients**), vous pouvez configurer les paramètres pour l'acceptation automatique des contrats de licence et l'approbation automatique des correctifs et, éventuellement, les propager à tous vos clients. Ainsi, vos clients hériteront des paramètres que vous configurez et ne pourront pas les modifier.

Si vous décidez de ne pas propager les paramètres que vous configurez, vos clients verront initialement les paramètres par défaut et seront autorisés à les modifier.

Pour configurer les paramètres de correctif au niveau du partenaire

1. Dans la console Cyber Protect au niveau du partenaire (**Tous les clients**), accédez à **Gestion des logiciels** > **Correctifs**.
2. Cliquez sur **Paramètres**, puis procédez comme suit :
   a. Cliquez sur **Durée de vie dans la liste**.
      Le correctif sera supprimé de la liste une fois qu'il sera correctement installé sur tous les ordinateurs sur lesquels il a été indiqué comme manquant ou une fois la durée de vie dans la liste écoulée.

      Remarque
      Ce paramètre n'est pas propagé à vos clients.

© Acronis International GmbH, 2003-2026

b. Configurez les paramètres d'approbation automatique des correctifs.

Paramètre	Description
Approbation automatique des correctifs	Un commutateur qui active ou désactive l'approbation automatique des correctifs pour vos clients.
Appliquer l'approbation automatique des correctifs à tous les tenants de bas niveau	Sélectionnez ce champ si vous souhaitez propager les paramètres d'approbation automatique des correctifs à vos clients. **Remarque** Si vous activez l'**Approbation automatique des correctifs**, le champ est automatiquement sélectionné et désactivé, pour éviter les conflits potentiels avec les paramètres de vos clients. Vos clients seront toujours autorisés à modifier la valeur de chaque correctif manuellement, si nécessaire.
Approbation et test automatiques des correctifs	Le statut d'approbation du correctif passera à **Approuvé** lorsque le nombre de jours sélectionnés sera écoulé après l'installation réussie du correctif.
Approbation automatique des correctifs sans test	Le statut d'approbation du correctif passera à **Approuvé** lorsque le nombre de jours sélectionnés sera écoulé après la détection du correctif.
Sélecteur de période	Sélectionnez le nombre de jours qui doivent s'écouler une fois que la condition de l'option Approbation automatique des correctifs est satisfaite. Après cette période, le statut d'approbation des correctifs passe automatiquement de **En attente d'approbation** à **Approuvé**. La période maximale que vous pouvez sélectionner est de 30 jours.

c. Configurez l'acceptation automatique des contrats de licence.

Paramètre	Description
Acceptez automatiquement les contrats de licence	Un commutateur qui active ou désactive l'acceptation automatique des contrats de licence pour vos clients.
Appliquer l'acceptation automatique des contrats de licence à tous les tenants de bas niveau	Sélectionnez ce champ si vous souhaitez propager les paramètres pour l'acceptation automatique du contrat de licence à vos clients.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	Remarque Si vous activez **Appliquer le contrat de licence automatique à tous les tenants de bas niveau**, le champ est automatiquement sélectionné et désactivé, pour éviter les conflits potentiels avec les paramètres de vos clients. Vos clients pourront toujours modifier la valeur de chaque accord manuellement, si nécessaire.

3. Cliquez sur **Appliquer**, puis, dans la fenêtre de confirmation qui s'ouvre, cliquez sur **Confirmer**.

Utilisation des référentiels de logiciels et des packages logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Avec le déploiement de logiciels par DeployPilot, vous pouvez effectuer les opérations suivantes :

- Installer des logiciels sur des terminaux distants.
- Mettre à jour les applications personnalisées qui ne sont pas prises en charge par les fonctionnalités Évaluation des vulnérabilités et Gestion des correctifs. Pour prendre en charge ces fonctions, le programme d'installation téléchargé doit être préconfiguré pour prendre en charge les mises à niveau.

Packages logiciels

Les packages logiciels sont des fichiers d'installation (.msi ou .exe) que vous pouvez utiliser pour déployer (installer ou désinstaller) des logiciels à distance sur des ressources Windows. Pour vérifier les versions de Windows prises en charge, voir "Versions de Windows prises en charge" (p. 1430).

Un package logiciel est défini par la version du logiciel et certains paramètres personnalisés tels que la langue et le type d'architecture.

Référentiels de logiciels

Les référentiels de logiciels sont des dépôts de stockage des packages de logiciels.

Il existe deux référentiels de logiciels : **Bibliothèque** et **Mes packages**.

Bibliothèque

Le référentiel **Bibliothèque** contient 40 des applications logicielles les plus utilisées. Le contenu de ce référentiel est prédéfini et géré par le système. Vous pouvez voir la liste complète de ces applications dans cet article de la base de connaissances.

© Acronis International GmbH, 2003-2026

Vous ne pouvez ni modifier ni supprimer des packages de ce référentiel. Par ailleurs, vous ne pouvez pas déployer un package directement à partir de cet emplacement. Pour déployer un package, vous devez d'abord l'ajouter au référentiel **Mes packages**.

Mes packages

Le référentiel **Mes packages** contient tous les packages logiciels que vous pouvez déployer et inclure dans les plans de déploiement de logiciels. Initialement, ce référentiel est vide, même s'il existe des packages dans le référentiel **Bibliothèque**. Vous pouvez ajouter des packages à **Mes packages** à l'aide de l'une des méthodes suivantes :

- En ajoutant un package à partir du référentiel **Bibliothèque**. Pour plus d'informations, voir "Ajout de packages logiciels à partir de la bibliothèque" (p. 1433).
- En transférant manuellement un package logiciel. Pour plus d'informations, voir "Transfert de packages logiciels" (p. 1434).

Après avoir ajouté un package à **Mes packages**, vous pouvez le déployer en utilisant une action de déploiement rapide ou en l'incluant dans un plan de déploiement de logiciels. Pour plus d'informations, voir "Installation du logiciel" (p. 1438), "Désinstallation du logiciel" (p. 1442) et "Création d'un plan de déploiement de logiciels" (p. 1446).

Remarque
DeployPilot fait la distinction entre les packages ajoutés à partir du référentiel **Bibliothèque** et ceux téléchargés manuellement. Pour les packages ajoutés à partir du référentiel **Bibliothèque**, DeployPilot vérifie avant le déploiement si le logiciel est déjà installé sur le terminal et, le cas échéant, empêche toute réinstallation inutile.

La capacité de stockage maximale du référentiel **Mes packages** est de 5 Go pour les tenants clients et de 20 Go pour les tenants partenaires.

Versions de Windows prises en charge

Le déploiement de logiciels par l'intermédiaire de DeployPilot est pris en charge pour les ordinateurs avec les systèmes d'exploitation suivants :

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 (Entreprise, Professionnel, Intégrale)
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

© Acronis International GmbH, 2003-2026

- Windows Server 2012
- Windows Server 2008 R2

Navigation dans les référentiels de logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez rechercher un package logiciel spécifique dans les référentiels de packages logiciels et afficher ses détails.

Prérequis

Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise, cyberadministrateur ou administrateur en lecture seule.

Pour rechercher un package logiciel

Dans la bibliothèque

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Bibliothèque**.
   Dans l'écran **Bibliothèque**, vous pouvez voir une liste de 40 des applications logicielles les plus utilisées, ainsi que les informations suivantes pour chaque application :

Champs	Description
Nom	Nom du logiciel.
Dernière version	Dernière version de l'application disponible dans le référentiel.
Fournisseur	Nom du fournisseur de logiciels.
Type de licence	Type de licence : propriétaire ou open source.

2. [Facultatif] Pour rechercher un package logiciel par nom, cliquez sur **Recherche**, puis saisissez le nom.
   La liste des packages est filtrée dynamiquement en fonction du texte que vous saisissez dans le champ.
3. [Facultatif] Pour filtrer la liste des packages, cliquez sur **Filtrer**, spécifiez les valeurs, puis cliquez sur **Appliquer**.
   Le tableau suivant fournit d'autres détails sur les filtres disponibles sur cette page.

Filtre	Description
Fournisseur	Utilisez ce filtre si vous connaissez le nom de l'éditeur de logiciels et souhaitez voir uniquement les logiciels de cet éditeur.
Type de licence	Utilisez ce filtre si vous souhaitez filtrer les résultats en fonction du type de licence : propriétaire ou open source.

© Acronis International GmbH, 2003-2026

Filtre	Description
Dernière période de publication	Utilisez ce filtre si vous souhaitez filtrer les résultats et n'afficher que les packages logiciels publiés pendant une période spécifique.

4. Pour afficher tous les détails d'un package, cliquez sur la ligne correspondante dans la liste.

Dans Mes packages

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Mes packages**.

   Dans l'écran **Mes packages**, vous pouvez voir les packages que vous pouvez déployer sur vos ressources gérées, ainsi que les informations suivantes pour chaque package :

Champs	Description
Nom	Nom du logiciel.
Version	Version du logiciel.
Fournisseur	Nom du fournisseur de logiciels.
Vérification de la signature numérique	État de la vérification de la signature numérique.
Système d'exploitation	Système d'exploitation sur lequel le package peut être déployé.
Dernière modification par	Nom de l'utilisateur qui a apporté la dernière modification au package.
Type de système	Type d'architecture du système d'exploitation sur lequel le package logiciel sera déployé.
Taille du package	Taille du package logiciel.

2. [Facultatif] Pour rechercher un package logiciel par nom, cliquez sur **Recherche**, puis saisissez le nom.

   La liste des packages est filtrée dynamiquement en fonction du texte que vous saisissez dans le champ.

3. [Facultatif] Pour filtrer la liste des packages, cliquez sur **Filtrer**, spécifiez les valeurs, puis cliquez sur **Appliquer**.

   Le tableau suivant fournit d'autres détails sur les filtres disponibles sur cette page.

Filtre	Description
Fournisseur	Utilisez ce filtre si vous connaissez le nom de l'éditeur de logiciels et souhaitez voir uniquement les logiciels de cet éditeur.
Dernière modification	Utilisez ce filtre si vous souhaitez filtrer les résultats et n'afficher que les packages modifiés par un utilisateur défini.

© Acronis International GmbH, 2003-2026

Filtre	Description
par	
Type de système	Utilisez ce filtre si vous souhaitez filtrer les résultats en fonction du type de l'architecture système.
Langue	Utilisez ce filtre si vous souhaitez filtrer les résultats en fonction de la langue du logiciel.
Période de publication	Utilisez ce filtre si vous souhaitez filtrer les résultats et n'afficher que les packages logiciels publiés pendant une période spécifique.

4. Pour afficher tous les détails d'un package, cliquez sur la ligne correspondante dans la liste.

Ajout de packages logiciels à partir de la bibliothèque

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Le référentiel **Bibliothèque** contient 40 des applications les plus utilisées. Pour pouvoir déployer un package à partir de la bibliothèque, vous devez d'abord l'ajouter à vos packages.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour ajouter un package de la bibliothèque à Mes packages

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Bibliothèque**.
2. Sur la ligne du package logiciel que vous souhaitez ajouter à vos packages, cliquez sur **Ajouter**.
3. Dans l'assistant **Ajouter à mes packages**, sélectionnez les paramètres du logiciel.

Paramètre	Description
Version	Version du logiciel.
Langue	Langue du logiciel.
Type d'architecture	Type d'architecture du système d'exploitation sur lequel le package logiciel sera déployé.

4. Sélectionnez **J'accepte les conditions générales du contrat de licence d'utilisateur final**, puis cliquez sur **Ajouter**.
   Le package est ajouté à vos packages. Vous pouvez le voir sur la page **Mes packages**.

© Acronis International GmbH, 2003-2026

Transfert de packages logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Sur la page **Mes packages**, vous pouvez transférer des packages logiciels aux formats suivants : .msi ou .exe.

Important
Si vous prévoyez d'utiliser le package pour mettre à jour des installations existantes, assurez-vous que le package que vous téléchargerez prend en charge les mises à niveau.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour transférer un package logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Mes packages**.
2. Cliquez sur **Ajouter un package**.
3. Dans l'onglet **Transférer le package**, procédez comme suit :
   a. Cliquez sur **Transférer**, sélectionnez le package logiciel à transférer, puis cliquez sur **Ouvrir**.
   b. En fonction de votre souhait d'utiliser Copilot pour remplir automatiquement les détails du package et les informations requises, telles que la commande et les arguments d'installation et de désinstallation, activez ou désactivez l'interrupteur **Essayer Copilot**.
   c. Cliquez sur **Suivant**.
4. Dans l'onglet **Détails du package**, procédez comme suit :
   - Si vous avez utilisé Copilot pour remplir automatiquement les détails du package, passez-les en revue, assurez-vous qu'ils sont corrects, puis cliquez sur **Suivant**.

     Remarque
     Vous pouvez corriger manuellement les détails du package qui ont été remplis par Copilot, ou cliquer sur **Annuler les modifications** pour supprimer tous les détails du package.

   - Si vous n'avez pas utilisé Copilot pour remplir automatiquement les détails du package, saisissez les détails, puis cliquez sur **Suivant**.

Champs	Description
Nom du logiciel	Nom du logiciel. Ce champ est obligatoire.

© Acronis International GmbH, 2003-2026

Champs	Description
Fournisseur/Éditeur	Nom du fournisseur de logiciels. Ce champ est obligatoire.
Description du logiciel	Description supplémentaire du logiciel. Ce champ est facultatif.
Type de licence	Type de licence du logiciel. • **Propriétaire**. Les licences propriétaires sont détenues et contrôlées par les éditeurs de logiciels. C'est la valeur par défaut. • **Open source**. Il s'agit des licences pour les logiciels open source qui sont gratuits pour la distribution publique.
Version	Version du logiciel. Ce champ est obligatoire.
Type d'architecture	Type d'architecture du système d'exploitation sur lequel le package logiciel sera déployé. Ce champ est obligatoire.
Langue	Langue du logiciel. Ce champ est facultatif.
Date de publication	Date de publication du logiciel. Ce champ est obligatoire.

5. Dans l'onglet **Commandes d'installation/de désinstallation**, procédez comme suit :
   - Si vous avez utilisé Copilot pour remplir automatiquement les commandes et arguments d'installation et de désinstallation, vérifiez les détails, assurez-vous qu'ils sont corrects, puis cliquez sur **Suivant**.
   - Si vous n'avez pas utilisé Copilot pour remplir automatiquement les informations du package, procédez comme suit :
     a. [Facultatif] Dans la section **Options d'installation**, champ **Arguments de commande**, saisissez les arguments de commande d'installation.
     b. [Facultatif] Dans les champs **Codes de retour de redémarrage** et **Codes de retour de réussite**, spécifiez les codes de retour qui indiquent le résultat du processus d'installation.
     c. Dans la section **Options de désinstallation**, sélectionnez la méthode de désinstallation :

Méthode de désinstallation	Description
Ligne de commande	Si vous sélectionnez cette méthode, vous devez fournir la commande et les arguments de désinstallation silencieuse corrects. Sinon, la désinstallation risque de ne pas répondre.
Nom du logiciel ou du fournisseur	Si vous sélectionnez cette méthode, le système utilisera le nom du logiciel, le nom du fournisseur ou le modèle d'expression régulière que vous avez fourni pour localiser et exécuter automatiquement la commande de désinstallation. Utilisez cette méthode si vous ne connaissez pas la commande de désinstallation de l'application.

© Acronis International GmbH, 2003-2026

d. [Si vous avez sélectionné **Nom du logiciel ou du fournisseur**] Dans le champ **Nom du logiciel**, saisissez le nom du logiciel.
e. [Si vous avez sélectionné **Nom du logiciel ou du fournisseur**] Dans le champ **Nom du fournisseur**, saisissez le nom du fournisseur du logiciel.
f. [Si vous avez sélectionné **Ligne de commande**] Dans le champ **Chemin de désinstallation**, saisissez le chemin et la commande de désinstallation.
   Le chemin de désinstallation est le chemin d'accès, sur un ordinateur, au répertoire où se trouve l'exécutable de désinstallation du programme. Le chemin de désinstallation est essentiel pour que le programme puisse être supprimé du système correctement et complètement.
g. Dans le champ **Arguments de commande**, saisissez les arguments de commande de désinstallation.
h. [Facultatif] Dans la zone **Codes de retour de réussite**, saisissez les codes de retour.
i. [Facultatif] Dans les champs **Codes de retour de réussite**, saisissez les codes de retour.
j. Cliquez sur **Suivant**.

Pour plus d'informations sur les commandes et les arguments d'installation et de désinstallation, voir "Arguments de commande" (p. 1437).

6. Dans l'onglet **Résumé**, examinez les détails du package logiciel, sélectionnez **J'ai examiné les détails du package et je confirme que je veux l'ajouter à Mes packages** et **J'accepte les Conditions générales du contrat de licence d'utilisateur final**, puis cliquez sur **Suivant**.
7. Dans l'onglet **Vérification de la signature numérique** :
   - Si vous souhaitez vérifier la signature numérique du package, sélectionnez **Activer la vérification de la signature numérique**.

     Remarque
     Nous vous recommandons de toujours vérifier la signature numérique. Cela garantit que le package personnalisé qui sera transféré est conforme et signé numériquement, et cela réduit également le risque de déployer un logiciel non vérifié ou falsifié.

   - Pour ignorer la vérification, désactivez l'option **Activer la vérification de la signature numérique**.
8. Cliquez sur **Ajouter un package**.

Commandes et arguments d'installation et de désinstallation

En fournissant des arguments d'installation et de désinstallation lors du chargement manuel de packages logiciels, vous pouvez garantir la réussite du déploiement de logiciels dans votre organisation.

Remarque
Vous pouvez utiliser Copilot pour remplir automatiquement les arguments d'installation et de désinstallation.

© Acronis International GmbH, 2003-2026

Commandes d'installation

Arguments de commande

Les arguments de ligne de commande sont des paramètres ou des indicateurs que vous pouvez spécifier pour le processus d'installation. Voici des exemples courants :

- Installation silencieuse (installe le logiciel sans afficher d'interface utilisateur) :
  `/s` ou `/quiet`
- Aucun redémarrage (empêche le système de redémarrer automatiquement après l'installation) :
  `/norestart`
- Fichier journal (crée un fichier journal permettant de suivre le processus d'installation) :
  `/l* log.txt`

Commandes de désinstallation

Chemin de désinstallation

Le chemin de désinstallation fournit le chemin d'accès au fichier nécessaire et la commande de désinstallation du logiciel. Par exemple :

```
%ProgramFiles%\7-Zip\Uninstall.exe
```

Arguments de commande

Les arguments de ligne de commande sont des paramètres ou des indicateurs que vous pouvez spécifier pour le processus de désinstallation. Voici des exemples courants :

- Désinstallation silencieuse (désinstalle le logiciel sans afficher d'interface utilisateur) :
  `/s` ou `/quiet`
- Aucun redémarrage (empêche le système de redémarrer automatiquement après la désinstallation) :
  `/norestart`
- Fichier journal (crée un fichier journal permettant de suivre le processus de désinstallation) :
  `/l* log.txt`

Modification des packages logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous ne pouvez modifier que les packages logiciels que vous avez transférés manuellement.

Prérequis

© Acronis International GmbH, 2003-2026

Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour modifier un package logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Mes packages**.
2. Pour le package que vous souhaitez modifier, cliquez sur l'icône **...**, puis sur **Modifier**.
3. Dans l'assistant **Modifier le package**, modifiez les paramètres, puis cliquez sur **Enregistrer**.

Suppression de packages logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez supprimer les packages logiciels dont vous n'avez plus besoin.

Prérequis

Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour supprimer un package logiciel

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Mes packages**.
2. Pour le package que vous souhaitez modifier, cliquez sur l'icône **...**, puis sur **Supprimer**.
3. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Si le package a été transféré manuellement, il sera définitivement supprimé. S'il a été ajouté à partir de la bibliothèque, il sera supprimé uniquement de vos packages.

Installation du logiciel

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez installer des logiciels à distance sur vos ressources gérées sans créer de plan de déploiement de logiciel. Cette action peut être effectuée pour un maximum de 15 packages logiciels et de 150 ressources cibles simultanément.

Prérequis

Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour installer un package logiciel

Depuis Mes packages

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Mes packages**.
2. Sélectionnez le logiciel que vous souhaitez installer, puis cliquez sur **Installer**.
3. Dans la fenêtre **Déployer le logiciel**, cliquez sur **Ajouter des ressources**.
4. Sélectionnez les ressources sur lesquelles vous souhaitez installer le package, puis cliquez sur **Ajouter**.
5. Pour configurer les options de redémarrage, procédez comme suit :
   a. Cliquez sur le champ **Options de redémarrage**.
   b. Dans l'écran **Options de redémarrage**, configurez si le système redémarrera les ressources après l'installation du logiciel.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à

© Acronis International GmbH, 2003-2026

Option	Description
	l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

c. Cliquez sur **Terminé**.

6. Cliquez sur **Installer maintenant**.

Remarque
Les packages pour lesquels la vérification de la signature numérique échoue ne seront pas déployés.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur une ressource, puis sur **Déployer le logiciel**.
3. Dans la fenêtre **Déployer le logiciel**, champ **Action**, sélectionnez **Installer**.
4. Cliquez sur **Sélectionner le logiciel**, sélectionnez le logiciel que vous souhaitez installer, puis cliquez sur **Terminé**.
5. Pour configurer les options de redémarrage, procédez comme suit :

© Acronis International GmbH, 2003-2026

a. Cliquez sur le champ **Options de redémarrage**.

b. Dans l'écran **Options de redémarrage**, configurez si le système redémarrera les ressources après l'installation du logiciel.

Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes.

© Acronis International GmbH, 2003-2026

Option	Description
	Remarque Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

c. Cliquez sur **Terminé**.

6. Cliquez sur **Déployer maintenant**.

Désinstallation du logiciel

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez désinstaller un logiciel à distance à partir de vos ressources gérées sans créer de plan de déploiement de logiciel.

Prérequis

Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour désinstaller un package logiciel

Depuis Mes packages

1. Dans la console Cyber Protect, accédez à **Gestion de logiciel** > **Mes packages**.
2. Sélectionnez le package que vous souhaitez installer, puis cliquez sur **Désinstaller**.
3. Dans la fenêtre **Déployer le logiciel**, cliquez sur **Ajouter des ressources**.

© Acronis International GmbH, 2003-2026

4. Sélectionnez une ou plusieurs ressources sur lesquelles vous souhaitez installer le package, puis cliquez sur **Ajouter**.
5. Pour configurer les options de redémarrage, procédez comme suit :
   a. Cliquez sur le champ **Options de redémarrage**.
   b. Dans l'écran **Options de redémarrage**, configurez si le système redémarrera les ressources après la désinstallation du logiciel.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures

© Acronis International GmbH, 2003-2026

Option	Description
	suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

c. Cliquez sur **Terminé**.

6. Cliquez sur **Désinstaller maintenant**.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur une ressource, puis sur **Déployer le logiciel**.
3. Dans la fenêtre **Déployer le logiciel**, champ **Action**, sélectionnez **Désinstaller**.
4. Cliquez sur **Sélectionner le logiciel**, sélectionnez le logiciel que vous voulez désinstaller, puis cliquez sur **Terminé**.
5. Pour configurer les options de redémarrage, procédez comme suit :
   a. Cliquez sur le champ **Options de redémarrage**.
   b. Dans l'écran **Options de redémarrage**, configurez si le système redémarrera les ressources après la désinstallation du logiciel.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.

© Acronis International GmbH, 2003-2026

Option	Description
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage.

© Acronis International GmbH, 2003-2026

Option	Description
	• 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal immédiatement	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

c. Cliquez sur **Terminé**.

6. Cliquez sur **Déployer maintenant**.

Plans de déploiement de logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Grâce aux plans de déploiement de logiciels, vous pouvez automatiser le processus de déploiement de logiciels et garantir que la distribution de logiciels sur vos ressources gérées est cohérente. Cette option comprend les fonctionnalités suivantes :

- Installation ou désinstallation à distance de logiciels.
- Planifications de l'installation ou de la désinstallation automatiques de logiciels.
- Actions ultérieures à l'installation.

Création d'un plan de déploiement de logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez créer un plan de déploiement de logiciels, puis l'affecter à une ou plusieurs ressources. Vous vous assurez ainsi de distribuer et d'installer des logiciels approuvés sur vos ressources gérées tout en désinstallant les logiciels obsolètes ou non approuvés par votre organisation.

Lorsqu'Active Protection est activée dans le plan de protection appliqué aux ressources, le déploiement de logiciels est protégé par le moteur antimalware. Avant d'installer un package sur les ressources, le système exécute automatiquement une analyse antimalware. Cette couche de défense proactive offre une protection contre les injections malveillantes, ce qui garantit que le déploiement de logiciels n'introduira pas de vulnérabilités dans les systèmes. Cela est particulièrement précieux dans les environnements où la sécurité est critique, et réduit le risque d'interruption d'activité et d'intervention sur incidents coûteuse.

© Acronis International GmbH, 2003-2026

Remarque
Un plan de déploiement de logiciel ne prend en charge qu'une seule des opérations de déploiement : installation ou désinstallation. Cela signifie que vous devez créer des plans distincts, l'un pour l'installation du logiciel et l'autre pour sa désinstallation.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour créer un plan de déploiement de logiciel

Depuis Plans de déploiement de logiciels

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de déploiement de logiciels**.
2. Créez un plan en utilisant l'une des deux options :
   - Si la liste ne comprend aucun plan de déploiement de logiciel, cliquez sur **Créer**.
   - Si la liste comprend des plans de déploiement de logiciel, cliquez sur **Créer un plan**.
3. [Facultatif] Pour ajouter des ressources au plan :
   a. Cliquez sur **Ajouter des ressources**.
   b. Sélectionnez les ressources, puis cliquez sur **Ajouter**.
4. Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **Poursuivre**.
5. Dans le champ **Action**, sélectionnez si le plan installera ou désinstallera le logiciel.
6. Dans le champ **Logiciel**, cliquez sur **Sélectionner un logiciel**, sélectionnez une ou plusieurs applications dans la liste, puis cliquez sur **Terminé**.
7. Pour configurer les options de redémarrage, procédez comme suit :
   a. Cliquez sur le champ **Options de redémarrage**.
   b. Dans l'écran **Options de redémarrage**, configurez si le système redémarrera les ressources après l'installation ou la désinstallation du logiciel.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.

© Acronis International GmbH, 2003-2026

Option	Description
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur	Cette option est disponible si vous avez sélectionné l'option

© Acronis International GmbH, 2003-2026

Option	Description
n'est connecté au terminal, redémarrer le terminal immédiatement	**Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le redémarrage automatique soit entièrement écoulée.

c. Cliquez sur **Terminé**.

8. Pour planifier l'exécution du plan, procédez comme suit :

a. Cliquez sur le champ **Planifier**.

b. Dans l'écran **Planifier**, champ **Planifiez l'exécution de la tâche à l'aide des événements suivants**, sélectionnez l'événement qui démarrera le plan.

Option	Description
Ex. une fois	Si vous sélectionnez cette option, vous devez configurer la date et l'heure d'exécution du plan.
Planifier selon l'horaire	Si vous sélectionnez cette option, vous pouvez configurer des plans qui s'exécutent toutes les heures, tous les jours ou tous les mois. Si vous souhaitez que cette planification soit effective uniquement pendant une période spécifique, cochez la case **Exécuter sur une plage de dates**, puis configurez la période (en jours) pendant laquelle le plan planifié s'exécutera.
Lorsque l'utilisateur se connecte au système	Si vous sélectionnez cette option, le plan s'exécutera lorsqu'un utilisateur spécifique ou n'importe quel utilisateur se connectera à la ressource cible.
Lorsqu'un utilisateur se déconnecte du système	Si vous sélectionnez cette option, le plan s'exécutera lorsqu'un utilisateur spécifique ou n'importe quel utilisateur se déconnectera de la ressource cible.
Au démarrage du système	Si vous sélectionnez cette option, le plan s'exécutera lorsque la ressource cible démarrera.
Lorsque le système est arrêté	Si vous sélectionnez cette option, le plan s'exécutera lorsque la ressource cible s'arrêtera.
Lorsque le système est en ligne	Si vous sélectionnez cette option, le plan s'exécutera lorsque la ressource cible sera en ligne.

© Acronis International GmbH, 2003-2026

c. Dans la section **Conditions de démarrage**, sélectionnez toutes les conditions qui doivent être remplies simultanément pour que le plan démarre.

Condition	Description
Exécuter uniquement si la ressource est en ligne	Cette condition est remplie lorsque la ressource cible est connectée à Internet.
L'utilisateur est inactif	Cette condition est remplie lorsqu'un écran de veille s'exécute sur l'ordinateur ou si l'ordinateur est verrouillé.
Utilisateur déconnecté	Si vous sélectionnez cette condition, vous pouvez reporter un plan planifié jusqu'à ce que l'utilisateur de la ressource cible se déconnecte.
Compris dans un intervalle de temps	Si vous sélectionnez cette condition, vous devez définir l'intervalle de temps pendant lequel le plan peut s'exécuter.
Économiser de la batterie	Si vous sélectionnez cette condition, vous pouvez vous assurer que le plan ne sera pas interrompu en raison d'une batterie faible. Les options suivantes sont disponibles : • **Ne pas démarrer lors d'une alimentation sur batterie** Le plan démarrera uniquement si l'ordinateur est connecté à une source d'alimentation. • **Démarrer pendant l'alimentation sur batterie si le niveau de batterie est supérieur à** Le plan démarrera si l'ordinateur est connecté à une source d'alimentation ou si le niveau de batterie est supérieur à la valeur spécifiée.
Ne pas démarrer pendant une connexion mesurée	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si la ressource cible accède à Internet via une connexion mesurée.
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si la ressource cible est connectée à l'un des réseaux sans fil spécifiés. Pour utiliser cette condition, vous devez indiquer le SSID du réseau interdit. La restriction s'applique à tous les réseaux qui contiennent le nom spécifié comme sous-chaîne dans leur nom, quelle que soit la casse. Par exemple, si vous spécifiez `téléphone` comme nom de réseau, le plan ne démarrera pas lorsque le terminal sera connecté à l'un des réseaux suivants : `Téléphone de Jean`, `téléphone_wifi` ou `mon_wifi_TÉLÉPHONE`.
Vérifier l'adresse IP du terminal	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si l'une des adresses IP de la ressource cible se trouve au sein ou en dehors de la plage d'adresses IP spécifiée. Les options suivantes sont disponibles : • **Démarrer si en dehors de la plage d'adresses IP**

© Acronis International GmbH, 2003-2026

Condition	Description
	• **Démarrer si dans la plage d'adresses IP** Prend en charge uniquement les adresses IPv4.
Si les conditions de démarrage ne sont pas remplies, exécuter quand même la tâche	Utilisez cette option pour définir l'intervalle de temps après lequel le plan sera exécuté, quelles que soient les autres conditions. Le plan démarrera dès que les autres conditions seront remplies ou dès que la période spécifiée sera écoulée. Cette option n'est pas disponible si vous avez sélectionné l'option **Exécuter une fois** pour la planification.

d. Cliquez sur **Terminé**.

9. Cliquez sur **Créer**.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de déploiement de logiciel.
3. Cliquez sur **Protection**, puis sur **Ajouter un plan**.
4. Cliquez sur **Créer un plan**, puis sélectionnez **Déploiement de logiciels**.
5. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **Poursuivre**.
6. Dans le champ **Action**, sélectionnez si le plan installera ou désinstallera le logiciel.
7. Dans le champ **Logiciel**, cliquez sur **Sélectionner un logiciel**, sélectionnez une ou plusieurs applications dans la liste, puis cliquez sur **Terminé**.
8. Pour configurer les options de redémarrage, procédez comme suit :
   a. Cliquez sur le champ **Options de redémarrage**.
   b. Dans l'écran **Options de redémarrage**, configurez si le système redémarrera les ressources après l'installation ou la désinstallation du logiciel.
   Le tableau suivant fournit d'autres d'informations sur les options de redémarrage.

Option	Description
Redémarrer si nécessaire	Cochez cette case si vous souhaitez que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel uniquement si le logiciel l'exige.
Toujours redémarrer	Cochez cette case si vous souhaitez que les ressources soient toujours redémarrées après l'installation ou la désinstallation du logiciel.
Ne pas afficher	Cochez cette case si vous ne souhaitez pas que les ressources soient redémarrées après l'installation ou la désinstallation du logiciel.

© Acronis International GmbH, 2003-2026

Option	Description
Planifier un redémarrage automatique	Cette option est disponible si vous avez sélectionné **Redémarrer si nécessaire** ou **Toujours redémarrer**. L'option permet le redémarrage automatique de la ressource.
Si un utilisateur est connecté au terminal, le terminal sera redémarré automatiquement après :	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez la période après laquelle la ressource sera redémarrée automatiquement. L'utilisateur connecté à la ressource sera informé d'un redémarrage automatique en attente et de l'heure à laquelle il se produira. De cette manière, les utilisateurs peuvent enregistrer leur travail et se préparer au redémarrage.
Notifications supplémentaires	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Sélectionnez cette option si vous souhaitez que l'utilisateur connecté à la ressource reçoive des rappels répétés à propos d'un redémarrage en attente avant la fin de la période sélectionnée. La planification des notifications dépend de la période sélectionnée et passe en mode de compte à rebours à l'approche de l'heure de redémarrage. De cette manière, les utilisateurs sont informés du redémarrage et peuvent s'y préparer. Les notifications sont déclenchées par la mise à jour ou le déploiement du logiciel, et sont envoyées aux heures suivantes. **Remarque** Le moment de la première notification coïncide avec la période sélectionnée. • 24 heures avant le redémarrage automatique. • 8 heures avant le redémarrage automatique. • 4 heures avant le redémarrage automatique. • 1 h avant le redémarrage automatique. • 30 minutes avant le redémarrage. • 15 minutes avant le redémarrage. • 5 minutes avant le redémarrage automatique. La dernière notification utilisateur ne peut être ni fermée ni ignorée.
Si aucun utilisateur n'est connecté au terminal, redémarrer le terminal	Cette option est disponible si vous avez sélectionné l'option **Planifier un redémarrage automatique**. Si vous sélectionnez cette option et si aucun utilisateur n'est connecté à la ressource, la ressource est redémarrée immédiatement, sans que la période sélectionnée avant le

© Acronis International GmbH, 2003-2026

Option	Description
immédiatement	redémarrage automatique soit entièrement écoulée.

c. Cliquez sur **Terminé**.

9. Pour planifier l'exécution du plan, procédez comme suit :

a. Cliquez sur le champ **Planifier**.

b. Dans l'écran **Planifier**, champ **Planifiez l'exécution de la tâche à l'aide des événements suivants**, sélectionnez l'événement qui démarrera le plan.

Option	Description
Ex. une fois	Si vous sélectionnez cette option, vous devez configurer la date et l'heure d'exécution du plan.
Planifier selon l'horaire	Si vous sélectionnez cette option, vous pouvez configurer des plans qui s'exécutent toutes les heures, tous les jours ou tous les mois. Si vous souhaitez que cette planification soit effective uniquement pendant une période spécifique, cochez la case **Exécuter sur une plage de dates**, puis configurez la période (en jours) pendant laquelle le plan planifié s'exécutera.
Lorsque l'utilisateur se connecte au système	Si vous sélectionnez cette option, le plan s'exécutera lorsqu'un utilisateur spécifique ou n'importe quel utilisateur se connectera à la ressource cible.
Lorsqu'un utilisateur se déconnecte du système	Si vous sélectionnez cette option, le plan s'exécutera lorsqu'un utilisateur spécifique ou n'importe quel utilisateur se déconnectera de la ressource cible.
Au démarrage du système	Si vous sélectionnez cette option, le plan s'exécutera lorsque la ressource cible démarrera.
Lorsque le système est arrêté	Si vous sélectionnez cette option, le plan s'exécutera lorsque la ressource cible s'arrêtera.
Lorsque le système est en ligne	Si vous sélectionnez cette option, le plan s'exécutera lorsque la ressource cible sera en ligne.

c. Dans la section **Conditions de démarrage**, sélectionnez toutes les conditions qui doivent être remplies simultanément pour que le plan démarre.

© Acronis International GmbH, 2003-2026

Condition	Description
Exécuter uniquement si la ressource est en ligne	Cette condition est remplie lorsque la ressource cible est connectée à Internet.
L'utilisateur est inactif	Cette condition est remplie lorsqu'un écran de veille s'exécute sur l'ordinateur ou si l'ordinateur est verrouillé.
Utilisateur déconnecté	Si vous sélectionnez cette condition, vous pouvez reporter un plan planifié jusqu'à ce que l'utilisateur de la ressource cible se déconnecte.
Compris dans un intervalle de temps	Si vous sélectionnez cette condition, vous devez définir l'intervalle de temps pendant lequel le plan peut s'exécuter.
Économiser de la batterie	Si vous sélectionnez cette condition, vous pouvez vous assurer que le plan ne sera pas interrompu en raison d'une batterie faible. Les options suivantes sont disponibles : • **Ne pas démarrer lors d'une alimentation sur batterie** Le plan démarrera uniquement si l'ordinateur est connecté à une source d'alimentation. • **Démarrer pendant l'alimentation sur batterie si le niveau de batterie est supérieur à** Le plan démarrera si l'ordinateur est connecté à une source d'alimentation ou si le niveau de batterie est supérieur à la valeur spécifiée.
Ne pas démarrer pendant une connexion mesurée	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si la ressource cible accède à Internet via une connexion mesurée.
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si la ressource cible est connectée à l'un des réseaux sans fil spécifiés. Pour utiliser cette condition, vous devez indiquer le SSID du réseau interdit. La restriction s'applique à tous les réseaux qui contiennent le nom spécifié comme sous-chaîne dans leur nom, quelle que soit la casse. Par exemple, si vous spécifiez `téléphone` comme nom de réseau, le plan ne démarrera pas lorsque le terminal sera connecté à l'un des réseaux suivants : `Téléphone de Jean`, `téléphone_wifi` ou `mon_wifi_TÉLÉPHONE`.
Vérifier l'adresse IP du terminal	Si vous sélectionnez cette condition, le plan ne s'exécutera pas si l'une des adresses IP de la ressource cible se trouve au sein ou en dehors de la plage d'adresses IP spécifiée. Les options suivantes sont disponibles : • **Démarrer si en dehors de la plage d'adresses IP** • **Démarrer si dans la plage d'adresses IP** Prend en charge uniquement les adresses IPv4.

© Acronis International GmbH, 2003-2026

Condition	Description
Si les conditions de démarrage ne sont pas remplies, exécuter quand même la tâche	Utilisez cette option pour définir l'intervalle de temps après lequel le plan sera exécuté, quelles que soient les autres conditions. Le plan démarrera dès que les autres conditions seront remplies ou dès que la période spécifiée sera écoulée. Cette option n'est pas disponible si vous avez sélectionné l'option **Exécuter une fois** pour la planification.

d. Cliquez sur **Terminé**.

10. Cliquez sur **Créer**.

Ajout d'une ressource à un plan de déploiement de logiciel

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez ajouter des ressources à un plan de déploiement de logiciel après la création de ce plan.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour ajouter une ressource à un plan de déploiement de logiciel

Depuis Plans de déploiement de logiciels

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de déploiement de logiciels**.
2. Cliquez sur le plan de déploiement de logiciels.
3. Selon que le plan est déjà appliqué ou pas à une ressource, effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter des ressources**, si le plan n'a encore été appliqué à aucune ressource.
   - Cliquez sur **Gérer les ressources** si le plan n'a été appliqué à aucune ressource.
4. Sélectionnez une ressource dans la liste, puis cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de déploiement de logiciel.
3. Cliquez sur **Protection**, puis sur **Ajouter un plan**.

© Acronis International GmbH, 2003-2026

4. Dans **Sélectionnez un plan dans la liste ci-dessous**, sélectionnez **Déploiement de logiciel** pour n'afficher que les plans de déploiement de logiciel.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

Suppression de ressources de plans de déploiement de logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Vous pouvez supprimer des ressources ajoutées à un plan de déploiement de logiciel.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Pour supprimer des ressources d'un plan de déploiement de logiciel

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de déploiement de logiciels**.
2. Cliquez sur le plan de déploiement de logiciels.
3. Cliquez sur **Gérer les ressources**.
4. Sélectionnez une ou plusieurs ressources que vous souhaitez supprimer du plan de déploiement de logiciel, puis cliquez sur **Supprimer**.
5. Cliquez sur **Terminé**.
6. Cliquez sur **Enregistrer**.

Opérations supplémentaires réalisables avec les plans de déploiement de logiciels

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Dans l'écran **Plans de déploiement de logiciels**, vous pouvez effectuer les opérations supplémentaires suivantes avec les plans de déploiement de logiciels : afficher les détails, modifier, afficher les activités, afficher les alertes, renommer, cloner, exporter, importer et supprimer.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Vous avez l'un des rôles suivants pour Cyber Protection : administrateur d'entreprise ou cyberadministrateur.

Afficher les détails

© Acronis International GmbH, 2003-2026

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour afficher les détails d'un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Afficher les détails**.

Modifier

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour modifier un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Modifier**.

Activités

Pour afficher les activités relatives à un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Activités**.
3. Cliquez sur une activité pour visualiser plus de détails la concernant.

Alertes

Pour afficher les alertes

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Alertes**.

Renommer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour renommer un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Renommer**.
3. Saisissez le nouveau nom du plan, puis cliquez sur **Poursuivre**.

Cloner

© Acronis International GmbH, 2003-2026

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour cloner un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Cloner**.
3. Cliquez sur **Créer**.

Exporter

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour exporter un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.
2. Cliquez sur **Exporter**.
   La configuration du plan est exportée au format JSON vers la machine locale.

Importer

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Un fichier JSON avec la configuration du plan est disponible sur l'ordinateur à partir duquel vous êtes connecté à la console.

Pour importer un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur **Importer un plan**.
2. Dans la fenêtre qui s'ouvre, parcourez jusqu'au fichier JSON.
3. Cliquez sur le fichier, puis cliquez sur **Ouvrir**.
   Le plan de déploiement du logiciel apparaît à l'écran. Vous pouvez maintenant l'appliquer aux ressources.

Supprimer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour supprimer un plan de déploiement de logiciel

1. Dans l'écran **Plans de déploiement de logiciels**, cliquez sur l'icône **Plus d'actions** du plan de déploiement de logiciel.

© Acronis International GmbH, 2003-2026

2. Cliquez sur **Supprimer**.
3. Sélectionnez **Je confirme**, puis cliquez sur **Supprimer**.

Connexion à des ressources de type Bureau ou assistance à distance

La fonctionnalité de bureau et assistance à distance permet de se connecter facilement à des ressources de votre organisation afin de les contrôler à distance ou d'intervenir à distance dans le cadre d'opérations d'assistance.

À partir de décembre 2022, la fonctionnalité prend en charge les protocoles NEAR, RDP et Partage d'écran Apple. Pour plus d'informations, voir "Protocoles de connexion à distance" (p. 1464).

Vous pouvez utiliser la fonctionnalité Bureau à distance pour effectuer les tâches suivantes.

- Connectez-vous à des ressources Windows, macOS et Linux distantes en utilisant NEAR en mode affichage seul.
- Vous connecter à des ressources Windows à l'aide du protocole RDP.
- Connectez-vous à des ressources macOS distantes en utilisant le partage d'écran Apple en mode affichage seul ou en mode rideau.
- Vous connecter à des ressources gérées et les contrôler à distance à l'aide de connexions à distance dans le cloud.
- Vous connecter à des ressources non gérées et les contrôler à distance à l'aide de connexions à distance directes.
- Vous connecter à des ressources distantes non gérées à l'aide de Acronis Assistance rapide.
- Vous connecter à des ressources distantes à l'aide de différentes méthodes d'authentification : avec identifiants de la ressource distante, en demandant l'autorisation d'observation ou de contrôle, ou avec un code d'accès (pour Assistance rapide).
- Observer simultanément plusieurs écrans dans la vue multiple.
- Enregistrer des sessions distantes (lors de la connexion via NEAR).
- Visualiser le rapport d'historique des sessions.

Vous pouvez utiliser la fonctionnalité d'assistance à distance pour effectuer les tâches suivantes.

- Vous connecter à des ressources Windows, macOS et Linux distantes à l'aide du protocole NEAR en mode de contrôle.
- Connectez-vous à des ressources macOS distantes en utilisant le partage d'écran Apple en mode contrôle.
- Fournir une assistance à distance à des ressources à l'aide de connexions à distance dans le cloud.
- Transférer des fichiers entre les ressources locales et distantes.

© Acronis International GmbH, 2003-2026

- Effectuer des actions de gestion de base sur la ressource distance : redémarrer, arrêter, veille, vider la corbeille et déconnecter l'utilisateur distant.
- Surveiller la ressource distante en effectuant régulièrement des captures d'écran de son bureau.

Important
Pour activer la fonctionnalité complète de bureau et assistance à distance pour une ressource gérée, vous devez configurer et appliquer un plan de gestion à distance à la ressource. Vous ne pouvez appliquer qu'un seul plan de gestion à distance par ressource, mais selon vos besoins, vous pouvez configurer différents plans de gestion à distance et les appliquer à différentes ressources.

De cette manière, vous pouvez contrôler la disponibilité des fonctionnalités dans les plans de gestion à distance pour qu'elle corresponde aux licences qui sont affectées à vos ressources.

Pour plus d'informations sur les plans de gestion à distance et sur leur utilisation, voir "Plans de gestion à distance" (p. 1467).

Remarque
La fonctionnalité de bureau et assistance à distance nécessite les éléments suivants :

- une installation unique de Connect Client sur la ressource de gestion (hôte). Lorsque vous essayez pour la première fois d'effectuer une action à distance (contrôle ou assistance à distance) sur une ressource cible, le système vous invite à télécharger le client. Vous pouvez également télécharger Connect Client à partir de la fenêtre **Téléchargements** dans la console Protection. Pour plus d'informations sur les paramètres que vous pouvez configurer, voir "Configuration des paramètres Connect Client" (p. 1509).
- une installation de Agent Connect sur les ressources gérées. Agent Connect est un module faisant partie de l'agent Protection à partir de la version 15.0.31266.
- Pour les ressources distantes macOS, les autorisations système requises doivent être accordées à Agent Connect. Pour plus d'informations, voir "Installation des agents de protection sous macOS" (p. 71).
- l'exécution de l'application Acronis Assistance rapide sur les ressources non gérées. Vous pouvez télécharger Acronis Assistance rapide à partir du site Web.

Pour plus d'informations sur les plates-formes prises en charge par chaque composant de bureau à distance et d'assistance, reportez-vous à "Systèmes d'exploitation pris en charge pour le bureau à distance et l'assistance" (p. 1463).

Fonctionnalités prises en charge de bureau et assistance à distance

Le tableau suivant fournit plus d'informations sur les fonctionnalités prises en charge de la fonctionnalité bureau à distance et assistance en fonction de la licence.

© Acronis International GmbH, 2003-2026

Fonctionnalité	Protection standard (mode de licence basé sur le service)	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Assistance à distance via RDP pour Windows	Non	Non
Partager une connexion à distance avec les utilisateurs	Non	Non
Connexions à distance		
Actions à distance	Oui	Oui
Sélection d'une session pour Windows/macOS/Linux à laquelle se connecter	Non	Oui
Connexion directe via RDP et Partage d'écran Apple	Non	Oui
Contrôle multifenêtre	Non	Oui
Modes de connexion : Contrôle/Affichage seul/Rideau	Non	Oui
Prise en charge d'identifiants communs pour les connexions à distance	Oui	Oui
Connexions simultanées par technicien		
via RDP	Oui	Oui
via NEAR	Non	Oui
Transfert et partage de fichiers		
depuis Windows vers Windows/macOS/Linux	Non	Oui
depuis macOS vers Windows/macOS/Linux	Non	Oui
depuis Linux vers Windows/macOS/Linux	Non	Oui
Connexion via l'application Assistance rapide		
depuis Windows vers	Non	Oui

© Acronis International GmbH, 2003-2026

Fonctionnalité	Protection standard (mode de licence basé sur le service)	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Windows/macOS/Linux		
depuis macOS vers Windows/macOS/Linux	Non	Oui
depuis Linux vers Windows/macOS/Linux	Non	Oui
Connexions à distance via des protocoles		
Connexion à distance via NEAR		
depuis Windows vers Windows/macOS/Linux	Non	Oui
depuis macOS vers Windows/macOS/Linux	Non	Oui
depuis Linux vers Windows/macOS/Linux	Non	Oui
Connexion à distance via RDP (client du bureau à distance)		
depuis Windows vers Windows	Oui	Oui
depuis macOS vers Windows	Oui	Oui
depuis Linux vers Windows	Oui	Oui
Connexion à distance via RDP (client Web)		
depuis Windows vers Windows	Oui	Oui
depuis macOS vers Windows	Oui	Oui
depuis Linux vers Windows	Oui	Oui
Connexion à distance via Partage d'écran Apple		
depuis Windows/macOS/Linux vers macOS	Non	Oui
Gestion de session		
Enregistrement de session	Non	Oui
Reporting et surveillance		

© Acronis International GmbH, 2003-2026

Fonctionnalité	Protection standard (mode de licence basé sur le service)	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Historique des sessions et recherche	Non	Oui
Transmission de captures d'écran	Non	Oui
Échange de fichiers via le Presse-papiers	Non	Oui

Systèmes d'exploitation pris en charge pour le bureau à distance et l'assistance

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par chaque composant de la fonctionnalité de bureau et assistance à distance.

Composant Bureau à distance	Plates-formes prises en charge
Connect Client	• Windows 7 ou version ultérieure • macOS 10.13 ou version ultérieure • Linux : openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Agent Connect	• Windows 7 ou version ultérieure • Windows Server 2008 R2 ou version ultérieure • macOS 10.13 ou version ultérieure • Linux : Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) - 19.04 (Disco Dingo) Debian 9, 10 CentOS 8

© Acronis International GmbH, 2003-2026

Composant Bureau à distance	Plates-formes prises en charge
	openSUSE 15.1
Acronis Assistance rapide	• Windows 7 ou version ultérieure • Windows Server 2008 R2 ou version ultérieure • macOS 10.13 ou version ultérieure • Linux : Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) - 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protocoles de connexion à distance

La fonctionnalité Bureau à distance utilise les protocoles suivants pour les connexions à distance.

NEAR

Le protocole NEAR est un protocole hautement sécurisé développé par Acronis et ayant les caractéristiques suivantes.

- #### H.264

  Le protocole NEAR implémente trois modes de qualité : **Lisse**, **Équilibré** et **Net**. En mode **Lisse**, le protocole NEAR utilise le codage matériel H.264 sous macOS et Windows afin de coder l'image du bureau. Par ailleurs, le basculement vers le codeur logiciel si le codeur matériel n'est pas disponible. La taille de l'image est actuellement limitée à la résolution Full HD (1 920 x 1 080).

- #### Codec adaptatif

  En modes de qualité **Équilibré** et **Net**, le protocole NEAR utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264.

  En mode **Équilibré**, la qualité de l'image est ajustée automatiquement en fonction de vos conditions réseau et la fréquence d'images actuelle est conservée.

  En mode **Net**, la qualité d'image est la meilleure. Toutefois, le nombre d'images par seconde peut être réduit si votre réseau, votre processeur ou votre carte vidéo sont surchargés.

  Le codec adaptatif utilise OpenCL sous Windows et macOS lorsqu'il est disponible dans les pilotes graphiques.

- #### Transfert audio

  Le protocole NEAR peut capturer le son de l'ordinateur distant et le transférer à l'hôte. Pour plus d'informations sur l'activation de la redirection du son à distance sous Windows, macOS et Linux,

© Acronis International GmbH, 2003-2026

voir "Redirection du son à distance" (p. 1465).

- Différentes options de connexion

  Vous pouvez utiliser les méthodes suivantes pour vous connecter à la ressource distante.

  Code d'accès : l'utilisateur qui est connecté à la ressource distante exécute Assistance rapide et vous indique le code d'accès. Grâce à cette méthode, vous vous connectez toujours à la session de l'utilisateur connecté.

  Identifiants de la ressource : connectez-vous à la ressource distante à l'aide des identifiants d'administrateur qui sont enregistrés dans la ressource.

  Demander l'autorisation d'observation ou de contrôle : le système demandera à l'utilisateur connecté à la ressource distante d'autoriser ou de refuser la connexion.

- Sécurité

  Vos données sont toujours chiffrées dans les deux sens avec le chiffrement AES dans NEAR.

RDP

Le protocole RDP (Remote Desktop Protocol) est un protocole propriétaire développé par Microsoft qui permet d'établir une connexion réseau à un ordinateur Windows distant.

Partage d'écran Apple

Le partage d'écran Apple est un client VNC d'Apple inclus dans macOS depuis la version 10.5.

Redirection du son à distance

Connect Client prend en charge la diffusion du son via le protocole de connexion NEAR. Pour plus d'informations sur NEAR, reportez-vous à "Protocoles de connexion à distance" (p. 1464).

Redirection du son d'une ressource distante Windows

Pour les ressources Windows, le son distant devrait être transmis automatiquement. Assurez-vous que des terminaux de sortie audio (haut-parleurs ou casque) sont connectés à la ressource distante.

Redirection du son d'une ressource distante macOS

Pour activer la redirection du son depuis une ressource macOS, vérifiez les points suivants :

- L'agent Protection est installé sur la ressource.
- La ressource dispose d'un pilote de capture audio.
- La ressource utilise le protocole NEAR pour les connexions à distance.

© Acronis International GmbH, 2003-2026

Remarque
Pour macOS 10.15 Catalina, l'autorisation d'accès au microphone doit être accordée à Agent Connect. Pour plus d'informations sur l'autorisation d'accès à Agent Connect, reportez-vous à "Attribution des autorisations système requises à Agent Connect" (p. 57).

L'agent utilise les pilotes de capture audio suivants : Soundflower ou Blackhole.

Le processus d'installation sur les dernières versions est décrit sur la page wiki de Blackhole : https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Remarque
Connect Client ne prend actuellement en charge que la version à 2 canaux de Blackhole.

Si Homebrew est installé sur la ressource, vous pouvez installer Blackhole en exécutant la commande suivante :

```
brew install --cask blackhole-2ch
```

Remarque
Si le son d'une ressource macOS distante est redirigé, l'utilisateur qui est connecté à la ressource distante n'entendra pas le son.

Redirection du son d'une ressource distante Linux

La redirection du son à distance devrait s'effectuer automatiquement sur la plupart des distributions Linux. Si la redirection du son à distance ne fonctionne pas par défaut, installez le pilote PulseAudio en exécutant la commande suivante :

```
sudo apt-get install pulseaudio
```

Connexions à des ressources distantes de type bureau ou assistance à distance

La fonctionnalité de bureau et assistance à distance propose différentes méthodes permettant d'établir des connexions à distance directes ou dans le cloud à vos ressources.

Les connexions directes sont établies par TCP/IP sur un réseau local entre Connect Client et la ressource distante sur laquelle aucun agent n'est installé. Elles ne nécessitent aucun accès Internet.

Les connexions dans le cloud sont établies entre Connect Client et l'agent ou Assistance rapide sur la ressource via Acronis Cloud.

Le tableau suivant fournit des informations complémentaires sur les options de connexion dans le cloud.

© Acronis International GmbH, 2003-2026

Connexion dans le cloud	Option Connexion dans le cloud	Mode d'affichage	Action à distance prise en charge	Disponible pour
via NEAR	de Connect Client à Agent Connect de Connect Client à Assistance rapide	Contrôle Affichage seul	Bureau à distance Assistance à distance	ressources gérées
via RDP	de Connect Client à Agent Connect depuis le client Web vers Agent Connect	Contrôle	Bureau à distance	ressources gérées
via Partage d'écran Apple	de Connect Client à Agent Connect	Contrôle Affichage seul Rideau	Bureau à distance Assistance à distance	ressources gérées

Le tableau suivant fournit des informations complémentaires sur les options de connexion directe.

Connexion directe	Option Connexion directe	Action à distance prise en charge	Disponible pour
via RDP	depuis Connect Client vers un serveur RDP	Bureau à distance	ressources non gérées
via Partage d'écran Apple	de Connect Client vers le serveur Partage d'écran Apple	Bureau à distance Assistance à distance	ressources non gérées

Plans de gestion à distance

Les plans de gestion à distance sont des plans que vous appliquez à l'agent Protection afin d'activer et de configurer la fonctionnalité de bureau et assistance à distance sur vos ressources gérées.

Si aucun plan de gestion à distance n'est appliqué à une ressource, la fonctionnalité de bureau et assistance à distance est limitée aux actions à distance (redémarrage, arrêt, mise en veille, vidage de la corbeille et déconnexion de l'utilisateur distant).

Remarque
La disponibilité de la fonctionnalité et des paramètres que vous pouvez configurer dans le plan de gestion à distance dépend de la licence qui est affectée à la ressource.

Création d'un plan de gestion à distance

Vous pouvez créer un plan de gestion à distance, puis l'affecter à une ressource afin de configurer la fonctionnalité de bureau et assistance à distance sur la ressource gérée.

© Acronis International GmbH, 2003-2026

Remarque
La disponibilité des paramètres du plan de gestion à distance dépend de la licence qui est affectée à la ressource.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Si le terminal géré est joint à Entra ID (anciennement Azure AD) et que vous souhaitez vous y connecter à l'aide du protocole NEAR, voir cet article de la base de connaissances.

Pour créer un plan de gestion à distance

Depuis les plans de gestion à distance

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Créez un plan de gestion à distance en utilisant l'une des deux options.
   - Si la liste ne comprend aucun plan de gestion à distance, cliquez sur **Créer**.
   - Si la liste comprend des plans de gestion à distance, cliquez sur **Création d'un plan**.
3. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **Poursuivre**.
4. Cliquez sur **Protocoles de connexion** et activez les protocoles que vous souhaitez voir disponibles dans ce plan de gestion à distance pour les connexions à distance - NEAR, RDP ou Partage d'écran Apple.
5. [Facultatif] Pour le protocole NEAR, dans la section **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible pour
Verrouiller la ressource lorsque l'utilisateur se déconnecte d'une session de console	Si vous sélectionnez ce paramètre, la ressource distante sera verrouillée lorsque vous vous déconnecterez de la session de console.	Windows, macOS
Autoriser un seul utilisateur à la fois à se connecter via NEAR ou à transférer des fichiers	Si vous sélectionnez ce paramètre, les connexions à l'aide du protocole NEAR et les transferts de fichiers ne seront pas possibles pendant qu'une connexion à distance à la ressource est active.	Windows, macOS, Linux
Autoriser l'administrateur de la ressource à se	Si vous sélectionnez ce paramètre, l'administrateur	Windows, macOS

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible pour
connecter à toute session d'utilisateur non-administrateur	est autorisé à se connecter à une session utilisateur standard sur la ressource. Si les options **Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur** et **Autoriser la création d'une session système** sont toutes deux désélectionnées, vous ne pourrez vous connecter qu'aux sessions administrateur actives sur les ressources macOS distantes.	
Autoriser la création d'une session système	Si vous sélectionnez ce paramètre, lors de l'établissement de connexions à distance, l'administrateur se connectera à une nouvelle session au lieu d'utiliser l'une des sessions actives.	macOS
Autoriser la synchronisation du Presse-papiers	Si vous sélectionnez ce paramètre, vous pourrez transférer des données entre votre Presse-papiers et celui de la ressource distante. Par exemple, vous pourrez copier du texte d'un fichier sur la ressource distante, puis le coller dans un fichier sur votre ressource, et inversement.	Windows, macOS, Linux

6. Cliquez sur **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description
Afficher si la ressource est contrôlée à distance	Si vous sélectionnez ce paramètre, une notification s'affichera sur le bureau de la ressource distante s'il existe une connexion Bureau à distance active à la ressource.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Demander l'autorisation de l'utilisateur à effectuer des captures d'écran de la ressource	Si vous sélectionnez ce paramètre, l'utilisateur de la ressource distante sera informé lorsque l'administrateur demande la transmission d'une capture d'écran depuis cette ressource.

7. Cliquez sur **Gestion des ressources**, sélectionnez les fonctionnalités que vous souhaitez mettre à la disposition des ressources distantes, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible sur
Transfert de fichiers	Permet les transferts de fichiers entre les ressources locales et distantes.	Windows, macOS, Linux
Transmission de captures d'écran	Permet la transmission des captures d'écran du bureau de la ressource distante à la console Cyber Protect.	Windows, macOS, Linux
Suivi de la géolocalisation	Permet de suivre l'emplacement de la ressource lorsque les services de localisation sont activés dans les paramètres du système d'exploitation de la ressource.	Windows, macOS, Linux
Chat	Active le chat en direct entre un technicien connecté à la console Cyber Protect et un utilisateur connecté à la ressource distante.	Windows, macOS

8. Cliquez sur **Paramètres d'affichage**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Remarque
Les **Paramètres d'affichage** sont uniquement disponibles pour les connexions via NEAR.

Paramètre	Description	Disponible sur
Utiliser la déduplication de bureau pour effectuer la capture d'un bureau	La duplication de bureau est l'une des méthodes de capture d'écran de Windows. Dans certains	Windows

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible sur
	environnements, l'opération peut être instable. Si vous n'utilisez pas la déduplication de bureau, vous utiliserez plutôt la méthode de base (BitBlt) qui est plus lente, mais plus stable.	
Utiliser l'accélération OpenCL	L'accélération OpenCL peut accélérer le codec adaptatif qui est responsable du mode de qualité **Équilibré** en exécutant des calculs sur le processeur graphique. Cette option nécessite l'installation d'un pilote OpenCL sur la ressource Linux distante. Le codec adaptatif utilise OpenCL sous macOS et Windows s'il est disponible dans vos pilotes graphiques.	Linux
Utiliser le codage matériel H.264	Le protocole NEAR prend en charge trois modes de qualité : **Lisse**, **Équilibré** et **Net**. Le mode **Lisse** utilise le codage matériel H.264 pour coder l'image du bureau. Le mode **Équilibré** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité de l'image est ajustée automatiquement en fonction de vos conditions réseau et la fréquence d'images actuelle est conservée. Le mode **Net** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en	Windows, macOS

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible sur
	32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité d'image est toujours la meilleure. Toutefois, le nombre d'images par seconde peut être réduit si votre réseau ou processeur/carte vidéo sont surchargés.	

9. Cliquez sur **Boîte à outils**, cochez ou décochez les cases à cocher pour activer ou désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible sur
Afficher les derniers utilisateurs connectés	Si vous sélectionnez ce paramètre, les informations sur les utilisateurs s'étant connectés en dernier aux ressources seront visibles dans les détails de la ressource. Pour plus d'informations sur les utilisateurs s'étant connectés en dernier, voir "Consultation du dernier utilisateur connecté" (p. 482).	Windows, macOS, Linux
Interface de ligne de commande distante	Ce paramètre active l'accès distant à l'interface de ligne de commande du terminal géré.	Windows, macOS

10. [Facultatif] Pour ajouter des ressources au plan :
    a. Cliquez sur **Ajouter des ressources**.
    b. Sélectionnez les ressources, puis cliquez sur **Ajouter**.
    c. Si vous avez des problèmes de compatibilité à résoudre, suivez la procédure décrite dans "Résolution des problèmes de compatibilité" (p. 253).
11. Cliquez sur **Créer**.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de gestion à distance.
3. Cliquez sur **Protection**, puis sur **Ajouter un plan**.

© Acronis International GmbH, 2003-2026

4. Cliquez sur **Création d'un plan**, puis sélectionnez **Gestion à distance**.
5. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **Poursuivre**.
6. Cliquez sur **Protocoles de connexion** et activez les protocoles que vous souhaitez voir disponibles dans ce plan de gestion à distance pour les connexions à distance - NEAR, RDP ou Partage d'écran Apple.
7. [Facultatif] Pour le protocole NEAR, dans la section **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible pour
Verrouiller la ressource lorsque l'utilisateur se déconnecte d'une session de console	Si vous sélectionnez ce paramètre, la ressource distante sera verrouillée lorsque vous vous déconnecterez de la session de console.	Windows, macOS
Autoriser un seul utilisateur à la fois à se connecter via NEAR ou à transférer des fichiers	Si vous sélectionnez ce paramètre, les connexions à l'aide du protocole NEAR et les transferts de fichiers ne seront pas possibles pendant qu'une connexion à distance à la ressource est active.	Windows, macOS, Linux
Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur	Si vous sélectionnez ce paramètre, l'administrateur est autorisé à se connecter à une session utilisateur standard sur la ressource. Si les options **Autoriser l'administrateur de la ressource à se connecter à toute session d'utilisateur non-administrateur** et **Autoriser la création d'une session système** sont toutes deux désélectionnées, vous ne pourrez vous connecter qu'aux sessions administrateur actives sur les ressources macOS distantes.	Windows, macOS
Autoriser la création d'une session système	Si vous sélectionnez ce paramètre, lors de	macOS

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible pour
	l'établissement de connexions à distance, l'administrateur se connectera à une nouvelle session au lieu d'utiliser l'une des sessions actives.	
Autoriser la synchronisation du Presse-papiers	Si vous sélectionnez ce paramètre, vous pourrez transférer des données entre votre Presse-papiers et celui de la ressource distante. Par exemple, vous pourrez copier du texte d'un fichier sur la ressource distante, puis le coller dans un fichier sur votre ressource, et inversement.	Windows, macOS, Linux

8. Cliquez sur **Paramètres de sécurité**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description
Afficher si la ressource est contrôlée à distance	Si vous sélectionnez ce paramètre, une notification s'affichera sur le bureau de la ressource distante s'il existe une connexion Bureau à distance active à la ressource.
Demander l'autorisation de l'utilisateur à effectuer des captures d'écran de la ressource	Si vous sélectionnez ce paramètre, l'utilisateur de la ressource distante sera informé lorsque l'administrateur demande la transmission d'une capture d'écran depuis cette ressource.

9. Cliquez sur **Gestion des ressources**, sélectionnez les fonctionnalités que vous souhaitez mettre à la disposition des ressources distantes, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible sur
Transfert de fichiers	Permet les transferts de fichiers entre les ressources locales et distantes.	Windows, macOS, Linux
Transmission de captures d'écran	Permet la transmission des captures d'écran du bureau de la ressource distante à la	Windows, macOS, Linux

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible sur
	console Cyber Protect.	
Suivi de la géolocalisation	Permet de suivre l'emplacement de la ressource lorsque les services de localisation sont activés dans les paramètres du système d'exploitation de la ressource.	Windows, macOS, Linux
Chat	Active le chat en direct entre un technicien connecté à la console Cyber Protect et un utilisateur connecté à la ressource distante.	Windows, macOS

10. Cliquez sur **Paramètres d'affichage**, cochez ou désélectionnez les cases afin d'activer ou de désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Remarque
Les **Paramètres d'affichage** sont uniquement disponibles pour les connexions via NEAR.

Paramètre	Description	Disponible sur
Utiliser la déduplication de bureau pour effectuer la capture d'un bureau	La duplication de bureau est l'une des méthodes de capture d'écran de Windows. Dans certains environnements, l'opération peut être instable. Si vous n'utilisez pas la déduplication de bureau, vous utiliserez plutôt la méthode de base (BitBlt) qui est plus lente, mais plus stable.	Windows
Utiliser l'accélération OpenCL	L'accélération OpenCL peut accélérer le codec adaptatif qui est responsable du mode de qualité **Équilibré** en exécutant des calculs sur le processeur graphique. Cette option nécessite l'installation d'un pilote OpenCL sur la ressource Linux distante.	Linux

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible sur
	Le codec adaptatif utilise OpenCL sous macOS et Windows s'il est disponible dans vos pilotes graphiques.	
Utiliser le codage matériel H.264	Le protocole NEAR prend en charge trois modes de qualité : **Lisse**, **Équilibré** et **Net**. Le mode **Lisse** utilise le codage matériel H.264 pour coder l'image du bureau. Le mode **Équilibré** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité de l'image est ajustée automatiquement en fonction de vos conditions réseau et la fréquence d'images actuelle est conservée. Le mode **Net** utilise le codec adaptatif, ce qui fournit la meilleure qualité d'image en 32 bits par rapport au mode vidéo utilisé par le protocole H.264. La qualité d'image est toujours la meilleure. Toutefois, le nombre d'images par seconde peut être réduit si votre réseau ou processeur/carte vidéo sont surchargés.	Windows, macOS

11. Cliquez sur **Boîte à outils**, cochez ou décochez les cases à cocher pour activer ou désactiver le paramètre correspondant, puis cliquez sur **Terminé**.

Paramètre	Description	Disponible sur
Afficher les derniers utilisateurs connectés	Si vous sélectionnez ce paramètre, les informations sur les utilisateurs s'étant	Windows, macOS, Linux

© Acronis International GmbH, 2003-2026

Paramètre	Description	Disponible sur
	connectés en dernier aux ressources seront visibles dans les détails de la ressource. Pour plus d'informations sur les utilisateurs s'étant connectés en dernier, voir "Consultation du dernier utilisateur connecté" (p. 482).	
Interface de ligne de commande distante	Ce paramètre active l'accès distant à l'interface de ligne de commande du terminal géré.	Windows, macOS

12. Cliquez sur **Créer**.

Ajout d'une ressource à un plan de gestion à distance

Vous pouvez ajouter des ressources à un plan de gestion à distance après la création de ce plan.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour ajouter une ressource à un plan de gestion à distance

Depuis les plans de gestion à distance

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Cliquez sur le plan de gestion à distance.
3. Selon que le plan est déjà appliqué ou pas à une ressource, effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter des ressources**, si le plan n'a encore été appliqué à aucune ressource.
   - Cliquez sur **Gérer les ressources** si le plan n'a été appliqué à aucune ressource.
4. Sélectionnez une ressource dans la liste, puis cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de gestion à distance.
3. Cliquez sur **Protection**, puis sur **Ajouter un plan**.

© Acronis International GmbH, 2003-2026

4. Dans **Sélectionnez un plan dans la liste ci-dessous**, sélectionnez **Gestion à distance** pour n'afficher que les plans de gestion à distance.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

Suppression de ressources d'un plan de gestion à distance

En fonction de vos besoins, vous pouvez supprimer des ressources d'un plan de gestion à distance.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour supprimer des ressources d'un plan de gestion à distance

1. Dans la console Cyber Protect, accédez à **Gestion** > **Plans de gestion à distance**.
2. Cliquez sur le plan de gestion à distance.
3. Cliquez sur **Gérer les ressources**.
4. Sélectionnez une ou plusieurs ressources que vous souhaitez supprimer du plan de gestion à distance, puis cliquez sur **Supprimer**.
5. Cliquez sur **Terminé**.
6. Cliquez sur **Enregistrer**.

Autres actions pouvant être effectuées dans le cadre de plans de gestion à distance existants

Depuis l'écran **Plans de gestion à distance**, vous pouvez effectuer les actions supplémentaires suivantes avec les plans de gestion à distance : afficher les détails, modifier, afficher les activités, afficher les alertes, renommer, activer, désactiver, cloner, exporter, importer, ajouter aux favoris, définir comme plan par défaut et supprimer.

Afficher les détails

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour afficher les détails d'un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Afficher les détails**.

Modifier

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

© Acronis International GmbH, 2003-2026

Pour modifier un plan

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Modifier**.
3. Modifiez les paramètres, puis cliquez sur **Enregistrer**.

Activités

Pour afficher les activités relatives à un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Activités**.
3. Cliquez sur une activité pour visualiser plus de détails la concernant.

Alertes

Pour afficher les alertes

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Alertes**.

Renommer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Renommer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Renommer**.
3. Saisissez le nouveau nom du plan, puis cliquez sur **Poursuivre**.

Activer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Activer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Activer**.

Désactiver

Prérequis

© Acronis International GmbH, 2003-2026

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Désactiver un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Désactiver**.

Cloner

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour cloner un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Cloner**.
3. Cliquez sur **Créer**.

Exporter

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour exporter un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Exporter**.
   La configuration du plan est exportée au format JSON vers la machine locale.

Importer

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Un fichier JSON avec la configuration du plan est disponible sur l'ordinateur à partir duquel vous êtes connecté à la console.

Pour importer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, **Importer un plan**.
2. Dans la fenêtre qui s'ouvre, parcourez jusqu'au fichier JSON.
3. Cliquez sur le fichier, puis cliquez sur **Ouvrir**.
   Le plan de gestion à distance apparaît à l'écran. Vous pouvez maintenant l'appliquer aux ressources.

Définir par défaut

© Acronis International GmbH, 2003-2026

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour définir un plan de gestion à distance par défaut

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Définir par défaut**.
3. Dans la fenêtre de confirmation, cliquez sur **Définir**.
   Dans l'écran **Plans de gestion à distance**, la balise **Par défaut** apparaît à côté du nom du plan.

Définir comme favori

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour définir un plan de gestion à distance comme favori

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Ajouter aux favoris**.
   Dans l'écran **Plans de gestion à distance**, l'icône d'étoile apparaît à côté du nom du plan.

Supprimer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Supprimer un plan de gestion à distance

1. Dans l'écran **Plans de gestion à distance**, cliquez sur l'icône **Autres actions** du plan de gestion à distance.
2. Cliquez sur **Supprimer**.
3. Sélectionnez **Je confirme**, puis cliquez sur **Supprimer**.

Identifiants de la ressource

Vous pouvez ajouter les identifiants de l'administrateur ou d'un autre type d'utilisateur des ressources distantes (nom d'utilisateur et mot de passe, ou mot de passe VNC), les enregistrer dans le magasin d'identifiants dans le cloud, puis les utiliser pour l'authentification automatique lors de la connexion aux ressources que vous gérez. De cette manière, au lieu de saisir ces identifiants manuellement à l'étape d'authentification de chaque connexion, vous pouvez ajouter ces identifiants au magasin d'identifiants une fois. Connect Client utilisera alors ces identifiants chaque fois que vous souhaiterez vous connecter aux ressources à distance.

© Acronis International GmbH, 2003-2026

Remarque
Les identifiants conservés dans le magasin d'identifiants ne sont pas partagés entre les différents niveaux de tenants. Ils ne sont partagés que sur le même niveau de tenant, pour le même tenant client ou tenant partenaire.

Cela signifie que si un tenant client comporte plusieurs administrateurs, ces derniers voient et partagent les identifiants dans le magasin d'identifiants, tandis que les autres administrateurs de partenaires ou les administrateurs clients d'autres tenants ne pourront ni visualiser ni utiliser ces identifiants.

Ajout d'identifiants

Vous pouvez ajouter des identifiants et les utiliser pour les connexions à distance à plusieurs ressources.

Pour ajouter les identifiants à une ressource et les enregistrer dans le magasin d'identifiants

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez ajouter des identifiants.
3. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
4. Cliquez sur **Ajouter les identifiants**.
5. Dans le **magasin d'identifiants**, cliquez sur **Ajouter les identifiants**.
6. Saisissez les identifiants.

Champs	Description
Nom des identifiants	Identificateur des identifiants qui sera visible dans le magasin d'identifiants.
Nom d'utilisateur	Nom d'utilisateur qui sera utilisé pour les connexions à distance à la ressource cible.
Mot de passe	Mot de passe qui sera utilisé pour les connexions à distance à la ressource cible.
Mot de passe VNC	Ce champ n'est disponible que pour le partage d'écran Apple.

7. Cliquez sur **Enregistrer**.

Affectation d'identifiants à une ressource

Après avoir ajouté des identifiants, vous pouvez les utiliser pour vous authentifier automatiquement lorsque vous vous connectez à une ressource que vous gérez.

© Acronis International GmbH, 2003-2026

Remarque
L'utilisation de comptes Microsoft Entra ID (anciennement Azure AD) avec le protocole NEAR nécessite une configuration supplémentaire. Voir cet article de la base de connaissances.

Pour affecter des identifiants enregistrés pour l'authentification automatique sur une ressource

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
3. Dans l'onglet du protocole supporté (NEAR, RDP ou Partage d'écran Apple) cliquez sur **Ajouter des identifiants**.
4. Dans le **magasin d'identifiants**, sélectionnez les identifiants dans la liste, puis cliquez sur **Sélectionner les identifiants**.

Suppression d'identifiants

Vous pouvez supprimer les identifiants qui ne sont plus utiles.

Pour supprimer des identifiants du magasin d'identifiants

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
3. Dans l'onglet du protocole pris en charge (NEAR, RDP ou Partage d'écran Apple), cliquez sur **Supprimer**.
4. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Annulation de l'affectation d'identifiants d'une ressource

Vous pouvez annuler l'affectation d'identifiants d'une ressource, mais les conserver dans le magasin d'identifiants.

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.
3. Dans l'onglet du protocole pris en charge (NEAR, RDP ou Partage d'écran Apple cliquez sur **Annuler l'affectation**.
4. Dans la fenêtre de confirmation, cliquez sur **Annuler l'affectation**.

© Acronis International GmbH, 2003-2026

Utilisation des ressources gérées

Les ressources gérées sont des ressources sur lesquelles l'agent Protection est installé.

Vous pouvez effectuer les opérations suivantes sur les ressources distantes gérées :

- se connecter pour l'assistance à distance ou le bureau à distance en utilisant NEAR en mode **Contrôle** ou **Visualisation uniquement**
- se connecter au bureau à distance via RDP en mode **Contrôle**
- se connecter pour l'assistance à distance ou le bureau à distance en utilisant le Partage d'écran Apple en mode **Contrôle**, **Visualisation uniquement** ou **Rideau**
- Effectuer une connexion de type Bureau à distance via un client Web
- Redémarrer un ordinateur, l'arrêter, le mettre en veille, vider la corbeille et déconnecter l'utilisateur distant des ressources distantes
- Transférer des fichiers entre votre ressource et les ressources distantes
- Surveiller les ressources en effectuant des captures d'écran

Remarque
Les connexions Bureau à distance aux ressources gérées nécessitent l'installation d'un agent Protection et l'application d'un plan de gestion à distance sur la ressource.

Configuration des paramètres RDP

Vous pouvez configurer les paramètres qui seront appliqués automatiquement aux connexions RDP à distance de type contrôle à la ressource gérée.

Pour configurer les paramètres RDP d'une ressource

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Accédez au menu **Paramètres** de l'une des manières suivantes :
   - Cliquez sur **Bureau à distance**, puis sur **Paramètres**.
   - Cliquez sur **Gérer**, puis sur **Paramètres**.

© Acronis International GmbH, 2003-2026

3. Dans l'onglet **RDP**, configurez les paramètres.

Paramètre	Description
Lecture audio	Ce paramètre active ou désactive la redirection du son de la ressource distante sur votre ressource locale.
Enregistrement audio	Ce paramètre détermine si l'enregistrement audio (effectué à l'aide du microphone) sera transféré à la ressource distante.
Rediriger les imprimantes	Si vous sélectionnez ce paramètre, les imprimantes de votre ressource seront disponibles sur la ressource distante. **Remarque** La redirection d'imprimante n'est pas prise en charge pour les connexions de bureau à distance via un client Web.
Rediriger les fichiers	Ce paramètre définit si les fichiers de votre ressource locale seront partagés sur la ressource distante.
Intensité de couleur	Ce paramètre détermine le nombre de couleurs dans l'image qui sera transférée par RDP. Plus la valeur est élevée, plus la bande passante nécessaire est importante. **32 768 couleurs** : 16 bits **Couleurs vraies** : • 24 bits pour les connexions RDP via le client Web • 32 bits pour les connexions RDP via Connect Client

4. Cliquez sur le bouton Fermer.

Connexion à des ressources gérées de type bureau ou assistance à distance

Remarque
La disponibilité des protocoles de connexion que vous pouvez utiliser pour les connexions à distance dépend de la configuration du plan de gestion à distance et du système d'exploitation de la ressource distante.

Prérequis

- [Pour les connexions en partage d'écran Apple] Partage d'écran Apple est activé sur la ressource macOS.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour établir une connexion de type bureau ou assistance à distance à une ressource gérée

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource à laquelle vous souhaitez vous connecter.
3. Cliquez sur **Bureau à distance**.

© Acronis International GmbH, 2003-2026

Par défaut, le protocole de connexion sélectionné est le protocole NEAR.

4. [Facultatif] Dans la liste déroulante **Protocole de connexion**, sélectionnez le protocole de connexion que vous souhaitez utiliser.
5. Cliquez sur le mode d'affichage que vous souhaitez utiliser.

Protocole	Connexions à distance à	Mode d'affichage	Action à distance prise en charge
NEAR	Windows Linux macOS	**Contrôle** : dans ce mode, vous pourrez observer la ressource distante et y effectuer des opérations. **Affichage seul** - Dans ce mode, vous ne pourrez qu'observer la ressource distante.	Bureau à distance Assistance à distance
RDP	Windows	**Contrôle** : dans ce mode, vous pourrez visualiser la ressource distante et y effectuer des opérations. **Remarque** Si RDP est désactivé dans les paramètres du système d'exploitation de la ressource, une fenêtre pop-up s'affiche. Utilisez cette fenêtre pour activer RDP pour la ressource, pour la session en cours ou en général : • Si vous souhaitez activer RDP pour cette ressource uniquement pour la session en cours, sélectionnez **Désactiver après la fin de la session**, puis cliquez sur **Autoriser**. • Si vous souhaitez activer RDP pour cette ressource, cliquez sur **Autoriser**.	Bureau à distance
Partage d'écran Apple	macOS	**Contrôle** : dans ce mode, vous pourrez observer la ressource distante et y effectuer des opérations. **Affichage seul** - Dans ce mode, vous ne pourrez qu'observer la ressource distante. **Rideau** : disponible uniquement pour les ressources macOS. Si vous vous connectez à la ressource distante en mode rideau, l'affichage de la ressource distante est assombri et l'utilisateur distant ne pourra pas voir vos actions sur la ressource.	Bureau à distance Assistance à distance

6. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :

© Acronis International GmbH, 2003-2026

- Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.

  Remarque
  Le système suggère automatiquement le plan le plus approprié, en fonction du protocole que vous avez sélectionné à l'étape précédente.

- Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

  Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

7. [Si la fonctionnalité correspondante n'est pas activée dans le plan de gestion à distance appliqué à la ressource] Dans la fenêtre **Mettre à jour un plan de gestion à distance**, cliquez sur **Mettre à jour**, activez la fonctionnalité, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
8. [Si Connect Client n'est pas installé sur votre ressource] Dans la boîte de dialogue **Connexion à la ressource**, cliquez sur **Télécharger Connect Client**, téléchargez et installez le client sur votre ressource, puis cliquez sur **Connexion**.
9. [Si une fenêtre contextuelle de confirmation apparaît] Cliquez sur **Ouvrir Connect Client**.
10. Dans la fenêtre **Authentification**, sélectionnez une option d'authentification, puis indiquez les identifiants nécessaires.

    Remarque
    Si vous avez affecté des identifiants à la ressource, l'authentification est automatique et cette étape est ignorée. Pour plus d'informations, voir "Affectation d'identifiants à une ressource" (p. 1482).

Option d'authentification	Description
Avec identifiants de la ressource distante	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur administrateur de la ressource distante. Cette option est disponible pour NEAR, RDP et Partage d'écran Apple. Vous pouvez utiliser cette option pour vous authentifier lors d'une connexion Bureau ou assistance à distance.
Demander l'autorisation d'observation	Vous pourrez établir la connexion à distance en mode d'observation lorsque l'utilisateur connecté sur la ressource distante l'aura autorisée. Cette option est disponible pour NEAR et Partage d'écran Apple. Vous pouvez utiliser cette option pour vous authentifier lors d'une

© Acronis International GmbH, 2003-2026

Option d'authentification	Description
	connexion de type assistance à distance.
Demander l'autorisation de contrôle	Vous pourrez établir la connexion à distance en mode de contrôle lorsque l'utilisateur connecté sur la ressource distante l'aura autorisée. Cette option est disponible pour NEAR et Partage d'écran Apple. Vous pouvez utiliser cette option pour vous authentifier lors d'une connexion de type assistance à distance.

11. Cliquez sur **Connexion**, puis sur la session à afficher (dans le cas où plusieurs sessions utilisateur sont disponibles sur la ressource).

    Connect Client ouvre une nouvelle fenêtre de visionneuse dans laquelle vous pouvez voir le bureau de la ressource distante. La visionneuse dispose d'une barre d'outils comportant d'autres actions que vous pouvez effectuer sur la ressource distante une fois la connexion à distance établie. Pour plus d'informations, voir "Utilisation de la barre d'outils dans la fenêtre de la visionneuse" (p. 1505).

Connexion à une ressource gérée via un client Web

Vous pouvez établir une connexion Bureau à distance à une ressource gérée via un client Web.

Remarque
La redirection d'imprimante n'est pas prise en charge pour les connexions de bureau à distance via un client Web.

Prérequis

- Le protocole RDP est activé sur la ressource gérée.
- Votre navigateur prend en charge HTML5.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour vous connecter à distance à une ressource via un client Web

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez vous connecter à distance, puis cliquez sur **Bureau à distance** > **Connecter via le client web**.
3. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur

© Acronis International GmbH, 2003-2026

Confirmer.

Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

4. [Si la fonctionnalité correspondante n'est pas activée dans le plan de gestion à distance appliqué à la ressource] Dans la fenêtre **Mettre à jour un plan de gestion à distance**, cliquez sur **Mettre à jour**, activez la fonctionnalité, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
5. Saisissez l'identifiant et le mot de passe pour accéder à la ressource, puis cliquez sur **Connexion**.

Remarque
Si vous avez affecté des identifiants à la ressource, l'authentification est automatique et cette étape est ignorée. Pour plus d'informations, voir "Affectation d'identifiants à une ressource" (p. 1482).

Transfert de fichiers

Vous pouvez transférer facilement des fichiers entre la ressource locale et une ressource gérée.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour transférer à distance des fichiers entre votre ressource et une ressource gérée

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource dont vous souhaitez transférer des fichiers.
3. Cliquez sur **Gérer**, puis sur **Transférer des fichiers**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.

     Remarque
     Le système suggère automatiquement le plan le plus approprié.

   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. [Si **Autoriser les connexions par NEAR** ou **Transfert de fichiers** est désactivé dans le plan de gestion à distance appliqué à la ressource] Dans la fenêtre **Mettre à jour un plan de gestion à distance**, cliquez sur **Mettre à jour**, activez les paramètres, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.

© Acronis International GmbH, 2003-2026

6. [Si Connect Client n'est pas installé sur votre ressource] Dans la boîte de dialogue **Connexion à la ressource**, cliquez sur **Télécharger Connect Client**, téléchargez et installez le client sur votre ressource, puis cliquez sur **Connexion**.
7. [Si une fenêtre contextuelle de confirmation apparaît] Cliquez sur **Ouvrir Connect Client**.
8. Dans la fenêtre **Authentification**, sélectionnez une option d'authentification, puis indiquez les identifiants nécessaires.

Option d'authentification	Description
Avec identifiants de la ressource distante	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur administrateur de la ressource distante.
Demander l'autorisation de transfert de fichiers	Vous pourrez transférer des fichiers lorsque l'utilisateur connecté sur la ressource distante l'aura autorisé.

9. [Pour afficher les fichiers cachés] Dans la fenêtre **Transfert de fichiers**, cliquez sur **Affichage**, puis cliquez sur **Afficher les fichiers cachés**.
10. Parcourez les fichiers que vous souhaitez transférer, puis faites-les glisser et déposez-les à l'emplacement souhaité.

Remarque
Les fichiers de la ressource locale sont répertoriés dans le panneau de gauche et ceux de la ressource distante figurent dans le panneau de droit.
Lorsqu'un transfert de fichiers commence, il est répertorié dans le panneau **Tâches**.

11. [Facultatif] Si vous souhaitez supprimer les tâches terminées du panneau **Tâches**, cliquez sur **Effacement terminé**.
12. Lorsque tous les transferts sont terminés, fermez la fenêtre.

Partage du contenu du Presse-papiers entre des ressources

Vous pouvez envoyer le contenu du Presse-papiers de votre ressource vers une ressource distante, ou obtenir le contenu du Presse-papiers d'une ressource distante via NEAR. Par exemple, vous pouvez copier un texte à partir d'un fichier sur la ressource distante et le coller dans un document sur votre ressource, et vice versa.

Envoyer le Presse-papiers

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour envoyer le contenu du Presse-papiers de votre ressource à une ressource distante

1. Démarrez une session de contrôle à distance vers une ressource gérée via NEAR.
   Pour plus d'informations, voir "Connexion à des ressources gérées de type bureau ou assistance

© Acronis International GmbH, 2003-2026

à distance" (p. 1485).

2. [Facultatif] Si vous souhaitez que les contenus de votre Presse-papiers et de celui des ressources distantes soient synchronisés automatiquement, cliquez dans la barre d'outils **Visionneuse** sur l'icône **Autre**, puis sélectionnez **Synchronisation automatique du Presse-papiers**.
3. Pour partager le contenu de votre Presse-papiers avec celui de la ressource distante, procédez comme suit.
   - Si l'option **Synchronisation automatique du Presse-papiers** est désactivée, effectuez les étapes correspondantes :
     a. Sur votre ressource locale, copiez le texte ou l'image que vous souhaitez envoyer.
     b. Dans la barre d'outils **Visionneuse** de la ressource distante, cliquez sur l'icône **Autres**.
     c. Cliquez sur **Envoyer le Presse-papiers**.
     d. Ouvrez le fichier dans lequel vous souhaitez coller le contenu, puis collez-le.
   - Si l'option **Synchronisation automatique du Presse-papiers** est activée, effectuez les étapes correspondantes en fonction du contenu que vous souhaitez partager.

Option	Actions
Si vous souhaitez partager un ou plusieurs fichiers de votre Presse-papiers local	a. Sur votre ressource locale, copiez le ou les fichiers que vous souhaitez envoyer. b. Ouvrez la fenêtre **Visionneuse** de la ressource distante. c. Dans la fenêtre contextuelle d'alerte qui s'affiche, cliquez sur **Envoyer à l'ordinateur distant**. d. Collez le contenu dans la ressource distante.
Si vous souhaitez partager un texte à partir d'un fichier de votre Presse-papiers local	a. Sur votre ressource locale, copiez le texte que vous souhaitez envoyer. b. Ouvrez la fenêtre **Visionneuse** de la ressource distante. c. Ouvrez le fichier dans lequel vous souhaitez coller le contenu. d. Collez le contenu dans le fichier.

Obtenir le Presse-papiers

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour obtenir le contenu du Presse-papiers d'une ressource distante vers votre ressource

1. Démarrez une session de contrôle à distance vers une ressource gérée via NEAR.
   Pour plus d'informations, voir "Connexion à des ressources gérées de type bureau ou assistance à distance" (p. 1485).

© Acronis International GmbH, 2003-2026

2. Si vous souhaitez que les contenus de votre Presse-papiers et de celui des ressources distantes soient synchronisés automatiquement, cliquez dans la barre d'outils **Visionneuse** sur l'icône **Autre**, puis sélectionnez **Synchronisation automatique du Presse-papiers**.
3. Pour obtenir le contenu du Presse-papiers de la ressource distante dans votre Presse-papiers, procédez comme suit.
   - Si l'option **Synchronisation automatique du Presse-papiers** est désactivée, effectuez les étapes correspondantes.
     a. Sur la ressource distante, copiez le texte ou l'image que vous souhaitez partager.
     b. Dans la barre d'outils **Visionneuse** de la ressource distante, cliquez sur l'icône **Autres**.
     c. Cliquez sur **Obtenir le Presse-papiers**.
     d. Sur la ressource locale, ouvrez le fichier dans lequel vous souhaitez coller le contenu.
     e. Collez le contenu dans le fichier.
   - Si l'option **Synchronisation automatique du Presse-papiers** est activée, effectuez les étapes correspondantes en fonction du contenu que vous souhaitez obtenir.

Option	Actions
Si vous souhaitez obtenir un ou plusieurs fichiers du Presse-papiers de la ressource distante vers votre Presse-papiers local	a. Sur la ressource distante, copiez le ou les fichiers que vous souhaitez obtenir. b. Dans la fenêtre contextuelle d'alerte qui s'affiche, cliquez sur **Recevoir le Presse-papiers**. c. Sur votre ressource locale, collez le contenu.
Si vous souhaitez copier un texte du Presse-papiers de la ressource distante vers le Presse-papiers local	a. Sur la ressource distante, copiez le texte que vous souhaitez obtenir. b. Sur votre ressource locale, collez le contenu dans un fichier.

Réalisation d'actions de contrôle sur les ressources gérées

Vous pouvez gérer une ressource distante en y effectuant des actions de contrôle de base : vider la corbeille, veille, redémarrer, arrêter et déconnecter l'utilisateur distant.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Vider la corbeille

Pour vider la corbeille sur la ressource distante

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Vider la corbeille**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. Sélectionnez la session utilisateur pour laquelle vous souhaitez effectuer cette action, puis cliquez sur **Vider la corbeille**.

Veille

Pour mettre la ressource distante en veille

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Veille**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

Redémarrer

Pour redémarrer une ressource distante

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Redémarrer**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.

© Acronis International GmbH, 2003-2026

- Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

  Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

5. En fonction du système d'exploitation installé sur la ressource distante, procédez comme suit :
   - Pour les ressources Windows, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant le redémarrage de la ressource, sélectionnez l'utilisateur, puis cliquez sur **Redémarrer** à nouveau.
   - Pour les ressources macOS, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant le redémarrage de la ressource, puis cliquez sur **Redémarrer** à nouveau.
   - Pour les ressources Linux, cliquez sur **Redémarrer**.

Arrêt du système

Pour arrêter une ressource distante

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Arrêt du système**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. En fonction du système d'exploitation installé sur la ressource distante, procédez comme suit :
   - Pour les ressources Windows, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant l'arrêt de la ressource, sélectionnez l'utilisateur, puis cliquez sur **Arrêt du système** à nouveau.
   - Pour les ressources macOS, sélectionnez si vous souhaitez autoriser l'utilisateur actuellement connecté localement à la ressource à enregistrer les modifications avant l'arrêt de la ressource, puis cliquez sur **Arrêt du système** à nouveau.
   - Pour les ressources Linux, cliquez sur **Arrêt du système**.

Déconnecter l'utilisateur distant

Pour déconnecter l'utilisateur d'une ressource distante

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource sur laquelle vous souhaitez effectuer cette opération.
3. Cliquez sur **Gérer**, puis sur **Déconnecter l'utilisateur distant**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. Sélectionnez l'utilisateur que vous souhaitez déconnecter, puis cliquez sur **Déconnexion**.

Connexion à distance à la ligne de commande

Vous pouvez vous connecter à distance à l'interface de ligne de commande de vos ressources Windows et macOS gérées et effectuer des tâches liées aux diagnostics, au dépannage, à la gestion de la configuration, à la maintenance, à l'automatisation et à la planification des tâches.

Prérequis

- Vous avez le rôle Administrateur Cyber.
- L'authentification à deux facteurs est activée pour votre compte dans Acronis Cyber Protect Cloud.

Windows

Pour vous connecter à distance à la ligne de commande d'un terminal Windows

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource pour laquelle vous souhaitez démarrer la ligne de commande à distance.
3. Dans le menu **Actions**, cliquez sur **Gérer**, puis cliquez sur **Ligne de commande**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.

     Remarque
     Le système suggère automatiquement le plan le plus approprié.

   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur

© Acronis International GmbH, 2003-2026

Confirmer.

Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

5. Dans l'onglet qui s'ouvre, sélectionnez l'interface de ligne de commande que vous souhaitez utiliser.

   Vous verrez les options suivantes, en fonction des outils de ligne de commande disponibles sur la ressource :

   - PowerShell 7 (64 bits)
   - PowerShell 7 (32 bits)
   - PowerShell 5 (64 bits)
   - PowerShell 5 (32 bits)
   - Invite de commandes (64 bits)
   - Invite de commandes (32 bits)

6. Dans le champ **Utilisateur**, sélectionnez le compte utilisateur sous lequel vous souhaitez démarrer la ligne de commande.

   Remarque
   Si vous démarrez la ligne de commande avec le compte système, vos actions ne seront pas visibles par l'utilisateur de la ressource à distance.

   Si vous démarrez la ligne de commande avec le compte utilisateur connecté, vos actions seront visibles.

7. En fonction de si vous souhaitez enregistrer les paramètres pour la prochaine session, sélectionnez ou désélectionnez **Enregistrer les paramètres pour la prochaine session**.
8. Cliquez sur **Démarrer la session**.

   La console de la ligne de commande s'ouvre. Vous pouvez maintenant effectuer des tâches dans la console.

   Remarque
   Le démarrage et la fin d'une session de ligne de commande à distance créent un enregistrement dans le **Journal d'audit**. L'enregistrement comprend des détails sur l'événement, tels que la date et l'heure, le tenant, le nom de la ressource, l'adresse IP et l'initiateur.

macOS

Pour se connecter à distance à la ligne de commande d'un terminal macOS

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource pour laquelle vous souhaitez démarrer la ligne de commande à distance.
3. Dans le menu **Actions**, cliquez sur **Gérer**, puis cliquez sur **Terminal**.

© Acronis International GmbH, 2003-2026

4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.

     Remarque
     Le système suggère automatiquement le plan le plus approprié.

   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. Dans l'onglet qui s'ouvre, sélectionnez l'interface de ligne de commande que vous souhaitez utiliser.

   Vous verrez les options suivantes, en fonction des outils de ligne de commande disponibles sur la ressource :
   - BASH
   - ZSH
6. Dans le champ **Utilisateur**, sélectionnez le compte utilisateur sous lequel vous souhaitez démarrer la ligne de commande.

   Remarque
   Vous pouvez sélectionner entre les comptes utilisateurs non-service et non cachés disponibles. Le compte utilisateur qui a été enregistré en premier (par date d'inscription) est sélectionné par défaut.

7. En fonction de si vous souhaitez enregistrer les paramètres pour la prochaine session, sélectionnez ou désélectionnez **Enregistrer les paramètres pour la prochaine session**.
8. Cliquez sur **Démarrer la session**.

   La console de la ligne de commande s'ouvre. Vous pouvez maintenant effectuer des tâches dans la console.

   Remarque
   Le démarrage et la fin d'une session de ligne de commande à distance créent un enregistrement dans le **Journal d'audit**. L'enregistrement comprend des détails sur l'événement, tels que la date et l'heure, le tenant, le nom de la ressource, l'adresse IP et l'initiateur.

Actions supplémentaires avec la console de ligne de commande à distance

Après avoir accédé à distance à la ligne de commande d'une ressource gérée, vous pouvez effectuer les actions suivantes depuis la console : copier le contenu de la console, coller le contenu dans la console, effacer la console et exporter le contenu de la console.

Copier

© Acronis International GmbH, 2003-2026

Vous pouvez copier des parties du contenu depuis la console.

Pour copier depuis la console

1. Dans la console de ligne de commande, sélectionnez le texte que vous souhaitez copier.
2. Cliquez sur **Copier**.
   Le texte sélectionné est copié.

Coller

Vous pouvez coller du texte dans la console de ligne de commande à distance.

Pour coller

1. Ouvrez la console de ligne de commande à distance.
2. Dans la console de ligne de commande, cliquez sur **Coller**.
   Le texte est collé dans la console.

Effacer la console

Vous pouvez effacer le contenu de la console de ligne de commande à distance.

Pour effacer la console

1. Ouvrez la console de ligne de commande à distance.
2. Dans la console de ligne de commande, cliquez sur **Effacer la console**.
   La console est effacée.

Exporter

Vous pouvez exporter le contenu complet de la console de ligne de commande sous forme de fichier TXT.

Pour exporter le contenu de la console de ligne de commande

1. Ouvrez la console de ligne de commande à distance.
2. Dans la console de ligne de commande, cliquez sur **Exporter**.
   Le contenu de la console est exporté et enregistré sous forme de fichier TXT dans le dossier de téléchargement par défaut de votre machine locale.

Surveillance des ressources par transmission de captures d'écran

Vous pouvez surveiller le statut d'une ressource à l'aide de la fonctionnalité de transmission de captures d'écran.

Prérequis

- La version de l'agent de protection est à jour et prend en charge la fonctionnalité de transmission de captures d'écran.
- La ressource est en ligne.

© Acronis International GmbH, 2003-2026

- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Correction de ressource

Pour surveiller une ressource par transmission de captures d'écran

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Transmission de captures d'écran**.
2. Cliquez sur la ressource que vous souhaitez ajouter.
3. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Cliquez sur **Appliquer un plan de gestion à distance**, puis effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
4. [Si **Transmission de captures d'écran** est désactivée dans le plan de gestion à distance appliqué à la ressource] Cliquez sur la fenêtre **Accéder au plan de gestion à distance**, cliquez sur **Modifier**, activez **Transmission de captures d'écran**, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
5. [Si **Demander l'autorisation de prendre des captures d'écran** est activé dans le plan de gestion à distance appliqué à la ressource] Cliquez sur **Demander la transmission de captures d'écran**.

   Vous verrez la capture d'écran après que l'utilisateur de la ressource distante a approuvé la demande.
6. [Facultatif] Sélectionnez la session utilisateur.
7. [Facultatif] Sélectionnez l'affichage.
8. [Facultatif] Sélectionnez le taux d'actualisation auquel une nouvelle capture d'écran du bureau est prise.
9. [Facultatif] Sélectionnez la qualité d'image.
10. [Facultatif] Pour télécharger la capture d'écran, cliquez sur l'icône de téléchargement.

Effectuer une capture d'écran

Pour effectuer une capture d'écran d'une ressource gérée

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Machines avec des agents**.
2. Cliquez sur la ressource dont vous souhaitez effectuer une capture d'écran.
3. Cliquez sur **Gérer**, puis sur **Prendre un instantané du bureau**.
4. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Cliquez sur **Appliquer un plan de gestion à distance**, puis effectuez l'une des opérations suivantes :

© Acronis International GmbH, 2003-2026

- Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
- Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

  Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

5. [Si **Transmission de captures d'écran** est désactivée dans le plan de gestion à distance appliqué à la ressource] Cliquez sur la fenêtre **Accéder au plan de gestion à distance**, cliquez sur **Modifier**, activez **Transmission de captures d'écran**, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
6. [Si **Demander l'autorisation de prendre des captures d'écran** est activé dans le plan de gestion à distance appliqué à la ressource] Cliquez sur **Demander la transmission de captures d'écran**.

   Vous verrez la capture d'écran après que l'utilisateur de la ressource distante a approuvé la demande.
7. [Facultatif] Sélectionnez la session utilisateur.
8. [Facultatif] Sélectionnez l'affichage.
9. [Facultatif] Sélectionnez le taux d'actualisation auquel une nouvelle capture d'écran du bureau est prise.
10. [Facultatif] Sélectionnez la qualité d'image.
11. [Facultatif] Pour télécharger la capture d'écran, cliquez sur l'icône de téléchargement.

Observation simultanée de plusieurs ressources gérées

Vous pouvez observer les bureaux de plusieurs ressources à distance simultanément dans une seule fenêtre. Cette fonctionnalité nécessite que NEAR ou le partage d'écran Apple soit activé dans les plans de gestion à distance qui sont appliqués aux ressources.

Remarque
Le nombre de bureaux que vous pouvez visualiser simultanément dans la fenêtre dépend de la taille de l'écran.

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour observer simultanément plusieurs ressources

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez les ressources que vous souhaitez observer.
3. Cliquez sur **Vue multiple**.

© Acronis International GmbH, 2003-2026

4. [Si aucun plan de gestion à distance n'est appliqué à aucune des ressources] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.

     Remarque
     Le système suggère automatiquement le plan le plus approprié.

   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. [Si la fonctionnalité correspondante n'est pas activée dans le plan de gestion à distance qui est appliqué aux ressources] Dans la fenêtre **Mettre à jour un plan de gestion à distance**, cliquez sur **Mettre à jour**, activez la fonctionnalité, puis démarrez cette procédure à partir de l'étape 1.
6. [Si Connect Client n'est pas installé sur votre ressource] Dans la boîte de dialogue **Connexion à la ressource**, cliquez sur **Télécharger Connect Client**, téléchargez et installez le client sur votre ressource, puis cliquez sur **Connexion**.
7. [Si une fenêtre contextuelle de confirmation apparaît] Cliquez sur **Ouvrir Connect Client**.
8. Dans la fenêtre **Authentification**, sélectionnez une option d'authentification, puis indiquez les identifiants nécessaires.

Option d'authentification	Description
Avec identifiants de la ressource distante	Vous serez autorisé à établir la connexion à distance après avoir indiqué le nom d'utilisateur et le mot de passe d'un utilisateur administrateur sur la ressource distante.
Demander l'autorisation d'observation	Vous pourrez établir la connexion à distance en mode d'observation lorsque l'utilisateur connecté sur la ressource distante l'aura autorisée.

9. Si vous souhaitez utiliser la même méthode d'authentification et les mêmes identifiants lors de la connexion à toutes les ressources distantes que vous avez sélectionnées à l'étape 2, sélectionnez **Utiliser sur les autres ordinateurs**.
10. Cliquez sur **Connexion**.

    Dans la barre d'outils de la fenêtre Vue multiple, vous pouvez sélectionner un mode d'affichage pour la connexion à une ressource. Cette action ouvre une autre fenêtre de visionneuse pour cette ressource.

© Acronis International GmbH, 2003-2026

Remarque
Si l'une des ressources sélectionnées est hors ligne ou si la version de l'agent qui y est installée est obsolète, cette ressource n'est pas affichée dans la fenêtre Vue multiple.
Toutes les connexions en vue multiple à des ressources distantes sont en mode **Affichage seul**.

Utilisation des ressources non gérées

Les ressources non gérées sont des ressources sur lesquelles l'agent Protection n'est pas installé.

Vous pouvez effectuer les opérations suivantes sur les ressources distantes non gérées :

- Effectuer une connexion de type assistance à distance à l'aide de Acronis Assistance rapide
- Effectuer une connexion de type assistance ou Bureau à distance à l'aide d'une adresse IP
- Transférer des fichiers entre votre ressource et la ressource distante à l'aide de Assistance rapide

Remarque
Pour vous connecter à distance à des ressources non gérées à l'aide de Assistance rapide, vérifiez les éléments suivants :

- La licence requise est affectée à votre tenant client.
- L'application Assistance rapide s'exécute sur la ressource distante à laquelle vous souhaitez vous connecter.

Connexion à des ressources non gérées via Acronis Assistance rapide

Vous pouvez utiliser la fonctionnalité Assistance rapide pour vous connecter à distance et à la demande à des ressources non gérées, et fournir une aide ponctuelle.

Prérequis

- La licence requise est affectée à votre tenant client.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.
- L'utilisateur distant a fourni l'identifiant de ressource et le code d'accès à partir de Assistance rapide.
- L'utilisateur distant a téléchargé et exécuté Acronis Assistance rapide.

Pour établir une connexion de type assistance à distance à une ressource à l'aide de Assistance rapide

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Assistance rapide**.
3. Dans la fenêtre **Assistance rapide**, saisissez l'identifiant de ressource que l'utilisateur final vous a donné, puis sélectionnez **Connexion**.
4. Cliquez sur **Connexion**.

© Acronis International GmbH, 2003-2026

5. Selon que Connect Client est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Connect Client n'est pas installé, téléchargez-le, installez-le, puis sélectionnez **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Connect Client est déjà installé, cliquez sur **Ouvrir Connect Client** dans la fenêtre de confirmation qui s'affiche.
6. Dans la fenêtre **Authentification**, saisissez le code d'accès.
7. Connect Client ouvre une nouvelle fenêtre de visionneuse dans laquelle vous pouvez voir le bureau de la ressource distante. La visionneuse dispose d'une barre d'outils comportant d'autres actions que vous pouvez effectuer sur la ressource distante une fois la connexion à distance établie. Pour plus d'informations, voir "Utilisation de la barre d'outils dans la fenêtre de la visionneuse" (p. 1505).

Connexion à des ressources non gérées via une adresse IP

Si une ressource non gérée se trouve sur votre réseau local, vous pouvez vous y connecter pour un contrôle ou une assistance à distance à l'aide de son adresse IP. Cette connexion ne nécessite aucun accès Internet.

Prérequis

- La licence requise est affectée à votre tenant client.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.

Pour établir une connexion de type bureau ou assistance à distance à une ressource à l'aide de son adresse IP

1. Dans la console Cyber Protect, accédez à **Tous les terminaux**.
2. Cliquez sur **Assistance rapide**.
3. Cliquez sur l'onglet **Par adresse IP**.
4. Saisissez l'adresse IP et le port de la ressource.
5. Sélectionnez un protocole de connexion - RDP (ressources Windows) ou Partage d'écran Apple (pour les ressources macOS), en fonction du système d'exploitation de la ressource distante.

   Remarque
   Les connexions via RDP prennent en charge l'action de bureau à distance, et les connexions via Partage d'écran Apple prennent en charge les actions de bureau à distance et d'assistance à distance.

6. Cliquez sur **Connexion**.
7. Dans la fenêtre **Authentification**, indiquez les identifiants nécessaires.

Pour les connexions Partage d'écran Apple, Connect Client ouvrira une nouvelle fenêtre de visualisation dans laquelle vous pourrez voir le bureau de la ressource distante. La visionneuse

© Acronis International GmbH, 2003-2026

comporte une barre d'outils avec des actions supplémentaires que vous pouvez effectuer sur la ressource distante après l'établissement de la connexion à distance. Pour plus d'informations, voir "Utilisation de la barre d'outils dans la fenêtre de la visionneuse" (p. 1505).

Transfert de fichiers via Acronis Assistance rapide

Vous pouvez utiliser la fonctionnalité Assistance rapide pour transférer des fichiers entre votre ressource et des ressources non gérées.

Prérequis

- La licence requise est affectée à votre tenant client.
- L'authentification à deux facteurs est activée pour votre compte utilisateur dans Acronis Cyber Protect Cloud.
- L'utilisateur distant a téléchargé et exécuté Acronis Assistance rapide.
- L'utilisateur distant a fourni l'identifiant d'ordinateur et le code d'accès à partir de Assistance rapide.

Pour transférer des fichiers à une ressource à l'aide de Assistance rapide

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Assistance rapide**.
3. Dans la fenêtre **Assistance rapide**, saisissez l'identifiant de ressource que l'utilisateur final vous a attribué, puis sélectionnez **Transfert de fichiers**.
4. Cliquez sur **Connexion**.
5. Selon que Connect Client est installé ou pas sur votre ressource, effectuez l'une des opérations suivantes :
   - Si Connect Client n'est pas installé, téléchargez-le, installez-le, puis sélectionnez **Autoriser** dans la fenêtre de confirmation qui s'affiche.
   - Si Connect Client est déjà installé, cliquez sur **Ouvrir Connect Client** dans la fenêtre de confirmation qui s'affiche.
6. Dans la fenêtre **Authentification**, saisissez le code d'accès.
7. Dans la fenêtre **Transfert de fichiers**, parcourez les fichiers et faites-les glisser pour les déposer dans la destination souhaitée.

   Remarque
   Les fichiers de la ressource locale sont répertoriés dans le panneau de gauche et ceux de la ressource distante figurent dans le panneau de droit.
   Lorsqu'un transfert de fichiers commence, il est répertorié dans le panneau **Tâches**.

8. [Facultatif] Si vous souhaitez supprimer les tâches terminées du panneau **Tâches**, cliquez sur **Effacement terminé**.
9. Lorsque tous les transferts sont terminés, fermez la fenêtre.

© Acronis International GmbH, 2003-2026

Utilisation de la barre d'outils dans la fenêtre de la visionneuse

Une fois que vous êtes connecté à une ressource distante, vous pouvez utiliser la barre d'outils de la fenêtre de la visionneuse pour effectuer rapidement les différentes actions.

Icône	Description
	**Taille réelle** Adapte le bureau de la ressource distante afin qu'un pixel du bureau distant corresponde à un pixel dans la fenêtre de la visionneuse.
	**Zoom pour ajuster** Adapte le bureau de la ressource distante à la fenêtre de la visionneuse.
	**Verrouiller** et **Déverrouiller l'écran** Affiche un espace réservé sur l'écran de la ressource distante afin que l'utilisateur distant ne voie pas vos actions.
	**Prendre un instantané** Enregistre l'image du bureau du serveur distant dans un fichier local.
	**Sélectionner l'affichage** Sélectionne l'écran de la ressource distante que vous souhaitez afficher, ainsi que la résolution souhaitée. Disponible pour les connexions de Partage d'écran Apple sur macOS et les connexions NEAR sur n'importe quel système d'exploitation. Si l'ordinateur distant possède plusieurs écrans, vous pouvez choisir l'un des modes d'affichage suivants pour plusieurs moniteurs : • **Combiné** : tous les affichages distants sont affichés dans une seule fenêtre. • **Fractionné** : chaque affichage à distance est affiché dans une fenêtre distincte. Ce mode est très pratique si vous avez plusieurs écrans connectés à votre ressource locale. Dans ce cas, par exemple, vous pouvez organiser l'affichage d'un écran distant sur chaque écran local. Si vous fermez l'un des affichages de ressource distants, la connexion distante est arrêtée. Pour afficher les affichages de la ressource distante, vous devez vous reconnecter. Disponible pour les connexions NEAR uniquement
	**Qualité d'image** Ajuste la qualité de l'image de l'écran distant du noir et blanc à la plus haute qualité possible sur les connexions de Partage d'écran Apple.

© Acronis International GmbH, 2003-2026

Icône	Description
	**Qualité d'image NEAR** Ajuste le ratio qualité/performance sur les connexions NEAR. La partie gauche du curseur (Lisse) donne la priorité aux performances sur la qualité d'image et la partie droite (Net) correspond à la meilleure qualité de l'écran du bureau distant, mais probablement aux pires performances.
	**Envoyer Ctrl+Alt+Suppr** Envoie une séquence Ctrl+Alt+Suppr à la ressource distante. Disponibles pour les ressources Windows et Linux.
	**Transfert de fichiers** Ouvre la fenêtre du Gestionnaire de fichiers afin d'échanger des fichiers entre la ressource distante et la ressource locale. Disponible pour les connexions NEAR.
	**Épingler la barre d'outils** Désactive le masquage automatique de la barre d'outils de la visionneuse. Disponible pour les ressources Windows.
	**Plein écran** Passe en plein écran et adapte la ressource distante afin qu'elle remplisse complètement l'écran local. Disponible pour les ressources Windows.
	**Fermer** Ferme la fenêtre de la visionneuse et met fin à la session de contrôle à distance. Disponible pour les ressources Windows.

Selon le type de connexion, d'autres options peuvent être disponibles lorsque vous cliquez sur l'icône **Autre**.

Option	Description
Commencer l'enregistrement/Arrêter l'enregistrement	Enregistre la session actuelle Bureau à distance. Les enregistrements des sessions sont sauvegardés sous forme de fichiers .crec sur la ressource locale. Vous pouvez ouvrir les fichiers .crec à l'aide de Acronis Connect Client. Disponible pour les connexions NEAR

© Acronis International GmbH, 2003-2026

Option	Description
Synchroniser automatiquement le Presse-papiers	Lorsque cette option est activée, le client synchronise automatiquement votre Presse-papiers local et celui de l'ordinateur distant. Disponible pour les connexions NEAR
Envoyer le Presse-papiers	Utilisez **Envoyer le presse-papiers** pour remplacer le contenu du presse-papiers de la ressource distante par celui du presse-papiers local. L'option est désactivée si l'option **Synchronisation automatique du Presse-papiers** est activée. Pour plus d'informations, voir "Partage du contenu du Presse-papiers entre des ressources" (p. 1490). Disponible pour les connexions NEAR
Coller le presse-papiers comme frappes	Utiliser **Coller le presse-papiers comme frappes** pour coller le contenu du presse-papiers local dans la ressource distante en simulant des frappes. Cette option est utile lorsque les autres options pour envoyer le contenu du presse-papiers ne sont pas disponibles, telles que : • Copier un mot de passe sur la ressource locale et le coller dans l'écran de connexion de la ressource distante. • Utiliser des applications qui ne supportent pas le collage depuis le presse-papiers via des raccourcis clavier ou des actions de souris. Disponible pour les connexions NEAR
Obtenir le Presse-papiers	Utilisez **Obtenir le presse-papiers** pour transférer le contenu du presse-papiers de la ressource distante vers le presse-papiers de la ressource locale. L'option est désactivée si l'option **Synchronisation automatique du Presse-papiers** est activée. Pour plus d'informations, voir "Partage du contenu du Presse-papiers entre des ressources" (p. 1490). Disponible pour les connexions NEAR
Clavier intelligent/Touches brutes/Touches brutes avec tous les raccourcis	Change le mode de saisie du clavier de la connexion en cours. **Clavier intelligent** : le client transmet les codes Unicode des symboles saisis localement à l'ordinateur distant **Touches brutes** : le client utilise les codes bruts des touches du clavier sur lesquelles vous appuyez. **Touches brutes avec tous les raccourcis** : le client désactive

© Acronis International GmbH, 2003-2026

Option	Description
	les raccourcis du système local afin qu'ils soient également transmis au système d'exploitation distant.
Activation de clavier lors du survol de la souris	Lorsque cette option est activée, le client ne capture la saisie au clavier que lorsque le curseur de la souris locale est placé sur la fenêtre de la visionneuse. Lorsque cette option est désactivée, le client capture la saisie au clavier dès que sa fenêtre est active.
Afficher les infos de connexion/Masquer les infos de connexion	Lorsque l'option **Afficher les infos de connexion** est sélectionnée, un petit panneau d'informations apparaît sur l'écran du bureau distant et affiche les données les plus essentielles concernant la connexion en cours.
Son distant	Permet au client de rediriger le son depuis l'ordinateur distant vers l'ordinateur local. Disponible pour les connexions NEAR
Préférences	Configurez les paramètres de Connect Client. Pour plus d'informations, voir "Configuration des paramètres Connect Client" (p. 1509).

Enregistrement et lecture de sessions à distance

Vous pouvez enregistrer une session à distance via NEAR sur Acronis Connect Client.

Pour enregistrer une session à distance

1. Dans la barre d'outils de la visionneuse dans Connect Client, cliquez sur **Autre** et sélectionnez **Démarrer l'enregistrement**.
2. Sélectionnez un nom et un emplacement pour l'enregistrement.
   Par défaut, le fichier est nommé avec la date et l'heure en cours ; il se trouve dans le dossier **Documents** du répertoire personnel de l'utilisateur actuel. Lorsque l'enregistrement est actif, la barre d'outils de la **visionneuse** affiche un cercle rouge clignotant dans l'angle supérieur droit de l'écran distant, ainsi que la minuterie d'enregistrement.
3. Pour arrêter l'enregistrement, cliquez sur **Autre**, puis sur **Arrêter l'enregistrement**. Sur un Mac, vous pouvez également cliquer sur **Arrêter** dans la barre d'outils.
   Tous les fichiers .crec créés par Acronis Connect Client seront ouverts par défaut avec Acronis Connect Client.

Pour écouter un enregistrement

1. Localisez le fichier d'enregistrement.
2. Ouvrez-le.

© Acronis International GmbH, 2003-2026

Le lecteur d'enregistrement de Acronis Connect Client s'ouvre. Notez qu'il n'est pas possible de naviguer dans l'enregistrement. Pour trouver un moment précis dans l'enregistrement, attendez que le lecteur l'atteigne.

3. [Facultatif] Pour régler la vitesse de lecture, utilisez les icônes **<<** et **>>** dans la section des commandes de lecture.

   L'enregistrement est stocké sous la forme d'une séquence d'événements transmis vers et depuis le serveur distant au cours d'une connexion. Cela garantit la meilleure qualité d'enregistrement pour une taille de fichier minimale. Toutefois, cela signifie également qu'il n'est pas possible de naviguer dans l'enregistrement. Pour l'instant, il n'est pas non plus possible de convertir les enregistrements dans un format vidéo.

Configuration des paramètres Connect Client

Après avoir installé Connect Client sur votre ressource, vous pouvez configurer ses paramètres en fonction de vos préférences.

Pour configurer les paramètres de Connect Client

1. Dans le menu Démarrer, recherchez **Connect Client** et démarrez-le.
2. Configurez les paramètres dans l'onglet **Général**.

Option	Description
Écrire des journaux détaillés	Sélectionnez cette option pour autoriser Connect Client à écrire des journaux détaillés. Si cette option est désactivée, le client n'écrira que des informations générales dans le fichier journal.
Paramètres proxy	Sélectionnez si vous souhaitez utiliser le proxy système par défaut ou configurer un proxy SOCKSS personnalisé.

3. Configurez les paramètres dans l'onglet **Visionneuse**.

Option	Description
Demander confirmation lors de la fermeture d'une visionneuse	Sélectionnez cette option si vous souhaitez que Connect Client affiche un message de confirmation lorsque vous essayez de fermer la fenêtre de la visionneuse afin d'éviter toute fermeture accidentelle.
Lors de la réduction en icône	Indiquez si vous souhaitez interrompre l'activité de la visionneuse lorsqu'elle est réduite en icône afin de diminuer la charge du processeur.
Lors de l'agrandissement	Indiquez si vous souhaitez activer le mode plein écran lors de l'agrandissement.
Transfert de Presse-papiers	Active l'affichage de l'indicateur de transfert du Presse-papiers dans la fenêtre de la visionneuse lorsque vous copiez ou collez du texte et des images.

© Acronis International GmbH, 2003-2026

Option	Description
Mode clavier	Active l'affichage de l'indicateur du mode de saisie dans le titre de la fenêtre de la visionneuse lorsque des événements à la souris ou au clavier sont envoyés à la machine distante.
Presse-papiers	Sélectionnez **Synchroniser le Presse-papiers automatiquement** afin d'activer la synchronisation automatique du Presse-papiers lorsqu'elle est disponible.
Envoyer les événements de clavier	Choisissez d'utiliser votre saisie au clavier local dès que la fenêtre Connect Client est active ou uniquement lorsque le pointeur de la souris locale la survole.
Couleur d'arrière-plan de la visionneuse	Change la couleur d'arrière-plan de la fenêtre de la visionneuse.
Se reconnecter automatiquement	Sélectionnez **Activer pour automatiser la reconnexion** si vous souhaitez que Connect Client rétablisse automatiquement la connexion si elle a été interrompue.
H.264	Vous pouvez désactiver les décodeurs matériels.
Fermer en veille	Sélectionnez l'intervalle de temps avant la mise en veille une fois la fenêtre de la visionneuse fermée.

4. Configurez les paramètres dans l'onglet **Clavier**.

Option	Description
Mappages de modificateurs	Change le comportement des clés de modificateurs à l'aide d'un menu contextuel. Ces paramètres sont enregistrés séparément pour les connexions NEAR, Partage d'écran Apple et RDP.
Mode d'entrée	Pour chaque type de connexion (sélectionné dans l'en-tête du panneau), sélectionnez le mode par défaut de saisie au clavier.

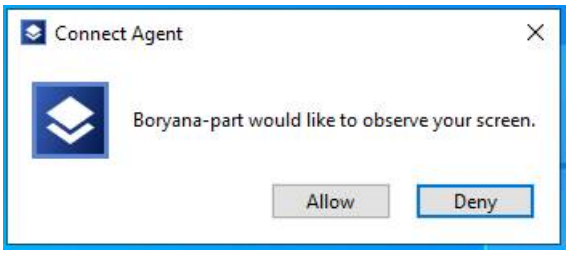
5. Cliquez sur **OK**.

Notificateurs de Bureau à distance

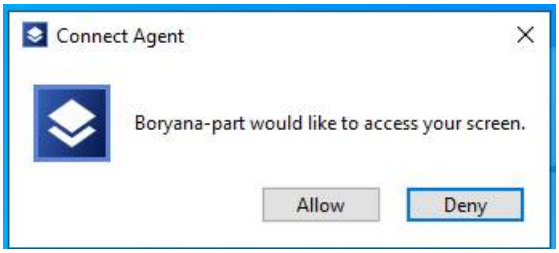
Agent Connect affiche des boîtes de dialogue d'action (notificateurs) sur le bureau de la ressource distante dans les cas suivants :

- lorsque vous essayez de vous connecter à la ressource distante en demandant l'autorisation d'observer. L'utilisateur qui est connecté à la ressource distante localement peut autoriser ou refuser la demande.

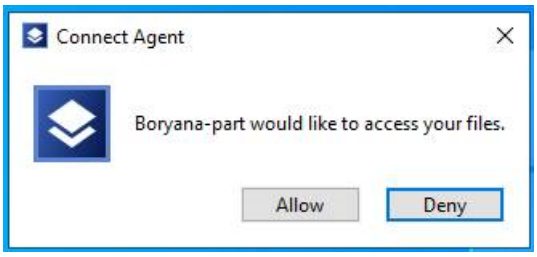
© Acronis International GmbH, 2003-2026



- lorsque vous essayez de vous connecter à la ressource distante en demandant l'autorisation de contrôler. L'utilisateur qui est connecté à la ressource distante localement peut autoriser ou refuser la demande.



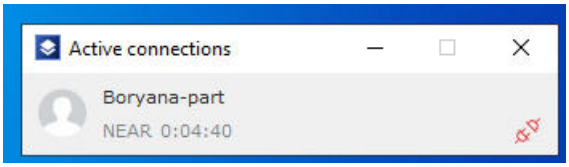
- lorsque vous essayez d'échanger des fichiers entre votre ressource et la ressource distante en demandant l'autorisation de transférer des fichiers. L'utilisateur qui est connecté à la ressource distante localement peut autoriser ou refuser la demande.



Lorsque vous établissez une connexion Bureau à distance à une ressource, l'utilisateur qui est connecté à la ressource recevra une notification de connexion différente contenant les informations suivantes :

- le nom d'utilisateur qui est connecté à distance
- le protocole de connexion qui est utilisé pour établir la connexion à distance
- la durée de la connexion à distance

L'utilisateur qui est connecté à la ressource distante localement peut mettre fin à la connexion à tout moment en cliquant sur l'icône **Déconnecter** ou **Fermer**.



© Acronis International GmbH, 2003-2026

Suivi de la géolocalisation

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Avec le suivi de la géolocalisation, vous pouvez visualiser l'emplacement physique de vos terminaux en temps réel. Vous pouvez utiliser ces informations pour :

- Restreindre l'accès aux données ou systèmes sensibles en fonction de l'emplacement du terminal.
- Suivre les terminaux volés ou perdus.
- Gérer les enregistrements précis de l'endroit où les terminaux de votre organisation sont utilisés.

Pour commencer à suivre l'emplacement d'un terminal, vous devez activer les services de localisation dans les paramètres de son système d'exploitation, puis appliquer un plan de gestion à distance avec l'option de suivi de géolocalisation activée. Pour plus d'informations, voir "Création d'un plan de gestion à distance" (p. 1467) et "Activation des services d'emplacement dans le système d'exploitation" (p. 1513).

En fonction du système d'exploitation du terminal, le suivi de géolocalisation utilise la géolocalisation par système d'exploitation ou la géolocalisation par IP.

La géolocalisation par système d'exploitation utilise les signaux GPS, Wi-Fi, Bluetooth et les données des tours cellulaires pour déterminer l'emplacement précis du terminal. La géolocalisation par IP utilise l'adresse IP du terminal et la compare aux régions géographiques connues de la base de données GeoIP pour déterminer l'emplacement du terminal.

Le terminal envoie les données d'emplacement toutes les 5 minutes pour la géolocalisation par système d'exploitation et toutes les 2 heures pour la géolocalisation par IP.

Pour plus d'informations sur la méthode de suivi de la géolocalisation prise en charge par le système d'exploitation, voir "Méthode de suivi de géolocalisation prise en charge par le système d'exploitation" (p. 1512).

Méthode de suivi de géolocalisation prise en charge par le système d'exploitation

Le suivi de la géolocalisation est pris en charge pour les systèmes d'exploitation Windows, macOS et Linux. Toutefois, la méthode utilisée pour suivre les terminaux peut différer selon les systèmes d'exploitation. Le tableau suivant fournit plus de détails.

Système d'exploitation	Méthode de suivi de géolocalisation prise en charge
Windows	Géolocalisation par système d'exploitation. Cette méthode est utilisée lorsque les services d'emplacement sont activés sur le terminal.

© Acronis International GmbH, 2003-2026

Système d'exploitation	Méthode de suivi de géolocalisation prise en charge
	Géolocalisation par IP
macOS	Géolocalisation par système d'exploitation. Cette méthode est utilisée lorsque les services d'emplacement sont activés sur le terminal. Géolocalisation par IP
Linux	Géolocalisation par IP

Activation des services d'emplacement dans le système d'exploitation

Pour que vous puissiez suivre l'emplacement d'un terminal, les services de localisation doivent être activés dans les paramètres du système d'exploitation du terminal.

Pour les terminaux macOS, vous pouvez activer les services de localisation lors de l'installation de l'agent sur le terminal en accordant l'autorisation **Services de localisation**. Pour plus d'informations, voir "Attribution des autorisations système requises à Agent Connect" (p. 57).

Si un plan de gestion à distance avec l'option **Suivi de la géolocalisation** activée est appliqué à un terminal sur lequel les services de localisation sont désactivés, une notification s'affiche sur le terminal. Vous pouvez cliquer sur le lien de la notification et activer les services de localisation.

Vous pouvez activer les services de localisation d'un terminal à tout moment. Pour plus d'informations sur les étapes à suivre, consultez la documentation du fournisseur du système d'exploitation correspondant.

Affichage de l'emplacement d'un terminal

Vous pouvez voir sur une carte le dernier emplacement où un terminal a été vu. Vous pouvez également voir les coordonnées et l'heure à laquelle le terminal se trouvait à cet emplacement.

Prérequis

- Les services d'emplacement sont activés dans les paramètres du système d'exploitation du terminal.
- L'agent installé sur le terminal prend en charge le suivi de l'emplacement.

Pour afficher l'emplacement d'un terminal

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur le terminal que vous souhaitez suivre et, dans le menu **Actions**, cliquez sur **Voir sur la carte**.
   La page **Suivi de l'emplacement** s'ouvre.
3. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la page **Suivi de l'emplacement**, cliquez sur **Appliquer un plan de gestion à distance**, puis effectuez l'une des

© Acronis International GmbH, 2003-2026

opérations suivantes :

- Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
- Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

  Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

4. [Si le **Suivi de la géolocalisation** est désactivé dans le plan de gestion à distance appliqué à la ressource] Dans la page **Suivi de l'emplacement**, cliquez sur **Accéder au plan**, cliquez sur **Modifier**, activez le **Suivi de la géolocalisation**, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
5. Sur la page **Suivi de l'emplacement**, cliquez sur l'épingle qui marque l'emplacement du terminal.

   Les informations supplémentaires suivantes sont affichées : statut du terminal (en ligne ou hors ligne), coordonnées GPS de l'emplacement du terminal et heure de la dernière détection.

À partir des détails du terminal

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur le terminal que vous souhaitez suivre et, dans le menu **Actions**, cliquez sur **Détails**.
3. Faites défiler la liste des détails jusqu'à ce que vous voyiez les données d'emplacement.

   Les informations supplémentaires suivantes sont affichées : méthode de géolocalisation, coordonnées GPS de l'emplacement du terminal, pays, ville et heure de la dernière détection.
4. [Facultatif] Pour voir l'emplacement du terminal sur une carte, cliquez sur **Accéder au suivi de l'emplacement**.

   Sur la carte, l'emplacement du terminal est marqué d'une épingle.

Depuis le suivi de l'emplacement

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Suivi de l'emplacement**.
2. [Facultatif] Pour filtrer les terminaux affichés, cliquez sur **Filtrer**, sélectionnez les conditions de filtrage, puis cliquez sur **Appliquer**.

   Vous pouvez filtrer les terminaux par statut : **Tous**, **En ligne** ou **Hors ligne**. Les tenants des partenaires peuvent également filtrer l'affichage par client.
3. [Facultatif] Pour rechercher le terminal par son nom, cliquez sur **Rechercher**, puis commencez à saisir le nom du terminal.

   Les résultats changent de manière dynamiqueme à chaque caractère que vous tapez.
4. Cliquez sur le terminal que vous souhaitez suivre.
5. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la page **Suivi de l'emplacement**, cliquez sur **Appliquer un plan de gestion à distance**, puis effectuez l'une des opérations suivantes :

© Acronis International GmbH, 2003-2026

- Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
- Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

  Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).

6. [Si le **Suivi de la géolocalisation** est désactivé dans le plan de gestion à distance appliqué à la ressource] Dans la page **Suivi de l'emplacement**, cliquez sur **Accéder au plan**, cliquez sur **Modifier**, activez le **Suivi de la géolocalisation**, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
7. Sur la page **Suivi de l'emplacement**, cliquez sur l'épingle qui marque l'emplacement du terminal.

   Les informations supplémentaires suivantes sont affichées : statut du terminal (en ligne ou hors ligne), coordonnées GPS de l'emplacement du terminal et heure de la dernière détection.

Chat d'assistance

Remarque
La disponibilité de cette fonctionnalité dépend de la licence dont vous disposez.

Le chat d'assistance est un outil de communication en temps réel entre les techniciens et les utilisateurs distants de ressources Windows et macOS gérées. En utilisant cette fonctionnalité, vous pouvez résoudre les problèmes plus rapidement et offrir un meilleur service client.

Vous pouvez utiliser la fonctionnalité chat d'assistance pour effectuer les tâches suivantes :

- Démarrer une session de chat avec un utilisateur distant d'une ressource gérée.

  Les chats peuvent être démarrés par le technicien, dans la console Cyber Protect, ou par l'utilisateur distant, dans Cyber Protect Monitor. Le technicien et l'utilisateur distant reçoivent des notifications concernant les nouveaux messages et les changements d'état des messages système de leurs chats. Les nouveaux chats démarrés par des utilisateurs distants sont ajoutés à une file d'attente dans l'état **Non affecté**, à partir de laquelle les administrateurs de tenant peuvent les affecter. Pour plus d'informations sur l'utilisation de chats dans Monitor, voir "Chats dans Monitor" (p. 375).

  Dans les chats, si le prénom et le nom de l'administrateur sont configurés dans Portail de gestion > **Mon entreprise** > **Utilisateurs**, le système les affiche. Sinon, le système génère et affiche un nom générique au format Technicien XXXX, où XXXX sont les 4 premiers caractères de l'identifiant de l'utilisateur interne.

  En tant que nom de l'utilisateur distant qui est connecté à la ressource gérée, le système affiche :
  - Pour les ressources Mac, le nom complet de l'utilisateur, ou si ce n'est pas disponible, alors l'identifiant de l'utilisateur.
  - Pour les ressources Windows, l'identifiant de l'utilisateur.

© Acronis International GmbH, 2003-2026

Remarque
Si l'administrateur ou le technicien auquel le chat est affecté dans la console est hors ligne ou absent pendant 15 minutes, et que le chat n'est pas mis en attente, le système change automatiquement le statut du chat en **Non affecté**.

- Gérez une session de chat en l'affectant, la réaffectant, la mettant en attente, la terminant et la rouvrant.
- Parcourir les sessions de chat dans le tenant.
- Modifier ou supprimer des messages dans des sessions de chat actives.
- Recherchez des sessions de chat pour des mots-clés ou des messages spécifiques.
- Exporter l'historique des chats dans un fichier `.txt`.

Démarrer un chat avec un utilisateur distant

Vous pouvez démarrer un nouveau chat avec un utilisateur distant depuis les écrans **Tous les terminaux** et **Chat**.

Prérequis

- Le système d'exploitation de la ressource est Windows ou macOS.
- La fonctionnalité de chat est prise en charge pour votre rôle d'utilisateur.

Pour démarrer un nouveau chat avec un utilisateur distant

À partir de tous les terminaux

1. Dans la console Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource avec laquelle vous souhaitez démarrer un chat, puis dans le menu **Actions**, cliquez sur **Chat**.
3. [Si aucun plan de gestion à distance n'est appliqué à la ressource] Dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.

     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
4. [Si le **Chat** est désactivé dans le plan de gestion à distance qui est appliqué à la ressource] Dans la fenêtre **Mettre à jour un plan de gestion à distance**, cliquez sur **Mettre à jour**, activez le **Chat**, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.
5. Dans la boîte de dialogue **Démarrer le chat**, sélectionnez la ressource et l'utilisateur connecté avec lequel vous souhaitez discuter, puis cliquez sur **Démarrer**.

© Acronis International GmbH, 2003-2026

Une fenêtre de chat s'ouvre où vous pouvez taper votre message. Le chat vous est automatiquement affecté et est répertorié dans la liste **Affecté à moi**.

Remarque
Si vous êtes hors ligne ou loin de la console pendant 15 minutes et que le chat n'est pas mis en attente, le système change automatiquement l'état du chat en **Annulé l'affectation**.

Du Chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Cliquez sur **Démarrer le chat**.
3. Dans la boîte de dialogue **Démarrer le chat**, sélectionnez la ressource et l'utilisateur connecté avec lequel vous souhaitez discuter, puis cliquez sur **Démarrer**.
   Une fenêtre de discussion s'ouvre où vous pouvez taper votre message. La discussion vous est automatiquement affectée et est répertoriée dans la liste **Affecté à moi**. La fenêtre de discussion est inactive si un plan de gestion à distance n'est pas appliqué à la ressource ou si la fonctionnalité de discussion est désactivée.
4. [Si un plan de gestion à distance n'est pas appliqué à la ressource] Dans le message d'avertissement, cliquez sur **Appliquer un plan**, puis dans la fenêtre **Appliquer un plan de gestion à distance**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez appliquer un plan de gestion à distance existant, cliquez sur le champ **Plans disponibles**, sélectionnez le plan, puis cliquez sur **Appliquer**.
   - Si vous souhaitez créer un nouveau plan de gestion à distance, cliquez sur **Ajouter**, configurez les paramètres, cliquez sur **Créer**, puis, dans la fenêtre de confirmation, cliquez sur **Confirmer**.
     Pour plus d'informations sur la création et la configuration d'un plan de gestion à distance, voir "Création d'un plan de gestion à distance" (p. 1467).
5. [Si le **Chat** est désactivé dans le plan de gestion à distance qui est appliqué à la ressource] Dans la fenêtre **Mettre à jour un plan de gestion à distance**, cliquez sur **Mettre à jour**, activez le **Chat**, enregistrez les modifications, puis démarrez cette procédure à partir de l'étape 1.

Remarque
Si vous êtes hors ligne ou loin de la console pendant 15 minutes et que le chat n'est pas mis en attente, le système change automatiquement l'état du chat en **Annulé l'affectation**.

Affecter des sessions de chat à vous-même

Vous pouvez affecter à vous-même les sessions de chat qui sont dans le statut **Non affectés** ou **Affectés à d'autres utilisateurs**.

Pour affecter une session de chat à vous-même

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Localisez la session de chat que vous souhaitez réattribuer, puis cliquez dessus.

© Acronis International GmbH, 2003-2026

3. Cliquez sur **Me l'affecter**.
   La session de chat vous est affectée. Vous pouvez maintenant envoyer des messages dans ce chat.

   Remarque
   Si vous êtes hors ligne ou loin de la console pendant 15 minutes et que le chat n'est pas mis en attente, le système change automatiquement l'état du chat en **Annulé l'affectation**.

Réaffectation de sessions de chat

Vous pouvez réattribuer des sessions de chat pour vous assurer que le technicien le plus approprié les gère.

- Lorsque la session de chat n'est pas affectée.
- Lorsque vous souhaitez modifier l'administrateur d'une session de chat affectée.

Les administrateurs partenaires peuvent réattribuer une session de chat à un administrateur du même tenant partenaire ou à un administrateur d'un tenant client direct (si le mode de gestion du client est **Géré par le fournisseur de services**).

Les administrateurs clients peuvent réattribuer une session de chat active à un autre administrateur du même tenant client ou de ses unités.

Les administrateurs d'unité peuvent réattribuer une session de chat active à un autre administrateur de la même unité.

Pour réattribuer un chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Localisez la session de chat que vous souhaitez réattribuer, puis cliquez dessus.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Réattribuer**.
4. Dans la boîte de dialogue **Réattribuer le chat**, sélectionnez l'administrateur à qui vous souhaitez attribuer la session de chat, puis cliquez sur **Réattribuer**.
   La session de chat est réaffectée et vous ne pouvez plus y envoyer de messages. Un message système concernant la réaffectation est affiché aux administrateurs et à l'utilisateur distant.

Exportation de chats

L'historique des chats est stocké pendant 180 jours. Vous pouvez télécharger des chats importants ou une partie de ceux-ci et les enregistrer sous forme de fichiers `.txt` sur votre machine locale.

Pour exporter un chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Recherchez le chat que vous souhaitez exporter, puis cliquez dessus.
3. Cliquez sur l'icône représentant des points de suspension (...), puis cliquez sur **Exporter**.

© Acronis International GmbH, 2003-2026

4. Dans la boîte de dialogue **Exporter le chat**, effectuez l'une des actions suivantes :
   - Pour exporter l'historique complet de chat, sélectionnez **Exporter le chat complet**.
   - Pour exporter l'historique de chat pour une période spécifiée, cliquez sur **Exporter le chat de la période suivante**, puis sélectionnez une période prédéfinie (**Dernier jour**, **Dernière semaine**, **Dernier mois** ou **6 derniers mois**) ou une période personnalisée.
5. Cliquez sur **Exporter**.
   Un fichier `.txt` contenant l'historique de la discussion est enregistré sur votre machine locale, dans le dossier de téléchargement par défaut.

Filtrage des sessions de chat

Vous pouvez filtrer la liste des sessions de chat affichées sur la page **Chat** et afficher uniquement les sessions de chat avec des utilisateurs distants spécifiques.

Pour filtrer les sessions de chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Pour filtrer les sessions de chat dans la liste par utilisateurs distants, cliquez sur **Filtrer**, sélectionnez les utilisateurs distants, puis cliquez sur **Appliquer**.
   Seules les sessions de chat avec les utilisateurs que vous avez sélectionnés sont répertoriées à l'écran.

Recherche de messages dans les sessions de chat

Vous pouvez rechercher certains messages ou mots clés dans les sessions de chat ou afficher l'historique des chats pour une date spécifique.

Recherche dans une seule session de discussion

Pour effectuer une recherche dans une seule session de chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Cliquez sur la session de chat dans laquelle vous souhaitez effectuer une recherche.
3. Cliquez sur l'icône en forme de boucle.
4. [Facultatif] Pour voir l'historique du chat pour une date spécifique, cliquez sur l'icône de calendrier, puis sélectionnez la date.

   Remarque
   Seules les dates pour lesquelles l'historique du chat est disponible sont activées pour la sélection.

   Le système affiche l'historique du chat à partir de la date que vous avez sélectionnée.
5. Dans le champ de recherche, tapez le mot-clé ou le message que vous souhaitez trouver.
   Le système affiche le nombre de résultats correspondant à la requête de recherche. Vous pouvez utiliser les flèches pour passer au résultat suivant ou précédent.

Recherche dans plusieurs sessions de chat

© Acronis International GmbH, 2003-2026

Pour effectuer une recherche dans plusieurs sessions de chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Dans le champ de recherche, saisissez la chaîne, le mot-clé ou le message que vous souhaitez trouver.
   La liste des chats affiche uniquement les sessions avec des messages qui correspondent à la recherche.

Actions supplémentaires avec les sessions de chat

En fonction de l'état d'une session de chat, vous pouvez effectuer les actions supplémentaires suivantes : mettre en attente, reprendre, terminer, rouvrir, actions de ressource à distance.

Mettre en attente

Vous pouvez mettre temporairement en pause une session de chat active lorsque vous avez besoin de plus de temps pour répondre. Par exemple, pour trouver la solution au problème de l'utilisateur.

Pour mettre une session de chat en attente

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Cliquez sur le chat actif que vous souhaitez mettre en attente.
3. Cliquez sur le bouton de points de suspension (...), puis cliquez sur **Mettre en attente**.
   La session de chat est mise en attente. La balise **En attente** est affichée pour ce chat dans la liste des chats.

Reprendre

Vous pouvez reprendre une session de chat qui a été mise en attente et continuer la conversation avec l'utilisateur distant.

Pour reprendre une session de chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Cliquez sur le chat que vous souhaitez reprendre, puis cliquez sur **Reprendre le chat**.
   La session de chat reprend. Vous pouvez continuer à discuter avec l'utilisateur à distance.

Terminer le chat

Vous pouvez mettre fin à une session de chat active avec un utilisateur distant à tout moment. Le système enregistrera l'historique du chat et notifiera l'utilisateur distant que le chat a été fermé.

Pour mettre fin à une session de chat

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Cliquez sur le chat actif que vous souhaitez terminer.
3. Cliquez sur **Terminer le chat**.
   La session de chat est fermée. Le statut du chat passe à **Fermé** et, sur l'écran **Chats**, le chat est déplacé de la liste **Affecté à moi** vers la liste des chats **Fermé**.

© Acronis International GmbH, 2003-2026

Rouvert

Vous pouvez rouvrir une session de chat fermée et continuer la conversation avec l'utilisateur distant. Tous les messages des sessions de chat précédentes sont affichés dans le fil de discussion.

Pour rouvrir une session de chat fermée

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Dans la liste de chats **Fermé**, cliquez sur le chat fermé que vous souhaitez rouvrir.
3. Cliquez sur **Rouvrir le chat**.
   La session de chat est rouverte. L'état du chat change en **Affecté à moi** et sur l'écran **Chats**, le chat est déplacé de la liste de chats **Fermé** à la liste de chats **Affecté à moi**.

Actions à distance

À partir de **Chats**, vous pouvez effectuer des actions à distance sur vos ressources gérées ou accéder à plusieurs écrans.

Prérequis

Connect Client est installé sur l'ordinateur à partir duquel vous êtes connecté à la console Cyber Protect.

Pour effectuer une action à distance sur une ressource

1. Dans la console Cyber Protect, accédez à **Chat**.
2. Dans la liste des chats, cliquez sur une session de chat avec la ressource sur laquelle vous souhaitez effectuer l'action.
3. Cliquez sur l'icône de points de suspension (...) après le nom de la ressource, puis cliquez sur l'option qui correspond à l'action que vous souhaitez effectuer.

Option	Description
Connexion	Utilisez cette option pour vous connecter à la ressource distante.
Transférer des fichiers	Utilisez cette option pour transférer des fichiers vers la ressource distante.
Redémarrer	Utilisez cette option pour redémarrer la ressource distante.
Correctif	Utilisez cette option pour corriger la ressource distante.
Accéder à la ressource	Lorsque vous cliquez sur cette action, les options suivantes sont affichées : • **Détails** • **Inventaire** • **Surveillance** • **Plans** • **Alertes** • **Activités**

© Acronis International GmbH, 2003-2026

Option	Description
Détails	Cette option devient visible lorsque vous cliquez sur **Accéder à la ressource**. Utilisez cette option pour accéder aux détails de la ressource.
Inventaire	Cette option devient visible lorsque vous cliquez sur **Accéder à la ressource**. Utilisez cette option pour accéder à l'onglet **Inventaire** > **Matériel** des détails de la ressource.
Surveillance	Cette option devient visible lorsque vous cliquez sur **Accéder à la ressource**. Utilisez cette option pour accéder à l'onglet **Surveillance** des détails de la ressource.
Plans	Cette option devient visible lorsque vous cliquez sur **Accéder à la ressource**. Utilisez cette option pour accéder à l'onglet **Plans** des détails de la ressource.
Alertes	Cette option devient visible lorsque vous cliquez sur **Accéder à la ressource**. Utilisez cette option pour accéder à l'onglet **Alertes** des détails de la ressource.
Activités	Cette option devient visible lorsque vous cliquez sur **Accéder à la ressource**. Utilisez cette option pour accéder à l'onglet **Activités** des détails de la ressource.

Actions supplémentaires avec les messages de chat

Dans les sessions de chat actives, vous pouvez modifier ou supprimer les messages que vous avez envoyés à l'utilisateur distant.

Modifier le message

Vous pouvez modifier tout message que vous avez envoyé dans la session de chat.

Pour modifier un message dans la session de chat

1. Dans la fenêtre de chat, localisez le message que vous souhaitez modifier.
2. Survolez le message, puis cliquez sur l'icône de crayon qui apparaît.
3. Modifiez le message, puis appuyez sur **Entrée**.
   Les modifications sont enregistrées. Le message est marqué comme **Édité**.

Supprimer le message

© Acronis International GmbH, 2003-2026

Vous pouvez supprimer tout message que vous avez envoyé dans le chat.

Pour supprimer un message dans la session de chat

1. Dans la fenêtre de chat, localisez le message que vous souhaitez supprimer.
2. Survolez le message, puis cliquez sur l'icône de la corbeille qui apparaît.
3. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.
   Le message est supprimé du chat et n'est plus visible. Le système affiche l'heure de la suppression et votre nom.

Surveillance de l'intégrité et des performances de la ressource

Vous pouvez surveiller les paramètres système et l'intégrité des ressources de votre organisation. Si un paramètre est hors norme, vous en êtes informé immédiatement et pouvez résoudre le problème rapidement. Vous pouvez également configurer des alertes personnalisées et des mesures d'intervention automatiques. Il s'agit de mesures qui seront réalisées automatiquement pour résoudre les anomalies de comportement de la ressource.

Remarque
La fonctionnalité de surveillance nécessite l'installation de l'agent Protection version 15.0.35324 ou ultérieure sur les ressources.

Plans de surveillance

Pour commencer la surveillance des performances, du matériel, du logiciel, du système et des paramètres de sécurité de vos ressources gérées, appliquez-leur un plan de surveillance. Les plans de surveillance se composent de différents moniteurs que vous pouvez activer et configurer. Certains moniteurs prennent en charge le type de surveillance basé sur une anomalie. Pour plus d'informations sur les plans de surveillance, voir "Plans de surveillance" (p. 1561). Pour plus d'informations sur les moniteurs disponibles que vous pouvez configurer dans les plans de surveillance, reportez-vous à "Moniteurs configurables" (p. 1525).

Si, pour une raison quelconque, l'agent ne peut pas collecter de données d'une ressource, le système génère une alerte.

Types de surveillance

Vous devez configurer le type de surveillance pour chaque moniteur que vous activez dans le plan. Le type de surveillance détermine l'algorithme qu'utilisera le moniteur pour estimer le comportement normal et l'écart de la ressource. Il existe deux types de surveillance : la surveillance basée sur un seuil et celle basée sur une anomalie. Certains moniteurs ne prennent en charge que le type de surveillance basé sur un seuil.

© Acronis International GmbH, 2003-2026

La surveillance basée sur un seuil vérifie si les valeurs des paramètres se trouvent au-dessus ou en dessous d'une valeur de seuil que vous configurez. Grâce à ce type de surveillance, vous avez la charge de définir les valeurs de seuil correctes pour les ressources. Le système détermine le comportement normal en fonction de ces valeurs de seuil statiques, sans prendre en compte d'autres conditions spécifiques qui pourraient provoquer ce comportement. C'est la raison pour laquelle la surveillance basée sur un seuil peut être moins précise que la surveillance basée sur une anomalie.

La surveillance basée sur une anomalie utilise l'apprentissage automatique pour créer les modèles de comportement normal d'une ressource et détecter un comportement anormal. Pour plus d'informations, voir "Surveillance basée sur une anomalie" (p. 1524).

Surveillance basée sur une anomalie

La surveillance basée sur une anomalie utilise les modèles d'apprentissage automatique afin de créer les modèles de comportement normal d'une ressource et de détecter les anomalies (crêtes inattendues dans les données temporelles) dans le comportement de la ressource. Lorsque vous activez ce type de surveillance, le système crée un modèle et démarre son autoformation, puis ajuste le modèle de la ressource spécifique en fonction des données collectées sur la ressource. Cela signifie que, au début de la période de formation, les données risquent de ne pas être totalement pertinentes. La création d'un modèle fiable nécessite au moins trois semaines de formation du modèle. À mesure que le système collecte des données et analyse les ensembles de données historiques, il affine le modèle petit à petit et crée les seuils supérieur et inférieur dynamiques de chaque mesure de la ressource. Ce type de surveillance est plus souple que la surveillance basée sur des seuils, car le système surveille les valeurs des paramètres et leur contexte. Par exemple, il peut être normal qu'une ressource spécifique ait une charge élevée à certaines heures de la journée. Le type de surveillance basée sur les seuils interpréterait par erreur ce comportement comme étant anormal et déclencherait une alerte.

Vous pouvez réinitialiser les modèles d'apprentissage automatique d'une ressource. Dans ce cas, le système supprime toutes les données et tous les modèles des moniteurs appliqués à la ressource. Pour plus d'informations, voir "Réinitialisation des modèles d'apprentissage automatique" (p. 1570).

Plates-formes prises en charge pour la surveillance

La fonctionnalité de surveillance est prise en charge pour les systèmes d'exploitation suivants.

Versions de Windows prises en charge	Versions de macOS prises en charge
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura) • macOS 14.x (Sonoma) • macOS 15.x (Sequoia)

© Acronis International GmbH, 2003-2026

Versions de Windows prises en charge	Versions de macOS prises en charge
• Windows Server 2016 • Windows Server 2019 • Windows Server 2022	

Moniteurs configurables

La fonctionnalité de surveillance prend en charge les contrôles suivants, divisés en six catégories : Matériel, Performance, Logiciel, Système, Sécurité et Personnalisé.

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
Matériel					
Espace disque	Surveille l'espace libre sur un lecteur spécifique de la ressource.	Windows macOS	1 minute	Oui	Protection standard (mode de licence basé sur le service) Sécurité et RMM (mode de licence basé sur la solution)
Température du processeur	Surveille la température du processeur.	Windows macOS	30 s	Oui	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Température du processeur graphique	Surveille la température du processeur	Windows macOS	30 s	Oui	Sécurité et RMM (mode de licence

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
	graphique.				basé sur la solution) Service RMM (mode de licence basé sur le service)
Modifications apportées au matériel	Surveille les modifications du matériel (ajout, suppression ou remplacement de matériel) sur une ressource.	Windows macOS	24 heures	Non	Protection standard (mode de licence basé sur le service) Sécurité et RMM (mode de licence basé sur la solution)
Performance					
Utilisation du processeur	Surveille l'utilisation globale du processeur (par tous les processeurs de la ressource).	Windows macOS	30 s	Oui	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Utilisation de la mémoire	Surveille l'utilisation globale de la mémoire (par tous les logements	Windows macOS	30 s	Oui	Sécurité et RMM (mode de licence basé sur la solution) Service RMM

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
	mémoire sur la ressource).				(mode de licence basé sur le service)
Vitesse de transfert du disque	Surveille la vitesse de lecture et d'écriture de chaque disque physique sur la ressource.	Windows macOS	30 s	Oui	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Utilisation du réseau	Surveille les trafics entrant et sortant pour chaque carte réseau de la ressource.	Windows macOS	30 s	Oui	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Utilisation du processeur par processus	Surveille l'utilisation du processeur par certains processus.	Windows macOS	30 s	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Utilisation de	Surveille	Windows	30 s	Non	Sécurité et

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
la mémoire par processus	l'utilisation de la mémoire par le processus sélectionné.	macOS			RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Vitesse de transfert du disque par processus	Surveille la vitesse de lecture et d'écriture du processus sélectionné.	Windows macOS	30 s	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Utilisation du réseau par processus	Surveille le trafic entrant et sortant du processus sélectionné.	Windows macOS	30 s	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Logiciel					
État du service Windows	Surveille l'état du service Windows sélectionné (en cours	Windows	30 s	Non	Sécurité et RMM (mode de licence basé sur la solution)

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
	d'exécution ou arrêté).				Service RMM (mode de licence basé sur le service)
État du processus	Surveille l'état du processus sélectionné (en cours d'exécution ou arrêté).	Windows macOS	30 s	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Logiciel installé	Surveille l'installation, la mise à jour ou la suppression des applications logicielles.	Windows macOS	24 heures	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Système					
Dernier redémarrage du système	Surveille le moment de redémarrage de la ressource.	Windows macOS	1 heure	Non	Protection standard (mode de licence basé sur le service) Sécurité et RMM (mode de licence

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
					basé sur la solution)
Journal des événements Windows	Surveille des événements essentiels spécifiques dans les journaux d'événements Windows.	Windows	10 min	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Taille des fichiers et dossiers	Surveille la taille totale des fichiers ou dossiers sélectionnés.	Windows macOS	10 min	Non	Protection standard (mode de licence basé sur le service) Sécurité et RMM (mode de licence basé sur la solution)
Sécurité					
État de Windows Update	Surveille l'état de Windows Update de la ressource et indique si les dernières mises à jour sont installées.	Windows	15 min	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
État du pare-feu	Surveille l'état du pare-feu intégré ou tiers qui est installé sur la ressource.	Windows macOS	5 min	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
État du logiciel antimalware	Surveille l'état du logiciel antimalware intégré ou tiers qui est installé sur la ressource.	Windows macOS	5 min	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
Échecs de connexion	Surveille les tentatives de connexion infructueuses sur la ressource.	Windows	1 heure	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)
État de l'exécution automatique	Surveille si la fonctionnalité d'exécution automatique pour le support de stockage	Windows	1 heure	Non	Sécurité et RMM (mode de licence basé sur la solution)

© Acronis International GmbH, 2003-2026

Moniteur	Description	Systèmes d'exploitation pris en charge	Fréquence de collecte des données	Prise en charge de la surveillance basée sur une anomalie	Disponibilité
	amovible est activée.				Service RMM (mode de licence basé sur le service)
Personnalisé					
Personnalisé	Surveille les objets personnalisés par l''exécution de scripts.	Windows macOS	personnalisé	Non	Sécurité et RMM (mode de licence basé sur la solution) Service RMM (mode de licence basé sur le service)

Paramètres du moniteur Espace disque

Le moniteur **Espace disque** surveille l'espace libre sur un lecteur spécifique de la ressource.

Remarque
Lors du calcul de l'espace, le moniteur utilise des octets binaires (1 024 octets par Ko, 1 024 Ko par Mo et 1 024 Mo par Go) pour les ressources Windows et macOS.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Lecteur	Lecteur que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Lecteur système** —Il s'agit de la valeur par défaut. Il s'agit du lecteur ou de la partition sur un ordinateur où le système d'exploitation est installé. Sur les systèmes Windows, le lecteur système est généralement le lecteur C: par défaut, mais peut varier en

© Acronis International GmbH, 2003-2026

Paramètre	Description
	fonction de la configuration. • **N'importe quel lecteur**
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Inférieur à** —Il s'agit de la valeur par défaut. • **Inférieur ou égal à**
Seuil d'espace libre sur le disque	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 20.
Inclure les lecteurs amovibles	Ce paramètre est disponible si la valeur **Lecteur** est **N'importe quel lecteur**. Sélectionnez ce paramètre si vous souhaitez ajouter des lecteurs amovibles tels que des lecteurs flash USB à surveiller. Ce paramètre est désactivé par défaut.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 30.
Surveillance basée sur une anomalie	
Lecteur	Lecteur que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Lecteur système** —Il s'agit de la valeur par défaut. Il s'agit du lecteur ou de la partition sur un ordinateur où le système d'exploitation est installé. Sur les systèmes Windows, le lecteur système est généralement le lecteur C: par défaut, mais peut varier en fonction de la configuration. • **N'importe quel lecteur**
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. La valeur par défaut est 30 minutes.

© Acronis International GmbH, 2003-2026

Paramètres du moniteur Température du processeur

Le moniteur **Température du processeur** surveille la température du processeur de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
La température du processeur a dépassé (C°)	Valeur minimale de la mesure surveillée. Si la valeur est dépassée, le système génère une alerte. Saisissez une valeur d'entier (C). La valeur par défaut est 80.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie

© Acronis International GmbH, 2003-2026

Paramètre	Description
	avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 15.

Paramètres du moniteur Température du processeur graphique

Le moniteur **Température du processeur graphique** surveille la température du processeur graphique de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
La température du processeur graphique a dépassé	Valeur minimale de la mesure surveillée. Si la valeur est dépassée, le système détecte une anomalie. Saisissez une valeur d'entier (C). La valeur par défaut est 80.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	• **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 15.

Paramètres du moniteur Modifications apportées au matériel

Le moniteur **Modifications apportées au matériel** surveille les modifications du matériel (ajout, suppression ou remplacement de matériel) sur une ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Composants matériels	Sélectionnez un ou plusieurs composants matériels dont vous souhaitez surveiller les modifications. Les valeurs suivantes sont disponibles. • **Tout** — Il s'agit de la valeur par défaut. • **Carte mère** • **CPU** • **RAM** • **Disque** • **GPU** • **Adaptateur réseau**
Que surveiller ?	Spécifiez les modifications pour lesquelles vous souhaitez surveiller les composants matériels sélectionnés. Vous pouvez sélectionner plusieurs éléments dans la liste. Les valeurs suivantes sont disponibles. • **Toute modification** —Il s'agit de la valeur par défaut. • **Nouveaux composants ajoutés** • **Composants remplacés** • **Composants supprimés**

Paramètres du moniteur Utilisation du processeur

Le moniteur **Utilisation du processeur** surveille l'utilisation totale du processeur de la ressource. Si la ressource comprend plusieurs processeurs, l'utilisation totale du processeur correspond à la somme des utilisations de tous les processeurs.

Vous pouvez configurer les paramètres suivants pour le moniteur.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Surveillance basée sur un seuil	
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil d'utilisation du processeur	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 90.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation :

© Acronis International GmbH, 2003-2026

Paramètre	Description
	1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 15.

Paramètres du moniteur Utilisation de la mémoire

Le moniteur **Utilisation de la mémoire** surveille l'utilisation totale de la mémoire par tous les modules de mémoire de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	• **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil d'utilisation de la mémoire	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 90.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 30 minutes.

Paramètres du moniteur Vitesse de transfert du disque

Le moniteur **Vitesse de transfert du disque** surveille la vitesse de lecture et d'écriture de chaque disque physique sur la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Que surveiller ?	Sélectionnez la vitesse que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Vitesse de lecture et d'écriture**. Il s'agit de la valeur par défaut. • **Vitesse de lecture** • **Vitesse d'écriture**
Opérateur de la vitesse de lecture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	Les valeurs suivantes sont disponibles. • **Supérieur à**. Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse de lecture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse de lecture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur de la vitesse d'écriture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse d'écriture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse d'écriture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Que surveiller ?	Sélectionnez la vitesse que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Vitesse de lecture et d'écriture**. Il s'agit de la valeur par défaut. • **Vitesse de lecture** • **Vitesse d'écriture**
Niveau de sensibilité	Le niveau de sensibilité agit comme un filtre préliminaire sur les anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois

© Acronis International GmbH, 2003-2026

Paramètre	Description
	la valeur de l'écart type.
Durée de l'anomalie (Vitesse de lecture)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.
Durée de l'anomalie (Vitesse d'écriture)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.

Paramètres du moniteur Utilisation du réseau

Le moniteur **Utilisation du réseau** surveille les trafics entrant et sortant pour chaque carte réseau de la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Surveillance basée sur un seuil	
Direction du trafic	Direction du trafic que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Trafics entrant et sortant**. Il s'agit de la valeur par défaut. • **Trafic entrant** • **Trafic sortant**
Opérateur du trafic entrant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic entrant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic	Le système ne générera une alerte pour un problème détecté que si la

© Acronis International GmbH, 2003-2026

Paramètre	Description
entrant	valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur du trafic sortant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic sortant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic sortant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Surveillance basée sur une anomalie	
Période d'entraînement du modèle	Période pendant laquelle le système formera les modèles d'apprentissage automatique à partir des données collectées auprès des agents, puis créera le modèle de comportement normal de la ressource. Plus l'entraînement du modèle est long, plus le modèle de comportement créé par le système est précis à long terme. Nous vous recommandons de définir un entraînement du modèle d'au moins vingt-et-un jours. Saisissez une valeur d'entier (jours). La valeur par défaut est 21.
Recevoir des alertes d'anomalie pendant la période de formation	Si vous sélectionnez ce paramètre, vous recevrez des alertes en cas d'anomalie pendant l'entraînement du modèle. Ces alertes peuvent être erronées, car l'entraînement des modèles est encore en cours et peut manquer de précision. Ce paramètre est sélectionné par défaut.
Direction du trafic	• **Trafics entrant et sortant**. Il s'agit de la valeur par défaut. • **Trafic entrant** • **Trafic sortant**
Niveau de	Le niveau de sensibilité agit comme un filtre préliminaire sur les

© Acronis International GmbH, 2003-2026

Paramètre	Description
sensibilité	anomalies si leurs valeurs sont comprises dans une plage spécifique. Ce filtre fonctionne indépendamment de l'algorithme de détection des anomalies. Il vise à arrêter le traitement des anomalies comprises dans la plage spécifiée par l'algorithme de détection des anomalies. Pendant la période de formation : 1. L'algorithme est formé à l'aide des données collectées pendant la formation. 2. L'algorithme détecte les anomalies dans les données de formation. 3. Un filtrage basé sur la moyenne et l'écart type est appliqué. 4. Toutes les anomalies détectées dans l'intervalle spécifié sont filtrées. 5. Dans les points de données anormaux restants, l'anomalie avec le niveau le plus faible est sélectionnée. Ce niveau (numéro flottant compris entre 0 et 1) est enregistré dans le modèle. Pendant la prévision : 1. L'algorithme prévoit les anomalies dans les données d'inférence. 2. Les anomalies prévues sont filtrées en fonction de la moyenne et de l'écart type, conformément au niveau de sensibilité. 3. Les anomalies restantes sont filtrées encore en fonction du principe suivant : les valeurs au-dessus du niveau de seuil sont considérées comme des anomalies et celles en dessous du niveau de seuil sont considérées comme ayant un comportement normal. Les valeurs suivantes sont disponibles. • **Bas** : le niveau bas est égal à la valeur de la moyenne et à la valeur de l'écart type. • **Normal** : il s'agit de la valeur par défaut. Le niveau normal est égal à la valeur de la moyenne et à deux fois la valeur de l'écart type. • **Élevé** : le niveau élevé est égal à la valeur de la moyenne et à trois fois la valeur de l'écart type.
Durée de l'anomalie (entrante)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.
Durée de l'anomalie (sortante)	Le système ne générera une alerte pour une anomalie détectée que si le comportement anormal persiste pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 25.

© Acronis International GmbH, 2003-2026

Paramètres du moniteur Utilisation du processeur par processus

Le moniteur **Utilisation du processeur par processus** surveille l'utilisation du processeur par le processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 100 (%). La valeur par défaut est 90.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur Utilisation de la mémoire par processus

Le moniteur **Utilisation de la mémoire par processus** surveille l'utilisation de la mémoire par le processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies.

Remarque
Les agents utilisent l'ensemble de travail total des processus (privés et partagés) pour estimer la taille de la mémoire utilisée par processus. C'est la raison pour laquelle les informations affichées dans le widget peuvent indiquer une taille de mémoire utilisée différente de celle affichée dans le Gestionnaire des tâches Windows (ensemble de travail privé).

© Acronis International GmbH, 2003-2026

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko). La valeur par défaut est 1.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur Vitesse de transfert du disque par processus

Le moniteur **Vitesse de transfert du disque par processus** surveille la vitesse de lecture et d'écriture du processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Que surveiller ?	Vitesse que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Vitesse de lecture et d'écriture**. Il s'agit de la valeur par défaut. • **Vitesse de lecture** • **Vitesse d'écriture**
Opérateur de la vitesse	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur.

© Acronis International GmbH, 2003-2026

Paramètre	Description
de lecture	Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse de lecture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse de lecture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur de la vitesse d'écriture	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil de la vitesse d'écriture	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période de la vitesse d'écriture	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur Utilisation du réseau par processus

Le moniteur **Utilisation du réseau par processus** surveille les trafics entrant et sortant du processus sélectionné. Si plusieurs instances d'un même processus sont présentes, le système surveille l'utilisation totale par toutes ces instances et génère une alerte lorsque les conditions sont remplies pour toutes les instances.

Vous pouvez configurer les paramètres suivants pour le moniteur.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du processus, sans l'extension.
Direction du trafic	Direction du trafic que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **Trafics entrant et sortant**. Il s'agit de la valeur par défaut. • **Trafic entrant** • **Trafic sortant**
Opérateur du trafic entrant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic entrant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic entrant	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.
Opérateur du trafic sortant	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Supérieur ou égal à** • **Inférieur à** • **Inférieur ou égal à**
Seuil du trafic sortant	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Ko/s). La valeur par défaut est 0 Ko/s.
Période du trafic sortant	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 5.

Paramètres du moniteur de statut du service Windows

Le **statut du service Windows** surveille si le service Windows sélectionné est en cours d'exécution ou est arrêté.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du service	Nom du service Windows que vous souhaitez surveiller. Vous pouvez sélectionner un nom de service dans la liste des services Windows. La liste répertorie tous les agents du tenant après l'analyse réussie de l'inventaire logiciel sur les ressources. Vous pouvez également ajouter un nom de service non répertorié. Il s'agit de la seule option disponible si l'analyse de l'inventaire logiciel n'a pas été effectuée sur les ressources.
État du service	Si le service est dans l'état sélectionné, le système génère un événement. Les valeurs suivantes sont disponibles. • **En cours d'exécution** • **Arrêté**—Il s'agit de la valeur par défaut.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 1.

Paramètres du moniteur État du processus

Le moniteur **État du processus** surveille si le processus sélectionné est en cours d'exécution ou est arrêté. Si plusieurs instances d'un même processus sont présentes, le système surveille chaque instance du processus et génère une alerte lorsque les conditions sont remplies pour toutes les instances du processus.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du processus	Nom du processus que vous souhaitez surveiller. Saisissez le nom du fichier exécutable, sans l'extension.
État du processus	Si le processus est dans l'état sélectionné, le système génère un événement. Les valeurs suivantes sont disponibles.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	• **En cours d'exécution** • **Arrêté**—Il s'agit de la valeur par défaut.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 60 (min). La valeur par défaut est 1.

Paramètres du moniteur Logiciel installé

Le moniteur **Logiciel installé** surveille l'installation, les mises à jour ou la suppression des applications logicielles sur la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Quel logiciel surveiller ?	Spécifiez le logiciel que vous souhaitez surveiller. Les valeurs suivantes sont disponibles. • **N'importe quel logiciel** —Il s'agit de la valeur par défaut. • **Logiciel spécifique**
Noms de logiciel	Ce paramètre devient disponible si vous sélectionnez la valeur **Logiciel spécifique** pour **Quel logiciel surveiller**. Saisissez le nom d'une ou de plusieurs applications logicielles. Vous pouvez sélectionner un nom d'application logicielle dans la liste des services Windows. La liste répertorie tous les agents du tenant après l'analyse réussie de l'inventaire logiciel sur les ressources. Vous pouvez également ajouter un nom d'application logiciel non répertorié. Il s'agit de la seule option disponible si l'analyse de l'inventaire logiciel n'a pas été effectuée sur les ressources.
Statut d'installation	Spécifiez si vous souhaitez surveiller les logiciels installés, non installés ou mis à jour. Les valeurs suivantes sont disponibles. • **Installé** - Il s'agit de la valeur par défaut. Si vous sélectionnez cette valeur, le moniteur génère une alerte lorsqu'une nouvelle application logicielle est installée sur la ressource. • **Mis à jour** : si vous sélectionnez cette valeur, le moniteur génère une alerte lors de la mise à jour d'une application logicielle. • **Non installé** : si vous sélectionnez cette valeur, le moniteur génère une alerte lorsqu'une application logicielle est désinstallée ou non disponible sur la ressource.

© Acronis International GmbH, 2003-2026

Paramètres du moniteur Dernier redémarrage du système

Dernier redémarrage du système lors du dernier redémarrage de la ressource.

Vous pouvez configurer le paramètre suivant du moniteur.

Paramètre	Description
La ressource n'a pas été redémarrée pour	Période (en nombre de jours) depuis le dernier redémarrage de la ressource. Si la ressource n'a pas été redémarrée pendant une période plus longue que celle que vous spécifiez, le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 180 (jours). La valeur par défaut est 30.

Paramètres du moniteur du journal des événements Windows

Le **Journal des événements Windows** surveille des événements critiques spécifiques dans les journaux des événements Windows.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Nom du journal des événements	Sélectionnez un journal des événements dans la liste des journaux des événements Windows disponibles dans l'Observateur d'événements Windows. Les valeurs suivantes sont disponibles. • **N'importe lequel** —Il s'agit de la valeur par défaut. • **Application** • **Sécurité** • **Système**
Source d'événement	Nom de la source d'événement Vous pouvez sélectionner la valeur dans la liste des sources d'événements collectées dans tous les agents du tenant ou saisissez le nom d'une nouvelle source manuellement. Si l'analyse Inventaire du logiciel est désactivée pour le tenant, la liste des sources d'événements est vide.
Mode de correspondance	Vous pouvez spécifier dans ce champ si les paramètres **Identifiants d'événement**, **Type d'événement** et **Description d'événement** doivent être connectés à l'aide de l'opérateur **N'importe lequel** ou **Tout**. Les valeurs suivantes sont disponibles. • **N'importe lequel** —Il s'agit de la valeur par défaut. Une alerte est générée uniquement si l'un des critères sélectionnés correspond.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	• **Tout** — Une alerte est générée uniquement si tous les critères sélectionnés correspondent.
Identifiants d'événement	Saisissez un ou plusieurs identifiants d'événement en les séparant par une virgule. Si le système trouve dans le journal des événements l'un des codes d'événement que vous avez saisis dans ce champ, il génère une alerte.
Type d'événement	Sélectionnez un ou plusieurs types d'événements à surveiller. Les valeurs suivantes sont disponibles. • **N'importe lequel** — Il s'agit de la valeur par défaut. • **Erreur** • **Avertissement** • **Informations** • **Audit de succès** • **Audit d'échec**
Description d'événement	Mots-clés ou expressions spécifiques figurant dans la description d'événement que vous recherchez. Chaque mot-clé ou expression que vous saisissez doit être mis entre guillemets et ils doivent tous être séparés par une virgule. Si le système trouve l'un des mots-clés ou expressions que vous avez saisis, il génère une alerte.
Nombre d'occurrences	Nombre minimal d'occurrences d'un événement dans le journal pendant la période pour que le système génère une alerte. Saisissez une valeur d'entier dans la plage comprise entre 1 et 1 000.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier, puis sélectionnez l'unité : minutes ou heures. La valeur par défaut est 60 minutes.

Paramètres du moniteur Taille des fichiers et dossiers

Le moniteur **Taille des fichiers et dossiers** surveille la taille totale des fichiers ou dossiers sélectionnés.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Fichiers ou dossiers à surveiller	Chemin d'accès aux fichiers ou dossiers que vous souhaitez surveiller. Vous pouvez également spécifier les fichiers ou dossiers que vous souhaitez exclure de la surveillance. Vous pouvez utiliser les caractères génériques suivants.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	• * — Pour zéro ou plusieurs caractères dans un nom de fichier ou de dossier • ? — Pour exactement un caractère dans un nom de fichier ou de dossier Pour les ressources Windows : • Le chemin d'accès complet doit commencer par la lettre de lecteur, suivie du séparateur :\. • Vous pouvez utiliser une barre oblique ou une barre oblique inverse comme caractère de séparation des chemins d'accès. • Le nom du fichier ou du dossier ne doit pas se terminer par un espace ou un point. Pour les ressources macOS : • Le chemin d'accès complet doit commencer par le répertoire racine. • Vous pouvez utiliser une barre oblique comme caractère de séparation des chemins d'accès. • Le nom du fichier ou du dossier ne doit pas se terminer par un espace ou un point.
Opérateur	L'opérateur est une fonctionnalité conditionnelle qui définit la méthode de mesure des performances sur l'indicateur. Les valeurs suivantes sont disponibles. • **Supérieur à** —Il s'agit de la valeur par défaut. • **Inférieur à**
Valeur de seuil	La valeur de seuil et la valeur **Opérateur** déterminent les performances normales de la mesure surveillée. Lorsque la valeur de la mesure surveillée est hors norme, le système génère une alerte. Saisissez une valeur d'entier (Mo).
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 10 et 60 (min). La valeur par défaut est 10.

Paramètres du moniteur de statut de Windows Update

Le **statut de Windows Update** surveille l'état de Windows Update de la ressource et indique si les dernières mises à jour sont installées.

Si vous activez ce moniteur, le système génère une alerte dans les cas suivants.

- Windows Update est désactivé sur la ressource.
- Windows Update est activé sur la ressource, mais les dernières mises à jour n'ont pas été installées.

© Acronis International GmbH, 2003-2026

Paramètres du moniteur État du pare-feu

Le moniteur **État du pare-feu** surveille l'état du pare-feu intégré ou tiers qui est installé sur la ressource.

Si vous activez ce moniteur, le système génère une alerte dans les cas suivants.

- Le pare-feu intégré du système d'exploitation (Pare-feu Windows Defender ou pare-feu macOS) est désactivé et aucun pare-feu tiers n'est en cours d'exécution.
- Le pare-feu Windows Defender est désactivé pour les réseaux publics.
- Le pare-feu Windows Defender est désactivé pour les réseaux privés.
- Le pare-feu Windows Defender est désactivé pour les réseaux de domaine.

Paramètres du moniteur Échecs de connexion

Le moniteur **Échecs de connexion** surveille les tentatives de connexion infructueuses sur la ressource.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Seuil de tentatives de connexion infructueuses	La valeur de seuil détermine les limites de performances normales de la mesure surveillée. Lorsque la valeur de seuil est dépassée, la valeur est hors norme. Saisissez une valeur d'entier. La valeur par défaut est 60.
Période	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée. Saisissez une valeur d'entier dans la plage comprise entre 1 et 24, puis sélectionnez une unité : heures ou jours. La valeur par défaut est 12.

Paramètres du moniteur État du logiciel antimalware

Le moniteur **État du logiciel antimalware** surveille l'état du logiciel antimalware intégré ou tiers qui est installé sur la ressource.

Si vous activez ce moniteur, le système génère une alerte lorsqu'il identifie l'une des conditions suivantes.

- Le logiciel antimalware n'est pas installé sur la ressource.
- Le logiciel antimalware est installé, mais n'est pas en cours d'exécution.
- Le logiciel antimalware est installé et est en cours d'exécution, mais les définitions de malware ne sont pas à jour.

© Acronis International GmbH, 2003-2026

Remarque

Cette condition est vérifiée pour les systèmes d'exploitation Windows et Windows Server.

Système d'exploitation	Logiciel antimalware pris en charge
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton Antivirus • SentinelOne • Trend Micro Endpoint Security with Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security

© Acronis International GmbH, 2003-2026

Système d'exploitation	Logiciel antimalware pris en charge
	Remarque Le moniteur peut fonctionner avec d'autres plateformes antimalware, mais cela n'est pas garanti.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **Remarque** Le moniteur peut fonctionner avec d'autres plateformes antimalware, mais cela n'est pas garanti.

Paramètres du moniteur État de la fonctionnalité d'exécution automatique

Le moniteur **État de la fonctionnalité d'exécution automatique** surveille si la fonctionnalité d'exécution automatique pour le support amovible est activée.

Pour des raisons de sécurité, nous vous recommandons de désactiver sur la ressource la fonctionnalité d'exécution automatique pour le support amovible. Si la fonctionnalité est activée, le système génère une alerte.

Paramètres du moniteur personnalisé

Le moniteur **Personnalisé** surveille les objets personnalisés par l'exécution d'un script.

Si le script a été exécuté, mais a renvoyé un code différent de 0, le système génère une alerte.

Vous pouvez configurer les paramètres suivants pour le moniteur.

Paramètre	Description
Script à exécuter	Liste des scripts prédéfinis dans le référentiel de scripts.

© Acronis International GmbH, 2003-2026

Paramètre	Description
Planification	Heure d'exécution du script et (facultatif) conditions supplémentaires devant être remplies pour que le script s'exécute. Les valeurs suivantes sont disponibles. • **Planifier selon l'horaire** — Le script s'exécute à l'heure exacte, les jours, les semaines ou les mois que vous indiquez. Il s'agit de la valeur par défaut. **Type de planification** — **Par heure**, **Par jour** ou **Par mois** **Exécuter sur une plage de dates** — Plage d'exécution du script. • **Lorsque l'utilisateur se connecte au système** — Le script s'exécute lorsqu'un utilisateur se connecte à la ressource. • **Lorsque l'utilisateur se connecte au système** — Le script s'exécute lorsqu'un utilisateur se déconnecte de la ressource. • **Au démarrage du système** — Le script s'exécute au démarrage du système d'exploitation de la ressource. • **Lorsque le système est arrêté** — Le script s'exécute à l'arrêt de la ressource. • **Lorsque le système est en ligne** — Le script s'exécute lorsque la ressource devient disponible en ligne. **Conditions de démarrage** — La tâche est effectuée à un moment ou à un événement spécifié uniquement si la condition est remplie. Si plusieurs conditions sont sélectionnées, toutes doivent être remplies simultanément pour permettre le démarrage de la tâche. Par défaut, la condition **Empêcher l'activation du mode veille ou veille prolongée pour démarrer une tâche planifiée** est sélectionnée. **Si les conditions de démarrage ne sont pas remplies, exécutez quand même la tâche par la suite** — Par défaut, cette condition est activée. La valeur par défaut est 1 heure.
Compte pour l'exécution du script	Compte sur lequel s'exécutera le script. Les valeurs suivantes sont disponibles. • **Compte système** — Il s'agit de la valeur par défaut. • **Compte actuellement connecté**
Durée maximale	Période maximale pendant laquelle le script peut s'exécuter sur la ressource. Si le script ne se termine pas pendant cette période, l'opération échoue. Saisissez une valeur d'entier dans la plage comprise entre 1 et 1 440 (minutes). La valeur par défaut est 3 minutes.
Stratégie d'exécution PowerShell	Stratégie d'exécution PowerShell. Les valeurs suivantes sont disponibles.

© Acronis International GmbH, 2003-2026

Paramètre	Description
	• **Undefined** • **AllSigned** • **Bypass** — Il s'agit de la valeur par défaut. • **RemoteSigned** • **Restricted** • **Unrestricted** Pour plus d'informations sur ces valeurs, reportez-vous à la documentation Microsoft.

Plans de surveillance

Les plans de surveillance sont des plans que vous appliquez aux ressources que vous gérez afin d'activer et de configurer la fonctionnalité de surveillance.

Si aucun plan de surveillance n'est appliqué à une ressource, les fonctionnalités de surveillance ne seront pas disponibles pour la ressource.

Remarque
La disponibilité de cette fonctionnalité et les paramètres que vous pouvez configurer dans le plan de surveillance dépendent de la licence que vous possédez.

Création d'un plan de surveillance

Vous pouvez créer un plan de surveillance, puis ajouter des ressources afin de configurer la fonctionnalité de surveillance sur les ressources gérées.

Prérequis

La version de l'agent installée sur la ressource prend en charge la fonctionnalité de surveillance.

Pour créer un plan de surveillance

À partir de Plans de surveillance

1. Dans la console Protection, accédez à **Gestion** > **Plans de surveillance**.
2. Créez un plan de surveillance en utilisant l'une des deux options.
   - Si la liste ne comprend aucun plan de surveillance, cliquez sur **Créer**.
   - Si la liste comprend des plans de surveillance, cliquez sur **Création d'un plan**.
3. Dans la fenêtre **Créer un plan de surveillance**, selon la licence de votre tenant, procédez comme suit :
   - Si le tenant utilise la protection standard, les quatre moniteurs suivants sont ajoutés automatiquement au plan de surveillance : Espace disque, Modifications apportées au matériel, Dernier redémarrage du système et Taille des fichiers et dossiers.

© Acronis International GmbH, 2003-2026

- Si le pack RMM est activé pour votre tenant (mode de licence basé sur le service) ou si vous utilisez Sécurité et RMM (mode de licence basé sur la solution), sélectionnez l'une des options de modèle, puis cliquez sur **Suivant**.

Option	Description
Recommandé	Sélectionnez cette option pour créer un plan de surveillance avec la configuration de surveillance par défaut.
Personnalisé	Utilisez cette option pour créer un plan de surveillance de toutes pièces.

4. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **OK**.
5. [Facultatif] Pour ajouter un moniteur au plan, cliquez d'abord sur **Ajouter un moniteur**, puis sur le moniteur dans la liste et enfin sur **Ajouter**.

   Remarque
   Les paramètres du moniteur seront remplis automatiquement avec les valeurs par défaut. Vous pouvez ajouter jusqu'à 30 moniteurs à un plan de surveillance.

6. [Facultatif] Dans l'écran Paramètres de moniteur, modifiez les paramètres par défaut du moniteur et des alertes, puis cliquez sur **Terminé**.

   Remarque
   Vous pouvez configurer différents paramètres pour chaque moniteur. Pour plus d'informations, voir "Moniteurs configurables" (p. 1525) et "Configuration des alertes de surveillance" (p. 1571).

7. [Facultatif] Pour supprimer un moniteur, cliquez sur l'icône de la corbeille, puis cliquez sur **Supprimer**.
8. [Facultatif] Pour ajouter des ressources au plan :
   a. Cliquez sur **Ajouter des ressources**.
   b. Sélectionnez les ressources, puis cliquez sur **Ajouter**.
   c. Si vous avez des problèmes de compatibilité à résoudre, suivez la procédure décrite dans "Résolution des problèmes de compatibilité" (p. 253).
9. Cliquez sur **Créer**.

À partir de tous les terminaux

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de surveillance.
3. Cliquez sur **Protection**.
4. Selon qu'un plan de surveillance est appliqué, ou pas, à la ressource, effectuez l'une des opérations suivantes :

© Acronis International GmbH, 2003-2026

- Si un plan de surveillance est déjà appliqué à la ressource, cliquez sur **Création d'un plan**, puis sélectionnez **Surveillance**.
- Si aucun plan de surveillance n'est appliqué à la ressource, cliquez sur **Ajouter un plan**, puis sur **Création d'un plan**, puis sélectionnez **Surveillance**.

5. Dans la fenêtre **Créer un plan de surveillance**, sélectionnez l'une des options de modèle, puis cliquez sur **Suivant**.

Option	Description
Recommandé	Sélectionnez cette option pour créer un plan de surveillance avec la configuration de surveillance par défaut.
Personnalisé	Utilisez cette option pour créer un plan de surveillance de toutes pièces.

6. [Facultatif] Pour modifier le nom par défaut du plan, cliquez sur l'icône en forme de crayon, saisissez le nom du plan, puis cliquez sur **OK**.
7. [Facultatif] Si vous souhaitez modifier les paramètres par défaut du moniteur et des alertes, configurez les nouvelles valeurs, puis cliquez sur **Terminé**.

   Remarque
   Vous pouvez ajouter jusqu'à 30 moniteurs à un plan de surveillance.

8. [Facultatif] Dans l'écran Paramètres de moniteur, modifiez les paramètres par défaut du moniteur et des alertes, puis cliquez sur **Terminé**.

   Remarque
   Vous pouvez configurer différents paramètres pour chaque moniteur. Pour plus d'informations, voir "Moniteurs configurables" (p. 1525) et "Configuration des alertes de surveillance" (p. 1571).

9. [Facultatif] Pour supprimer un moniteur, cliquez sur l'icône de la corbeille, puis cliquez sur **Supprimer**.
10. Cliquez sur **Créer**.

Ajout de ressources à des plans de surveillance

En fonction de vos besoins, vous pouvez ajouter des ressources à un plan de surveillance après sa création.

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- La version de l'agent installée sur la ressource prend en charge la fonctionnalité de surveillance.
- Un plan de surveillance au moins est disponible.

Pour ajouter une ressource à un plan de surveillance

À partir de Plans de surveillance

© Acronis International GmbH, 2003-2026

1. Dans la console Protection, accédez à **Gestion** > **Plans de surveillance**.
2. Cliquez sur le plan de surveillance.
3. Selon que le plan est déjà appliqué, ou pas, à une ressource, effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter des ressources**, si le plan n'a encore été appliqué à aucune ressource.
   - Cliquez sur **Gérer les ressources** si le plan n'a été appliqué à aucune ressource.
4. Sélectionnez une ressource dans la liste, puis cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.
6. Si nécessaire, cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

À partir de Tous les terminaux

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource à laquelle vous souhaitez appliquer un plan de surveillance.
3. Cliquez sur **Protection**.
4. Recherchez le plan de surveillance auquel vous souhaitez ajouter la ressource, puis cliquez sur **Appliquer**.
5. Si nécessaire, cliquez sur **Confirmer** pour appliquer le quota de service requis à la ressource.

Révocation de plans de surveillance

Vous pouvez révoquer un plan de surveillance d'une ressource à laquelle le plan a été appliqué.

Prérequis

Un plan de surveillance au moins est appliqué à la ressource.

Pour révoquer un plan de surveillance

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la ressource, puis sur **Protection**.
3. Cliquez sur l'icône **Plus d'actions** du plan de surveillance que vous souhaitez révoquer, puis sur **Retirer**.

Configuration des mesures d'intervention automatiques

Les mesures d'intervention automatiques sur les événements indiqués dans les alertes sont des actions ou des mesures prédéfinies qui sont déclenchées automatiquement en réponse à des événements ou des incidents détectés. Ces actions sont conçues pour limiter les menaces potentielles et réduire des dommages.

Vous pouvez configurer une ou plusieurs mesures d'intervention automatiques sur les événements indiqués dans les alertes. Le nombre maximal de mesures d'intervention automatiques par moniteur est de 20.

Pour configurer des mesures d'intervention automatiques

© Acronis International GmbH, 2003-2026

1. Dans la console Protection, accédez à **Gestion** > **Plans de surveillance**.
2. Sélectionnez le plan de surveillance pour lequel vous souhaitez configurer des mesures d'intervention automatiques.
3. Sélectionnez le moniteur dans lequel vous souhaitez configurer des mesures d'intervention automatique ou, si vous n'avez pas encore ajouté de moniteurs, cliquez sur **Ajouter un moniteur**, sélectionnez le moniteur souhaité dans la liste, cliquez sur **Ajouter**, puis sélectionnez le moniteur.
4. Cliquez sur le lien situé à côté de **Mesures d'intervention automatiques**.
5. Dans la fenêtre **Mesures d'intervention automatiques**, ajoutez une ou plusieurs mesures d'intervention qui devront s'exécuter automatiquement lors du déclenchement d'une alerte.
6. Configurez chaque mesure d'intervention automatique. Par exemple, si vous avez ajouté la mesure d'intervention automatique **Démarrer un service Windows**, procédez comme suit :
   a. À côté de **Service Windows**, cliquez sur **Spécifier**.
   b. Dans le champ **Service**, sélectionnez un service pour démarrer une mesure d'intervention.
   c. Cliquez sur **Terminé**.
7. Dans la liste de toutes les mesures d'intervention ajoutées, utilisez les flèches Haut et Bas ou la fonctionnalité de glisser-déposer pour configurer la séquence des mesures d'intervention.
8. Configurez comment gérer des mesures d'intervention successives si la mesure précédente a échoué. Sélectionnez l'une des options suivantes :
   a. **Passer à la mesure d'intervention suivante**.
   b. **Ne pas passer à la mesure d'intervention suivante**.
9. Cliquez sur **Terminé**.

   Le nombre de mesures configurées figure à côté du paramètre **Mesures d'intervention automatiques** de votre plan de surveillance. Vous pouvez modifier ou supprimer ces mesures, et en ajouter d'autres ultérieurement.

Le tableau suivant répertorie et décrit toutes les mesures d'intervention automatiques disponibles dans les paramètres de moniteur.

Mesure d'intervention automatique	Description	Système d'exploitation pris en charge
Exécuter un script	Si vous ajoutez cette action, vous pouvez effectuer les opérations suivantes : 1. Sélectionnez un script à exécuter sur la ressource. 2. Spécifiez le compte sous lequel vous souhaitez exécuter le script. 3. Spécifiez la durée maximale de l'opération. 4. Spécifiez la stratégie d'exécution	Windows, macOS

© Acronis International GmbH, 2003-2026

Mesure d'intervention automatique	Description	Système d'exploitation pris en charge
	PowerShell. 5. Exécutez un script. **Remarque** Pour effectuer cette action, vous avez besoin de la licence RMM (mode de licence basé sur le service) ou de la sécurité et RMM (mode de licence basé sur la solution) pour la ressource, si elle n'est pas encore affectée. Lorsque les conditions sont réunies, le système exécute le script distant sélectionné avec les paramètres spécifiés.	
Redémarrer la ressource	Lorsque les conditions sont réunies et que vous ajoutez cette action, le système redémarre la ressource à distance.	Windows, macOS
Arrêter le processus	Si vous ajoutez cette action, vous pouvez indiquer le processus à arrêter par l'intermédiaire de la saisie manuelle du nom du processus. Lorsque les conditions sont réunies, le système arrête le processus.	Windows, macOS
Démarrer le service Windows	Si vous ajoutez cette action, vous pouvez sélectionner le service Windows à démarrer depuis la liste dynamique des services que remplissent les agents. Lorsque les conditions sont réunies, le système redémarre le service.	Windows
Arrêter le service Windows	Si vous ajoutez cette action, vous pouvez sélectionner le service Windows à arrêter depuis la liste dynamique des services que remplissent les agents. Lorsque les conditions sont réunies, le système arrête le service.	Windows
Activer Windows Update	Lorsque les conditions sont réunies et que vous ajoutez cette action, le système redémarre la ressource à distance. Cette action n'est disponible que pour le	Windows

© Acronis International GmbH, 2003-2026

Mesure d'intervention automatique	Description	Système d'exploitation pris en charge
	moniteur de statut Windows Update.	
Désactiver l'exécution automatique sur les lecteurs amovibles	Lorsque les conditions sont réunies et que vous ajoutez cette action, le système désactive la fonctionnalité d'exécution automatique sur le support de stockage amovible de la ressource. Cette action n'est disponible que pour le moniteur de statut de l'exécution automatique.	Windows

Actions supplémentaires avec plans de surveillance

Depuis l'écran **Plans de surveillance**, vous pouvez effectuer les actions supplémentaires suivantes avec les plans de surveillance : afficher les détails, modifier, afficher les activités, afficher les alertes, renommer, activer, désactiver, cloner, exporter, importer, ajouter aux favoris, retirer des favoris, définir comme plan par défaut, effacer la valeur par défaut et supprimer.

Afficher les détails

Pour afficher les détails d'un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Afficher les détails**.
3. [Facultatif] Si vous souhaitez afficher les détails d'un moniteur activé dans le plan, cliquez sur le nom du moniteur.

Modifier

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour modifier un plan

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Modifier**.
3. [Facultatif] Pour supprimer un moniteur du plan, cliquez sur l'icône de la corbeille, à droite du nom du moniteur.
4. [Facultatif] Pour activer ou désactiver un moniteur dans le plan, utilisez le bouton bascule à côté du nom du moniteur.
5. [Facultatif] Pour modifier les paramètres de moniteur, procédez comme suit.
   a. Cliquez sur le nom du moniteur.
   b. Cliquez sur la vue d'ensemble des paramètres de moniteur.

© Acronis International GmbH, 2003-2026

c. Dans l'écran **Paramètres de moniteur**, configurez les paramètres, puis cliquez sur **Terminé**.

> **Remarque**
> Vous pouvez configurer différents paramètres pour chaque moniteur. Pour plus d'informations, voir "Moniteurs configurables" (p. 1525) et "Configuration des alertes de surveillance" (p. 1571).

d. Fermez l'écran et confirmez les modifications.

6. [Facultatif] Pour ajouter un moniteur, cliquez sur **Ajouter un moniteur**, puis, si nécessaire, modifiez les paramètres en suivant les explications de l'étape précédente.
7. Cliquez sur **Enregistrer**.

Activités

Pour afficher les activités relatives à un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Activités**.
3. Cliquez sur une activité pour visualiser plus de détails la concernant.

Alertes

Pour afficher les alertes

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Alertes**.

Renommer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour renommer un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Renommer**.
3. Saisissez le nouveau nom du plan, puis cliquez sur **OK**.

Activer

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Le plan de surveillance est appliqué à au moins une ressource.

Pour activer un plan de surveillance

© Acronis International GmbH, 2003-2026

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Activer**.

Désactiver

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour désactiver un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Désactiver**.

Cloner

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour cloner un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Cloner**.
3. Cliquez sur **Créer**.

Exporter

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour exporter un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Exporter**.
   La configuration du plan est exportée au format JSON vers la machine locale.

Importer

Prérequis

- L'authentification à deux facteurs est activée pour votre compte utilisateur.
- Un fichier JSON avec la configuration du plan est disponible sur l'ordinateur à partir duquel vous êtes connecté à la console.

Pour importer un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur **Importer un plan**.
2. Dans la fenêtre qui s'ouvre, parcourez jusqu'au fichier JSON.

© Acronis International GmbH, 2003-2026

3. Cliquez sur le fichier, puis cliquez sur **Ouvrir**.
   Le plan de surveillance apparaît à l'écran. Vous pouvez maintenant l'appliquer aux ressources.

Supprimer

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour supprimer un plan de surveillance

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Supprimer**.
3. Sélectionnez **Je confirme**, puis cliquez sur **Supprimer**.

Définir par défaut

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour définir un plan de surveillance par défaut

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Définir par défaut**.
3. Dans la fenêtre de confirmation, cliquez sur **Définir**.
   Dans l'écran **Plans de surveillance**, la balise **Défaut** apparaît à côté du nom du plan.

Ajouter aux favoris

Prérequis

L'authentification à deux facteurs est activée pour votre compte utilisateur.

Pour définir un plan de surveillance comme favori

1. Dans l'écran **Plans de surveillance**, cliquez sur l'icône **Autres actions** du plan de surveillance.
2. Cliquez sur **Ajouter aux favoris**.
   Dans l'écran **Plans de surveillance**, une icône en forme d'étoile apparaît à côté du nom du plan.

Réinitialisation des modèles d'apprentissage automatique

Vous pouvez réinitialiser les modèles d'une ressource lorsqu'ils deviennent obsolètes ou invalides. Cette action supprime les modèles créés et les données collectées pour la ressource par les surveillance basée sur une anomalie, puis démarre de toutes pièces la formation des modèles d'apprentissage automatique pour la ressource.

Pour réinitialiser les modèles d'apprentissage automatique pour une ressource

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur une ressource dans la liste, puis sur l'onglet **Détails**.

© Acronis International GmbH, 2003-2026

3. Dans la section **Réinitialiser les modèles d'apprentissage automatique**, cliquez sur **Réinitialiser**.
4. Dans la fenêtre de confirmation, cliquez de nouveau sur **Réinitialiser**.

Alertes de surveillance

Les alertes de surveillance sont affichées dans la console Protection et sont envoyées par e-mail lorsque le comportement surveillé des ressources est hors norme. Les alertes garantissent que les parties prenantes sont informées dans les meilleurs délais en cas de problème dans l'environnement informatique de l'organisation.

Remarque
Pour activer les alertes de surveillance via e-mail, vous devez configurer au moins une stratégie de notification par e-mail pour le type d'alerte correspondant. Pour plus d'informations, voir "Configuration des stratégies de notification par e-mail" (p. 1579).

Configuration des alertes de surveillance

Vous pouvez configurer les paramètres d'alerte du moniteur lorsque vous ajoutez un moniteur à un plan de surveillance ou que vous modifiez un moniteur déjà disponible dans un plan de surveillance.

Pour configurer des alertes de surveillance

1. Dans la fenêtre **Paramètres de moniteur**, accédez à la section **Générer des alertes**.
2. Dans **Gravité de l'alerte**, sélectionnez la gravité correspondant à la priorité de l'alerte.

Option	Description
Critique	Ces alertes ont la priorité la plus élevée et concernent des problèmes critiques qui ont un impact sur le fonctionnement de la ressource. Résolvez ces problèmes dès que possible.
Erreur	Une alerte d'erreur est moins grave et indique que quelque chose ne marche pas ou ne se comporte pas normalement. Résolvez les problèmes à temps pour éviter qu'ils provoquent des difficultés plus graves.
Avertissement	Une alerte d'avertissement indique qu'il existe une condition que vous devez connaître, mais qui ne devrait pas créer de problème pour l'instant. Résolvez ces problèmes après avoir réglé ce qui provoque des alertes critiques ou d'erreur. Il s'agit de la valeur par défaut.
Infomations	Ces alertes ont la priorité la plus faible. La gravité Informations n'indique pas de problème. Ces alertes fournissent des informations sur les actions associées à un objet surveillé.

© Acronis International GmbH, 2003-2026

3. Dans **Fréquence des alertes**, sélectionnez le mode de génération d'une alerte lorsque la condition est remplie.

Option	Description
Une seule fois jusqu'à la réussite de la vérification	Le système génère une alerte une fois la vérification terminée avec succès. Il s'agit de la valeur par défaut.
Après X échecs consécutifs	Le système génère une alerte après X tentatives consécutives infructueuses, X étant une valeur d'entier.

4. Dans **Message d'alerte**, cliquez sur l'icône représentant un crayon pour modifier le message par défaut qui sera utilisé par le système lors de la génération de l'alerte. Vous pouvez spécifier un message d'alerte personnalisé qui contient des variables. Pour plus d'informations sur les variables que vous pouvez utiliser, reportez-vous à "Variables des alertes de surveillance" (p. 1572).

   Remarque
   Vous pouvez configurer plusieurs messages d'alerte pour certains des moniteurs.

5. Activez **Résolution automatique des alertes** si vous souhaitez que le système résolve automatiquement l'alerte lorsque la mesure surveillée revient à l'état normal et que le comportement est à nouveau normal. Ce paramètre est activé par défaut.

Variables des alertes de surveillance

Vous pouvez configurer différentes variables d'alerte pour les différents moniteurs. Pour utiliser une variable, vous devez la mettre entre {{}}.

Le tableau suivant fournit plus d'informations sur les variables disponibles.

Variable	Description	Disponible pour le moniteur
plan_name	Nom de la stratégie	Tous les moniteurs
monitor_name	Nom de la sous-stratégie du plan de surveillance	Tous les moniteurs
workload_ name	Nom de la ressource	Tous les moniteurs
threshold_ value	Conditions spécifiques de surveillance ou seuils de génération d'une alerte	Tous les moniteurs prenant en charge la surveillance basée sur un seuil.
threshold_unit	Unité associée à la valeur de seuil. Par exemple, %, Mo ou Mo/s.	Tous les moniteurs prenant en charge la

© Acronis International GmbH, 2003-2026

Variable	Description	Disponible pour le moniteur
		surveillance basée sur un seuil.
time_period	Le système ne générera une alerte pour un problème détecté que si la valeur de la mesure est hors norme pendant la période spécifiée.	Tous les moniteurs prenant en charge la surveillance basée sur un seuil.
time_unit	Unité qui sera associée à la période (s/min/heures/jour).	Tous les moniteurs prenant en charge la surveillance basée sur un seuil.
anomaly_value	Valeur d'anomalie	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
anomaly_unit	Unité qui sera associée à la valeur d'anomalie	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
deviation_value	Valeur d'écart	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
deviation_unit	Unité qui sera associée à la valeur d'écart	Tous les moniteurs prenant en charge la surveillance basée sur une anomalie.
drive_name	Lecteur pour Windows ou partition pour macOS	Espace disque,
CPU_model	Modèle du processeur surveillé	Température du processeur
GPU_model	Modèle du processeur graphique surveillé	Température du processeur graphique
hardware_model	Modèle du composant surveillé	Modifications apportées au matériel
hardware_component	Type du matériel surveillé	Modifications apportées au matériel
hardware_model_old	Modèle du composant surveillé qui a été remplacé	Modifications apportées au matériel

© Acronis International GmbH, 2003-2026

Variable	Description	Disponible pour le moniteur
hardware_model_new	Modèle du nouveau composant surveillé qui a été ajouté	Modifications apportées au matériel
disk_model	Modèle du disque	Vitesse de transfert du disque
network_adapter_model	Modèle de la carte réseau	Utilisation du réseau
process_name	Nom du processus	Utilisation du processeur par processus Utilisation de la mémoire par processus Vitesse de transfert du disque par processus Utilisation du réseau par processus État du processus
service_name	Nom du service	État du service Windows
software_name	Nom de l'application logicielle	Logiciel installé
software_version	Version de l'application logicielle	Logiciel installé
software_version_old	Version de l'application logicielle avant la mise à jour	Logiciel installé
software_version_new	Version de la nouvelle application logicielle ou de l'application mise à jour	Logiciel installé
number_of_occurrences	Nombre d'occurrences d'un événement dans le journal	Journal des événements Windows
event_types	Type de l'événement	Journal des événements Windows
event_source	Source de l'événement	Journal des événements Windows
event_log_name	Nom de l'événement	Journal des événements Windows
firewall_software_name	Nom du logiciel du pare-feu	État du pare-feu

© Acronis International GmbH, 2003-2026

Variable	Description	Disponible pour le moniteur
antimalware_software_name	Nom du logiciel antimalware	État du logiciel antimalware
user_name	Nom de l'utilisateur	État de la fonctionnalité d'exécution automatique
script_name	Nom du script	Personnalisé

Mesures d'intervention manuelles

Lorsque vous voyez une alerte, vous pouvez sélectionner une mesure d'intervention que vous souhaitez prendre sur les événements figurant dans les alertes.

Pour réaliser une mesure d'intervention manuelle

1. Dans la console Protection, accédez à **Alertes**.
2. Ouvrez l'alerte que vous souhaitez afficher.
3. Cliquez sur **Mesure d'intervention**, puis sélectionnez une mesure d'intervention dans la liste déroulante.

La liste des mesures d'intervention disponibles pour une alerte particulière dépend du type d'alerte, de la disponibilité des fonctionnalités pour un tenant particulier et du système d'exploitation de la ressource.

Pour information, le tableau suivant répertorie et décrit toutes les mesures d'intervention manuelles.

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
Parcourir la tendance d'utilisation de l'espace disque	Ouvre une fenêtre comportant le graphique **Utilisation de l'espace disque** dans laquelle vous pouvez effectuer les opérations suivantes : • Consulter l'évolution dans le temps de l'utilisation de l'espace disque (pendant le dernier jour/les 7 derniers jours/le dernier mois). • Consulter la différence d'utilisation de l'espace disque en valeur relative (%) pendant la période sélectionnée.	Windows, macOS
Parcourir la tendance d'augmentation de la taille	Ouvre une fenêtre comportant le graphique **Augmentation de la taille**	Windows, macOS

© Acronis International GmbH, 2003-2026

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
des fichiers	**des fichiers** dans laquelle vous pouvez effectuer les opérations suivantes : • Consulter l'évolution dans le temps de la taille totale des fichiers et dossiers surveillés (pendant le dernier jour/les 7 derniers jours/le dernier mois). • Consulter la différence de la taille totale des fichiers en valeur relative (%) pendant la période sélectionnée.	
Exécuter un script	Ouvre une fenêtre dans laquelle vous pouvez effectuer les opérations suivantes : 1. Sélectionnez un script à exécuter sur la ressource. 2. Spécifiez le compte sous lequel vous souhaitez exécuter le script. 3. Spécifiez la durée maximale de l'opération. 4. Spécifiez la stratégie d'exécution PowerShell. 5. Exécutez un script. Pour effectuer cette action, une licence RMM (mode de licence basé sur le service) ou Sécurité et RMM (mode de licence basé sur la solution) doit être affectée à la ressource.	Windows, macOS
Connecter via NEAR	Acronis Connect Client établit une connexion à distance.	Windows, macOS
Connecter via RDP	Acronis Connect Client établit une connexion à distance.	Windows
Exécuter la ligne de commande	Démarre la ligne de commande (Invite de commandes ou PowerShell) de la ressource.	Windows
Exécuter le terminal	Démarre l'appli Terminal (BASH ou ZSH) de la ressource.	macOS
Ouvrir l'inventaire matériel	Vous êtes redirigé vers l'onglet **Inventaire du matériel** de la ressource	Windows, macOS

© Acronis International GmbH, 2003-2026

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
	actuelle.	
Parcourir les 10 principaux processus qui ont chargé le processeur	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé le processeur et ont peut-être provoqué sa surchauffe (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé le processeur graphique	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé le processeur graphique et ont peut-être provoqué sa surchauffe (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé la mémoire	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé la mémoire (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé le disque	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé le disque (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir les 10 principaux processus qui ont chargé le réseau	Ouvre une fenêtre avec les 10 principaux processus qui ont chargé l'adaptateur de l'interface réseau (instantané du système au moment de la génération de l'alerte).	Windows, macOS
Parcourir l'utilisation des ressources par processus	Ouvre une fenêtre comprenant des informations détaillées sur l'utilisation des ressources matérielles par le processus concerné : Utilisation du processeur, utilisation de la mémoire, E/S disque, utilisation du réseau.	Windows, macOS
Redémarrer la ressource	Ouvre une fenêtre de confirmation. Démarre la ressource après la confirmation.	Windows, macOS
Démarrer le service Windows	Ouvre une fenêtre de confirmation. Démarre le service Windows après la confirmation.	Windows
Arrêter le service Windows	Ouvre une fenêtre de confirmation. Arrête le service Windows après la confirmation.	Windows

© Acronis International GmbH, 2003-2026

Mesure d'intervention manuelle	Description	Système d'exploitation pris en charge
Stopper le processus	Ouvre une fenêtre de confirmation. Arrête le processus auquel l'alerte fait référence après la confirmation.	Windows, macOS
Activer Windows Update	Ouvre une fenêtre de confirmation. Active Windows Update après la confirmation.	Windows
Désactiver la fonctionnalité d'exécution automatique sur les lecteurs amovibles	Ouvre une fenêtre de confirmation. Désactive la fonctionnalité d'exécution automatique au niveau du système de la ressource après la confirmation.	Windows

Important
Pour des raisons de sécurité, l'authentification à deux facteurs est nécessaire à la réalisation des mesures d'intervention manuelles suivantes :

- Exécuter un script
- Connecter via NEAR
- Connecter via RDP
- Redémarrer la ressource
- Démarrer le service Windows
- Arrêter le service Windows
- Stopper le processus
- Activer Windows Update
- Désactiver la fonctionnalité d'exécution automatique sur les lecteurs amovibles

Visualisation des alertes de surveillance pour une ressource

Dans l'onglet **Alertes**, vous pouvez voir les alertes de surveillance d'une ressource spécifique et effectuer différentes actions.

Pour voir les alertes de surveillance d'une ressource

1. Dans la console Protection, accédez à **Tous les terminaux**.
2. Cliquez sur une ressource, puis sélectionnez l'onglet **Alertes**.
3. [Facultatif] Dans le volet d'alerte de surveillance, effectuez l'une des actions suivantes :
   - Pour effacer l'alerte, cliquez sur **Effacer**.
   - Pour prendre une mesure d'intervention, cliquez sur **Mesure d'intervention**, puis sur

© Acronis International GmbH, 2003-2026

l'action.

- Pour contacter l'équipe de support, cliquez sur **Obtenir du support**.

4. [Facultatif] Pour effacer toutes les alertes de surveillance concernant la ressource, cliquez sur **Tout effacer**.

Affichage du journal des alertes de surveillance

Vous pouvez voir tous les événements associés à une alerte de surveillance, classés dans l'ordre chronologique : les mesures d'interventions (automatiques ou manuelles) réalisées, ainsi que les notifications par e-mail envoyées.

Pour afficher le journal des alertes d'une alerte de surveillance

1. Dans la console Protection, accédez à **Alertes**.
2. Ouvrez l'**affichage tableau**.
3. Dans la liste des alertes, clique sur l'alerte de surveillance que vous souhaitez afficher.
4. Cliquez sur **Détails**, puis sur **Journal des alertes**.

Configuration des stratégies de notification par e-mail

Les stratégies de notification par e-mail spécifient les utilisateurs qui recevront des notifications par e-mail envoyées par les différents moniteurs.

Dans l'écran **Notifications par e-mail**, vous pouvez effectuer les actions suivantes avec les stratégies de notification par e-mail : ajout, modification, activation, désactivation et suppression.

Ajouter

Pour ajouter une nouvelle stratégie de notification

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par e-mail**.
2. Cliquez sur **Ajouter une stratégie**.
3. Cliquez sur **Sélectionner les destinataires**.
4. Dans l'écran **Sélectionner les destinataires**, sélectionnez les utilisateurs devant recevoir des alertes par e-mail, puis cliquez sur **Sélectionner**.
5. Dans **Types d'alerte**, sélectionnez les moniteurs pour lesquels vous souhaitez que le système envoie des alertes par e-mail.
6. Cliquez sur **Ajouter**.

Modifier

Pour modifier une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par e-mail**.
2. Cliquez sur l'icône représentant des points de suspension de la stratégie de notification, puis cliquez sur **Modifier**.

© Acronis International GmbH, 2003-2026

3. [Facultatif] Pour changer les destinataires, cliquez sur **Modifier les destinataires**, ajoutez ou supprimez des utilisateurs de la liste, puis cliquez sur **Sélectionner**.
4. [Facultatif] Dans **Types d'alerte**, sélectionnez les types d'alertes de surveillance que vous souhaitez envoyer aux destinataires sélectionnés.
5. Cliquez sur **Enregistrer**.

Activer

Pour activer une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par e-mail**.
2. Dans l'écran **Notifications par e-mail**, cliquez sur l'icône représentant des points de suspension **...** de la stratégie de notification par e-mail.
3. Cliquez sur **Activer**.

Désactiver

Pour désactiver une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par e-mail**.
2. Dans l'écran **Notifications par e-mail**, cliquez sur l'icône représentant des points de suspension **...** de la stratégie de notification par e-mail.
3. Cliquez sur **Désactiver**.

Supprimer

Pour supprimer une stratégie de notification par e-mail

1. Dans la console Protection, accédez à **Paramètres** > **Notifications par e-mail**.
2. Dans l'écran **Notifications par e-mail**, cliquez sur l'icône représentant des points de suspension **...** de la stratégie de notification par e-mail.
3. Cliquez sur **Supprimer**, puis sur **Confirmer**.

Visualisation des données des moniteurs

Pour chaque ressource, vous pouvez voir la liste des moniteurs appliqués, l'état actuel des moniteurs et les détails historiques des performances dans une vue graphique. Vous pouvez utiliser ces informations pour analyser l'état de la ressource et l'évolution dans le temps de son état.

Prérequis

- Un plan de surveillance est appliqué à la ressource.
- La ressource est en ligne et comprend des données pour le moniteur correspondant.
- La version de l'agent installée sur la ressource prend en charge les plans de surveillance.

Pour afficher les moniteurs appliqués à une ressource et les données de moniteur

© Acronis International GmbH, 2003-2026

1. Dans la console Protection, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur une ressource, puis sur l'onglet **Surveillance**.

   L'onglet **Surveillance** affiche un widget pour chaque moniteur activé pour la ressource. Chaque widget affiche les informations suivantes.

Informations affichées	Description
Nom du moniteur	Nom du moniteur
Dernier résultat	Valeur la plus récente de la mesure surveillée ou dernier état de l'événement
Dernière vérification	Date et heure de collecte des dernières données par le moniteur
Alertes	Nombre d'alertes générées par le moniteur et restant non résolues. Si le moniteur a généré au moins une alerte qui n'est pas résolue, le fait de cliquer sur le nombre ouvre l'onglet **Alertes**. Les alertes sont filtrées, et seules les alertes de ce moniteur sont répertoriées.

   Remarque
   Les widgets deviennent visibles dans l'onglet 15 minutes (ou à la fréquence minimale définie pour un moniteur) après l'application d'un plan de surveillance à la ressource.

3. [Facultatif] Pour afficher d'autres détails sur le moniteur et, le cas échéant, les données historiques collectées pour la mesure surveillée, cliquez dans le widget du moniteur sur l'icône représentant des points de suspension, puis sur **Détails**.

   Pour plus d'informations sur les paramètres de moniteur que vous pouvez voir dans les widgets, reportez-vous à "Widgets de moniteurs" (p. 1581).

Widgets de moniteurs

Dans le widget de moniteur, vous pouvez consulter les détails suivants concernant le moniteur.

Détail	Description
Plan de surveillance	Nom du plan de surveillance contenant le moniteur. Le nom du plan de surveillance est un lien qui ouvre le plan de surveillance en mode d'affichage.
Fréquence de surveillance	Intervalle de collecte par le moniteur des données de la ressource
Dernier résultat	Valeur la plus récente de la mesure surveillée ou dernier état de l'événement
Dernière vérification	Date et heure de collecte des dernières données par le moniteur

© Acronis International GmbH, 2003-2026

Détail	Description
Dernière alerte	Date et heure de génération de la dernière alerte Le champ ne s'affiche que si une alerte au moins est générée pour le moniteur.
Graphique historique	Pour les moniteurs qui collectent des données de série temporelle, le widget affiche les données historiques d'une période sélectionnée (1 heure, 6 heures, 12 heures, 1 jour, 1 semaine ou 1 mois) dans une vue graphique. Le graphique affiche les valeurs réelles des indicateurs pendant la période que vous sélectionnez. Si, pour une raison quelconque, l'agent n'a pas envoyé les données collectées au cloud, les valeurs manquantes sont affichées sous forme de ligne en pointillé qui relie les points de données aux valeurs réelles qui précèdent et suivent la valeur manquante. Pour les moniteurs qui utilisent la surveillance **basée sur les anomalies**, le graphique affiche la zone des valeurs de référence, c'est-à-dire une ligne qui indique les valeurs réelles de l'indicateur, ainsi que les anomalies. Les anomalies correspondent aux pics ou aux valeurs en dehors des valeurs de référence, et elles sont affichées sur le graphique sous la forme de points rouges. Si vous survolez le graphique, vous voyez la valeur réelle et les valeurs de seuil d'une durée spécifique.  **Remarque** Les données affichées sur les graphiques sont affichées dans le fuseau horaire du système local. Il s'agit du fuseau horaire du navigateur de la ressource à partir de laquelle vous accédez à la console Protection.

© Acronis International GmbH, 2003-2026

Prévention des pertes de données

Le module Data Loss Prevention analyse le contenu et le contexte des transferts de données dans les ressources protégées, et empêche toute fuite de données sensibles par l'intermédiaire de périphériques ou de transferts réseau, à l'intérieur et à l'extérieur du réseau d'entreprise, en fonction de la stratégie de flux de données.

Les fonctionnalités Data Loss Prevention peuvent être incluses dans n'importe quel plan de protection d'un tenant client si le service de protection et le pack Data Loss Prevention sont activés pour ce client.

Avant de commencer à utiliser le module Data Loss Prevention, veillez à lire et à comprendre les concepts de base et la logique de la gestion DLP qui sont décrits dans le guide des principes fondamentaux.

Vous souhaiterez peut-être consulter également le document Caractéristiques techniques.

Création des règles et des règles de flux de données

Le principe de prévention de la perte de données exige que les utilisateurs d'un système informatique d'entreprise soient autorisés à gérer les données sensibles uniquement dans la mesure nécessaire aux tâches qu'ils doivent effectuer. Tous les autres transferts de données sensibles qui ne sont pas pertinents pour les processus professionnels doivent être bloqués. Il est par conséquent essentiel de distinguer les transferts, ou flux de données professionnels et non autorisés.

La règle de flux de données contient des règles qui indiquent les flux de données autorisés et non autorisés, et par conséquent empêche les transferts non autorisés d'informations sensibles lorsque le module de prévention de la perte de données est activé dans un plan de protection et s'exécute en mode Application.

Chaque catégorie de sensibilité de la règle contient une règle par défaut, marquée d'un astérisque (*), et une ou plusieurs règles explicites (autres que par défaut) qui définissent les flux de données d'utilisateurs ou de groupes spécifiques. Pour plus d'informations sur les types de règles, consultez le guides des principes fondamentaux.

La stratégie de flux de données est généralement créée automatiquement lorsque le module Data Loss Prevention s'exécute en mode d'observation. La durée nécessaire à la création d'une stratégie de flux de données représentative est d'environ un mois, mais elle peut varier en fonction des processus de votre organisation. La stratégie de flux de données peut également être créée, configurée ou modifiée manuellement par un administrateur d'entreprise ou d'unité.

Pour démarrer la création automatique de la règle de flux de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Gestion** > **Plans de protection**.
3. Cliquez sur **Création d'un plan**.

© Acronis International GmbH, 2003-2026

4. Développez la section **Prévention des pertes de données** et cliquez sur la ligne **Mode**.
5. Dans la boîte de dialogue Mode, Sélectionnez **Mode d'observation**, puis sélectionnez le mode de traitement des transferts de données :

Option	Description
Tout autoriser	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise et sécurisés. Une nouvelle règle est créée pour chaque flux de données détecté qui ne correspond pas à une règle déjà définie.
Justifier tout	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise, mais risqués. Par conséquent, pour chaque transfert intercepté de données sensibles vers une destination ou un destinataire à l'intérieur ou à l'extérieur de l'organisation qui ne correspond à aucune règle de flux de données créée, l'utilisateur doit saisir une justification commerciale unique. Lorsque la justification est soumise, une nouvelle règle de flux de données est créée dans la règle de flux de données.
Mixte	La logique Tout autoriser est appliquée à tous les flux de données sensibles internes et la logique Justifier tout est appliquée à tous les flux de données externes. **Remarque** Pour plus d'informations sur les données internes et externes, voir Détection automatique de la destination

6. Enregistrez le plan de protection et appliquez-le aux ressources à partir desquelles vous souhaitez collecter des données pour concevoir la règle.

Remarque
La fuite des données n'est pas évitée pendant le mode d'observation.

Pour configurer la règle de flux de données manuellement

1. Dans la console Cyber Protect, accédez à **Protection** > **Règle de flux de données**.
2. Cliquez sur **Nouvelle règle de flux de données**.
   Le panneau Nouvelle règle de flux de données se développe sur la droite.
3. Sélectionnez une catégorie de sensibilité, ajoutez un expéditeur et un destinataire, puis définissez l'autorisation de transferts de données pour la catégorie, l'expéditeur et le destinataires sélectionnés.

Option	Description
Autoriser	Autorise cet expéditeur à transférer des données de cette catégorie de sensibilité pour ce destinataire.
Exception	N'autorise pas cet expéditeur à transférer des données de cette catégorie de sensibilité pour ce destinataire, mais permet à l'expéditeur de soumettre une exception à la règle

© Acronis International GmbH, 2003-2026

Option	Description
	pour un transfert spécifique. Lorsque cet expéditeur essaie de transférer des données de cette catégorie de sensibilité à ce destinataire, bloque le transfert et demande à l'expéditeur de soumettre une exception pour autoriser le transfert. Lorsque l'exception est soumise, le transfert de données peut être effectué. **Important** Tous les autres transferts de données entre cet expéditeur et ce destinataire pour cette catégorie de sensibilité seront autorisés pendant cinq minutes après la soumission de l'exception.
Refuser	N'autorise pas cet expéditeur à transférer des données de cette catégorie de sensibilité pour ce destinataire et ne permet pas à l'expéditeur de demander une exception à la règle.

4. (Facultatif) Sélectionnez une action à exécuter lors du déclenchement de la règle.

Action	Description
Écrire dans un journal	Stocke un enregistrement d'événements dans le journal d'audit lors du déclenchement de la règle. Nous vous recommandons de sélectionner cette action pour les règles avec autorisation **Exception**.
Générer une alerte	Génère une alerte dans l'onglet **Alertes** Cyber Protect lors du déclenchement de la règle. Si les notifications sont activées pour l'administrateur, un e-mail de notification est également envoyé.
Notifier l'utilisateur final lorsqu'un transfert de données est refusé	Notifie l'utilisateur en temps réel par un avertissement à l'écran lors du déclenchement de la règle.

5. Cliquez sur **Enregistrer**.
6. Répétez les étapes 2 à 5 pour créer plusieurs règles de différentes catégories et options de sensibilité, puis vérifie que les règles qui en résultent correspondent aux options que vous avez sélectionnées.

Structure de la règle de flux de données

Dans la vue **Règle de flux de données**, les règles sont regroupées en fonction de la catégorie de données sensibles qu'elles contrôlent. L'identificateur de catégorie de sensibilité s'affiche immédiatement au-dessus du groupe de règles.

- Sensible
  - Informations de santé protégées (PHI)
  - Informations personnelles identifiables (PII)

© Acronis International GmbH, 2003-2026

- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS),
- Marqué confidentiel
- Non sensible

Pour plus d'informations sur le concept et les fonctionnalités de règle de flux de données, voir le guides des principes fondamentaux.

Structure de règle

Chaque règle est constituée des éléments suivants.

- **Catégorie de sensibilité**
  - **Informations de santé protégées (PHI)**
  - **Informations personnelles identifiables (PII)**
  - **Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)**
  - **Marqué confidentiel**

    Voir "Définitions des données sensibles" (p. 1597)
- **Expéditeur** - spécifie l'initiateur d'un transfert de données contrôlé par cette règle. Il peut s'agir d'un seul utilisateur, d'une liste d'utilisateurs ou d'un groupe d'utilisateurs.
  - **N'importe quel interne** - groupe d'utilisateurs qui comprend tous les utilisateurs internes de l'organisation.
  - **Contact / Organisation d'origine** – compte Windows dans l'organisation et reconnu par Data Loss Prevention, ainsi que tous les autres comptes (y compris ceux utilisés par des applications de communication tierces) qu'un compte Windows donné a utilisés précédemment.
  - **Contact/Identité personnalisée** - identificateur d'un utilisateur interne dans l'un des formats suivants : adresse e-mail, ID Skype, identificateur ICQ, identificateur IRC, adresse e-mail Jabber, adresse e-mail Mail.ru Agent, numéro de téléphone Viber, adresse e-mail Zoom.
    Les caractères génériques suivants peuvent être utilisés pour indiquer un groupe de contacts :
    - ***** - n'importe quel nombre de symboles
    - **?** - n'importe quel symbole unique
- **Destinataire** - spécifie la destination d'un transfert de données contrôlé par cette règle. Il peut s'agir d'un seul utilisateur, d'une liste d'utilisateurs ou d'un groupe d'utilisateurs, et également des autres types de destinations indiqués ci-dessous.
  - **Tout** – n'importe quel type de destinataire pris en charge par DLP.
  - **Contact/N'importe quel contact** - tout contact interne ou externe.
  - **Contact/N'importe quel contact interne** - tout contact d'un utilisateur interne (voir "Détection automatique de la destination" (p. 1596)).
  - **Contact/N'importe quel contact externe** - tout contact d'une personne ou d'une entité externe.
  - **Contact/Organisation d'origine** - même principe que celui décrit dans le champ Expéditeur.
  - **Contact/Identité personnalisée** - même principe que celui décrit dans le champ Expéditeur.

© Acronis International GmbH, 2003-2026

  - **Services de partage de fichiers** - identificateur d'un service de partage de fichiers contrôlé.
  - **Réseau social** - identificateur d'un réseau social contrôlé.
  - **Hôte / N'importe quel hôte** – tout ordinateur reconnu par DLP comme interne ou externe.
  - **Hôte / N'importe quel hôte interne** – tout ordinateur reconnu par DLP comme interne.
  - **Hôte / N'importe quel hôte externe** – tout ordinateur reconnu par DLP comme externe.
  - **Hôte/Hôte spécifique** - identificateur d'ordinateur spécifié comme nom d'hôte (exemple : FQDN) ou adresse IP (IPv4 ou IPv6).
  - **Terminal/N'importe quel terminal** - tout périphérique connecté à la ressource.
  - **Terminal/Stockage externe** - stockage amovible ou lecteur mappé redirigé et connecté à la ressource.
  - **Terminal/Amovible chiffré** : un périphérique de stockage amovible chiffré avec BitLocker To Go.
  - **Terminal/Presse-papiers redirigé** - Presse-papiers redirigé et connecté à la ressource.
  - **Imprimantes** - imprimante locale ou réseau connectée à la ressource.
- **Autorisation** - contrôle préventif appliqué à un transfert de données contrôlé par cette règle. Décrite en détail dans la rubrique Autorisations dans les règles de flux de données.
- **Action** - action non préventive exécutée au déclenchement de cette règle. Par défaut, ce champ est défini sur Aucune action. Les options sont les suivantes :
  - **Écrire dans un journal** - stocke un enregistrement d'événements dans le journal d'audit lors du déclenchement de la règle.
  - **Notifier l'utilisateur final lorsqu'un transfert de données est refusé** - notifie l'utilisateur à l'aide d'un avertissement à l'écran en temps réel lors du déclenchement de la règle.
  - **Générer une alerte** - alerte l'administrateur lors du déclenchement de la règle.

Avertissement !
Lorsque l'option **Aucune action** est sélectionnée et que la règle est déclenchée :
- aucun enregistrement d'événement n'est ajouté au journal d'audit ;
- aucune alerte n'est envoyée à l'administrateur ;
- aucune notification n'est affichée sur l'écran de l'utilisateur final.

Qu'est-ce qui déclenche une règle ?

Un transfert de données correspond à une règle de flux de données si toutes les conditions suivantes sont vraies :

- Tous les expéditeurs de ce transfert de données sont répertoriés ou appartiennent à un groupe d'utilisateurs spécifié dans le champ **Expéditeur** de la règle.
- Tous les destinataires de ce transfert de données sont répertoriés ou appartiennent à un groupe d'utilisateurs spécifié dans le champ **Destinataire** de la règle.
- Les données transférées correspondent à la **catégorie de sensibilité** de la règle.

© Acronis International GmbH, 2003-2026

Ajustement des autorisations dans les règles de flux de données

Data Loss Prevention prend en charge trois types d'autorisations dans les règles de flux de données. Les autorisations sont configurées individuellement dans chaque règle de la stratégie.

Autoriser (autorisation)	Les transferts de données autorisés sont ceux qui correspondent à la combinaison catégorie de sensibilité, expéditeur et destinataire définie dans la règle.
Exception (interdiction)	Les transferts de données non autorisés sont ceux qui correspondent à la combinaison catégorie de sensibilité, expéditeur et destinataire définie dans la règle. Toutefois, l'expéditeur peut soumettre une exception à la règle pour autoriser un transfert spécifique. **Important** Tous les autres transferts de données entre cet expéditeur et ce destinataire pour cette catégorie de sensibilité seront autorisés pendant cinq minutes après la soumission de l'exception.
Refuser (interdiction)	Les transferts de données non autorisés sont ceux qui correspondent à la combinaison catégorie de sensibilité, expéditeur et destinataire définie dans la règle. L'expéditeur n'a pas la possibilité de soumettre une exception.

Par ailleurs, un indicateur de priorité peut être affecté aux autorisations **Autoriser** et **Exception** afin d'améliorer la flexibilité de la gestion des règles. Grâce à ce paramètre, vous pouvez ignorer les autorisations définies pour des groupes spécifiques dans d'autres règles de flux de données. Vous pouvez l'utiliser pour n'appliquer une règle de flux de données de groupes qu'à certains de ses membres. Pour ce faire, vous devez créer une règle de flux de données pour des utilisateurs spécifiques que vous souhaitez exclure des règles de groupe, puis donner la priorité à leurs autorisations par rapport aux restrictions de flux de données configurées dans les règles du groupe auquel ces utilisateurs appartiennent. Pour plus d'informations sur les priorités d'autorisation lors de la combinaison de règles, voir "Combinaison de règles de flux de données" (p. 1589).

Important
Avant de faire passer une règle d'entreprise ou d'unité du mode d'observation au mode d'application, il est essentiel d'ajuster les règles par défaut de chaque catégorie de données sensibles en les faisant passer de l'état d'autorisation à l'état d'interdiction. Les règles par défaut sont marquées d'un (*) dans la vue **Règle de flux de données**. Pour plus d'informations sur les types de règles, consultez le guides des principes fondamentaux.

Pour modifier les autorisations dans les règles

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Règle de flux de données**.
3. Sélectionnez la règle à modifier, puis cliquez sur **Modifier** au-dessus de la liste de règles.
   La fenêtre **Modifier la règle de flux de données** s'ouvre.

© Acronis International GmbH, 2003-2026

4. Dans la section **Autorisation**, sélectionnez **Autoriser**, **Exception** ou **Refuser**.
5. (Facultatif) Pour donner la priorité à l'autorisation **Autoriser** ou **Exception** sur les autorisations des autres règles, cochez la case **Prioriser**.
   Vous n'avez pas besoin d'utiliser cette case à cocher pour donner la priorité à une règle de flux de données sur la règle par défaut Tout > Autre, car ce flux a par défaut la priorité la plus faible dans une règle.
   Pour plus d'informations sur les priorités d'autorisation lors de la combinaison de règles, voir "Combinaison de règles de flux de données" (p. 1589).
6. (Facultatif) Sélectionnez une action à exécuter lors du déclenchement de la règle.
7. Enregistrez les modifications apportées à la règle.

Combinaison de règles de flux de données

Lorsqu'un transfert de données correspond à plusieurs règles, les autorisations et les actions configurées pour toutes les règles sont combinées et appliquées comme suit.

Autorisations

Si un transfert de données correspond à plusieurs règles dont les autorisations diffèrent pour une même catégorie de données, la règle prioritaire est celle dont l'autorisation a la priorité la plus élevée dans la liste des priorités des autorisations suivantes (classées dans l'ordre décroissant) :

1. Exception avec drapeau **Prioritaire**
2. Autoriser avec le drapeau **Prioritaire**
3. Refuser
4. Exception
5. Autoriser

Si un transfert de données correspond à plusieurs règles dont les autorisations diffèrent d'une catégorie de données à l'autre, la logique de remplacement suivante est appliquée :

1. L'autorisation de règle la plus restrictive est définie pour chacune des catégories de sensibilité correspondant au transfert de données.
2. Les autorisations de règles les plus restrictives et définies au point 1 sont appliquées.

Exemple

Un transfert de fichiers correspond à trois règles dans différentes catégories de sensibilité comme suit :

Catégorie de sensibilité	Autorisation
IPI	Autoriser - Prioritaire
IMP	Exception - Prioritaire
PCI	Refuser

© Acronis International GmbH, 2003-2026

L'autorisation qui sera appliquée est Refuser.

Actions

Si un transfert de données correspond à plusieurs règles dont les options configurées dans le champ **Action** sont différentes, toutes les actions configurées dans toutes les règles déclenchées sont effectuées.

Examen et gestion des stratégies

Avant d'être appliquée, la stratégie de flux de données de référence créée automatiquement doit être examinée, validée et approuvée par le client, car c'est lui qui connaît toutes les spécificités de son activité et peut évaluer si elles sont interprétées de manière cohérente dans la stratégie de référence. De la même manière, le client peut identifier les incohérences que peut alors résoudre l'administrateur partenaire.

Pendant l'examen de la stratégie, l'administrateur partenaire présente la stratégie de flux de données de référence au client qui examine chaque flux et valide sa cohérence avec les processus professionnels. La validation n'exige aucune compétence technique, car la représentation des stratégies de la console Cyber Protect est très intuitive : chaque règle décrit qui est l'expéditeur et qui est le destinataire d'un flux de données sensibles.

En fonction des instructions du client, l'administrateur partenaire ajuste la stratégie de référence manuellement en modifiant, en supprimant et en créant les règles de flux de données. Après l'approbation du client, la règle examinée est appliquée aux ressources protégées par le passage en mode Application du plan de protection appliqué à ces ressources.

Avant l'application d'une stratégie examinée, il est important de modifier l'autorisation **Autoriser** dans toutes les règles par défaut créées automatiquement pour les catégories de données sensibles sur l'état **Refuser** ou **Exception**. L'autorisation **Refuser** ne peut pas être remplacée par les utilisateurs tandis que l'autorisation **Exception** bloque un transfert correspondant à la règle, mais permet aux utilisateurs d'ignorer une situation d'urgence en soumettant une exception de nature commerciale.

Renouvellement de la règle de flux de données

Lorsque le processus professionnel de l'entreprise ou son unité est considérablement modifié, les règles DLP correspondantes doivent être renouvelées pour qu'elles soient cohérentes avec les modifications apportées aux flux de données sensibles du processus professionnel mis à jour. Un renouvellement de règle est également nécessaire si le rôle d'un employé est modifié. Dans ce cas, la partie de la règle d'unité utilisée pour protéger la ressource de l'employé doit également être renouvelée.

Le workflow de gestion de la stratégie DLP permet aux administrateurs d'automatiser les renouvellements de la stratégie pour l'intégralité de l'entreprise, une unité, un utilisateur ou une partie des utilisateurs d'une unité.

© Acronis International GmbH, 2003-2026

Renouvellement de la règle d'une société ou d'une unité

Toutes les options du mode d'observation peuvent être utilisées pour renouveler la règle de l'entreprise ou de l'unité, et également une règle d'unité pour un ou plusieurs utilisateurs de l'unité.

Pour renouveler la règle d'une société ou d'une unité

Le processus de renouvellement se compose des étapes suivantes qui doivent être effectuées par un administrateur de l'entreprise ou un partenaire qui gère les ressources de l'entreprise.

1. Supprimez toutes les règles qui ne sont pas par défaut dans la règle appliquée.
2. Pour démarrer le renouvellement, faites passer le plan de protection avec DLP appliqué à l'entreprise ou à l'unité à l'une des options de mode d'observation, en utilisant l'option optimale pour cette entreprise ou cette unité, puis appliquez le plan à toutes les ressources de l'entreprise ou de l'unité.
3. À la fin de la période de renouvellement, examinez la nouvelle règle d'entreprise ou d'unité avec le client, effectuez les modifications nécessaires, puis obtenez l'approbation du client.
4. Faites passer le plan de protection appliqué aux ressources de l'entreprise ou de l'unité à une option de mode d'application approprié que le client considère comme étant optimale pour empêcher les fuites de données à partir des ressources de l'unité.

Renouvellement de la règle d'un ou plusieurs utilisateurs de la société ou de l'unité

Les règles de niveau utilisateur peuvent être renouvelées à l'aide de n'importe quelle option du mode d'observation et également du mode d'application adaptative.

Utilisation du mode d'observation pour le renouvellement d'une règle utilisateur

L'utilisation du mode d'observation pour le renouvellement de la règle d'un ou de plusieurs utilisateurs de l'entreprise (ou de l'unité) a les particularités suivantes : la règle de flux de données appliquée à l'intégralité de l'entreprise (ou de l'unité) n'est pas appliquée aux transferts de données des utilisateurs pendant la période de renouvellement. Par conséquent, les nouvelles règles de l'utilisateur créées pendant le renouvellement pourraient contredire les règles de groupe existantes (ou y correspondre) dans la règle appliquée pour l'entreprise (unité). Une fois le renouvellement terminé et la règle réappliquée aux transferts de données de l'utilisateur, ces nouvelles règles créées pour l'utilisateur sont appliquées ou non aux transferts de données de l'utilisateur selon les priorités sur d'autres règles auxquelles ces transferts de données doivent correspondre.

Pour renouveler la règle d'un utilisateur en mode d'observation

Le processus de renouvellement se compose des étapes suivantes qui doivent être effectuées par un administrateur de l'entreprise ou un partenaire qui gère les ressources de l'entreprise.

1. Supprimez toutes les règles qui ne sont pas par défaut et sont appliquées pour l'entreprise (ou l'unité) dont l'utilisateur est le seul expéditeur.

© Acronis International GmbH, 2003-2026

2. Supprimez l'utilisateur des listes d'expéditeurs de toutes les règles de flux de données qui ne sont pas par défaut dans la règle appliquée.
3. Créez un nouveau plan de protection avec DLP en mode d'observation et appliquez-le à la ressource de l'utilisateur pour démarrer la période de renouvellement (observation).
   La durée de la période de renouvellement dépend de la durée nécessaire à l'utilisateur pour effectuer toutes (ou 90 à 95 %) les activités régulières qui impliquent le transfert de données sensibles à partir de ses ressources.
4. À la fin de la période de renouvellement, examinez les nouvelles règles associées à cet utilisateur et qui ont été ajoutées à la règle appliquée, effectuez les modifications nécessaires, puis obtenez l'approbation du client.
5. Faites passer le plan de protection appliqué à la ressource de l'utilisateur au mode **Application stricte** ou **Application adaptative** selon l'option que le client considère comme étant optimale pour empêcher les fuites de données à partir de la ressource de l'utilisateur.
   Vous pouvez également réappliquer à la ressource de l'utilisateur le plan de protection appliqué à l'entreprise (ou à l'unité).

Utilisation du mode d'application adaptative pour le renouvellement d'une règle utilisateur

Le renouvellement de la stratégie d'un ou de plusieurs utilisateurs de l'entreprise (ou de l'unité) peut être effectué à l'aide du mode d'application adaptative d'un plan de protection avec DLP appliqué à la ressource de l'utilisateur.

Remarque
Cette méthode de renouvellement de règle a les particularités suivantes : les règles d'entreprise (d'unité) appliquée aux groupes d'expéditeurs avec adhésion de l'utilisateur (par exemple, N'importe quel interne) sont également appliquées aux transferts de données de cet utilisateur pendant le renouvellement. Par conséquent, le renouvellement ne crée pas pour l'utilisateur de nouvelles règles qui contrediraient les règles existantes des groupes d'expéditeurs (ou y correspondraient). La méthode la plus efficace pour les renouvellements de règles utilisateur d'un client dépend des exigences spécifiques en matière de sécurité informatique.

Pour renouveler la règle d'un utilisateur en mode d'application adaptative

Le processus de renouvellement se compose des étapes suivantes qui doivent être effectuées par un administrateur de l'entreprise ou un partenaire qui gère les ressources de l'entreprise.

1. Supprimez toutes les règles qui ne sont pas par défaut et sont appliquées pour l'entreprise (ou l'unité) et dont l'utilisateur est le seul expéditeur.
2. Supprimez l'utilisateur des listes d'expéditeurs de toutes les règles de flux de données qui ne sont pas par défaut dans la règle appliquée.
3. Pour toutes les règles par défaut appliquées pour l'entreprise (ou l'unité), définissez leur autorisation sur **Exception**, puis sélectionnez l'action **Écrire dans un journal** dans le champ **Action**.

© Acronis International GmbH, 2003-2026

4. Si le plan de protection appliqué à la ressource de l'utilisateur est défini sur le mode **Application stricte**, créez un plan de protection avec DLP et appliquez-le à la ressource de l'utilisateur en mode **Application adaptative** pour démarrer la période de renouvellement.
   La durée de la période de renouvellement dépend de la durée nécessaire à l'utilisateur pour effectuer toutes (ou 90 à 95 %) les activités régulières qui impliquent le transfert de données sensibles à partir de ses ressources.
5. À la fin de la période de renouvellement, examinez les nouvelles règles associées à cet utilisateur et qui ont été ajoutées à la règle appliquée, effectuez les modifications nécessaires, puis obtenez l'approbation du client.
6. Faites passer le plan de protection appliqué à la ressource de l'utilisateur au mode **Application stricte** ou conservez le mode **Application adaptative** selon l'option que le client considère comme étant optimale pour empêcher les fuites de données à partir de la ressource de l'utilisateur.
   Vous pouvez également réappliquer à la ressource de l'utilisateur le plan de protection appliqué à l'entreprise (ou à l'unité).

Activation de Data Loss Prevention dans les plans de protection

Les fonctionnalités Data Loss Prevention peuvent être incluses dans n'importe quel plan de protection d'un tenant client si le service de protection et le pack Data Loss Prevention sont activés pour ce client.

Les fonctionnalités DLP et le contrôle des terminaux peuvent être utilisés indépendamment ou ensemble (dans un seul plan de protection, ou dans deux plans protégeant la même ressource). S'ils sont utilisés ensemble, leurs capacités fonctionnelles sont coordonnées comme suit.

- Le contrôle de terminal cesse de contrôler l'accès de l'utilisateur à ces canaux locaux dans lesquels DLP inspecte le contenu des données transférées. En revanche, il conserve le contrôle sur les types de terminaux suivants s'ils sont configurés en accès en lecture seule ou si leur accès est refusé :
  - Amovible
  - Amovible chiffré
  - Lecteur mappé

  Par exemple, si le contrôle de terminal et DLP sont activés dans un seul plan de protection ou dans deux plans protégeant la même ressource, et que l'accès en lecture seule est configuré pour les périphériques USB dans le contrôle de terminal, l'accès en lecture seule est appliqué à tous les périphériques USB, à l'exception de ceux figurant dans la liste d'autorisation, indépendamment des paramètres d'accès du module DLP. Si l'accès est activé par défaut et configuré dans le contrôle de terminal, le paramètre d'accès de DLP est appliqué.
- L'accès des utilisateurs aux canaux locaux et terminaux suivants de la liste d'autorisation est appliqué par le contrôle des terminaux :

© Acronis International GmbH, 2003-2026

- Lecteurs optiques
- Disquettes
- Terminaux mobiles connectés par MTP
- Adaptateurs Bluetooth
- Presse-papiers Windows
- Captures d'écran
- Périphériques USB et types de périphériques (à l'exception du stockage amovible et des périphériques chiffrés)

Pour créer un plan de protection avec DLP

1. Accédez à **Gestion** > **Plans de protection**.
2. Cliquez sur **Création d'un plan**.
3. Développez la section **Prévention des pertes de données** et cliquez sur la ligne **Mode**.
   La boîte de dialogue **Mode** s'ouvre.
   - Pour démarrer la création ou le renouvellement de la règle de flux de données, sélectionnez **Mode d'observation**, puis le mode de traitement des transferts de données :

Option	Description
Tout autoriser	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise et sécurisés. Une nouvelle règle est créée pour chaque flux de données détecté qui ne correspond pas à une règle déjà définie.
Justifier tout	Tous les transferts de données sensibles des ressources utilisateur sont traités comme étant nécessaires aux processus de l'entreprise, mais risqués. Par conséquent, pour chaque transfert intercepté de données sensibles vers une destination ou un destinataire à l'intérieur ou à l'extérieur de l'organisation qui ne correspond à aucune règle de flux de données créée, l'utilisateur doit saisir une justification commerciale unique. Lorsque la justification est soumise, une nouvelle règle de flux de données est créée dans la règle de flux de données.
Mixte	La logique Tout autoriser est appliquée à tous les transferts internes de flux de données sensibles et la logique Justifier tout est appliquée à tous les transferts externes de flux de données sensibles. Pour la définition des destinations internes, voir "Détection automatique de la destination" (p. 1596)

© Acronis International GmbH, 2003-2026

Avertissement !

- Sélectionnez **Mode d'observation** uniquement si vous n'avez aucune règle de flux de données créée ou si vous renouvelez la règle. Avant de commencer le renouvellement de règle, voir "Renouvellement de la règle de flux de données" (p. 1590).
- La fuite des données n'est pas évitée en Mode d'observation. Reportez-vous à Mode d'observation dans le guides des principes fondamentaux.

- Pour appliquer la règle de flux de données existante, sélectionnez **Mode d'application**, puis choisissez le mode d'application des règles de flux de données :

Option	Description
Application stricte	La règle de flux de données est appliquée en l'état et n'est pas étendue avec les nouvelles règles d'autorisation en cas de détection de flux de données sensibles non observés précédemment. Reportez-vous à Application stricte dans le guides des principes fondamentaux.
Application adaptative (application avec apprentissage)	La règle appliquée continue à s'adapter automatiquement aux opérations qui n'ont pas été effectuées pendant la période d'observation ou aux modifications apportées aux processus professionnels. Ce mode permet d'étendre la règle de flux de données appliquée en fonction des nouveaux flux de données appris et détectés dans les ressources. Reportez-vous à Application adaptative dans le guides des principes fondamentaux.

Important

Avant de faire passer une règle d'entreprise ou d'unité du mode d'observation au mode d'application, il est essentiel d'ajuster les règles par défaut de chaque catégorie de données sensibles en les faisant passer de l'état d'autorisation à l'état d'interdiction. Les règles par défaut sont marquées d'un (*) dans la vue **Règle de flux de données**. Pour plus d'informations sur les types de règles, consultez le guides des principes fondamentaux.

4. Cliquez sur **Terminé** pour fermer la boîte de dialogue Mode.
5. (Facultatif) Pour configurer la reconnaissance optique des caractères, les listes d'autorisation et d'autres options de protection, cliquez sur **Paramètres Avancés**.
   Pour plus d'informations sur les options disponibles, voir "Paramètres avancés" (p. 1595).
6. Enregistrez le plan de protection et appliquez-le aux ressources que vous souhaitez protéger.

Paramètres avancés

Vous pouvez utiliser les paramètres avancés des plans de protection avec Data Loss Prevention afin d'augmenter la qualité de l'inspection du contenu de données dans les canaux contrôlés par Data Loss Prevention (DLP), ainsi que pour exclure des contrôles préventifs les transferts de données vers les types de périphériques figurant dans la liste d'autorisation, les catégories de communications réseau, les hôtes de destination, ainsi que les transferts de données initiés par les applications de la liste d'autorisation. Vous pouvez configurer les paramètres avancés suivants :

© Acronis International GmbH, 2003-2026

- **Reconnaissance optique des caractères**
  Ce paramètre active ou désactive la reconnaissance optique des caractères afin d'extraire des sections de texte dans 31 langues pour une inspection de contenu plus poussée à partir de fichiers graphiques et d'images qui se trouvent dans les documents, les messages, les analyses, les captures d'écran et d'autres objets.
- **Transfert des données protégées par mot de passe**
  Le contenu des archives et des documents protégés par mot de passe ne peut pas être inspecté. Grâce à ce paramètre, Data Loss Prevention (DLP) permet à l'administrateur de choisir si les transferts sortants de données protégées par mot de passe doivent être autorisés ou bloqués.
- **Empêcher le transfert de données en cas d'erreur**
  L'analyse de contenu envoyée peut parfois échouer ou une autre erreur de contrôle peut se produire dans les opérations de l'agent DLP. Si cette option est activée, le transfert est bloqué. Si l'option est désactivée, le transfert est autorisé malgré l'erreur.
- **Liste d'autorisation des types de terminal et des communications réseau**
  Les transferts de données vers des types de périphériques et dans les communications réseau sélectionnés dans cette liste sont autorisés, quelles que soient la sensibilité des données et la règle de flux des données appliquée.

  Avertissement !
  Cette option est utilisée si des problèmes liés à un type de terminal ou à un protocole spécifique se produisent. N'activez pas cette option, sauf si un représentant du support vous le conseille.

- **Liste d'autorisation des hôtes distants**
  Les transferts de données vers des hôtes de destination spécifiés dans cette liste sont autorisés, quelles que soient la sensibilité des données et la règle de flux des données appliquée.
- **Liste d'autorisation des applications**
  Les transferts de données réalisés par des applications spécifiées dans cette liste sont autorisés, quelles que soient la sensibilité des données et la règle de flux des données appliquée.

L'indicateur **Niveau de sécurité** des Paramètres avancés affichés dans les vues **Créer un plan de protection** et Détails d'un plan de protection comprend la logique suivante d'indication de niveau :

- **Basique** indique qu'aucun paramètre avancé n'est activé.
- **Modéré** indique qu'un ou que plusieurs paramètres sont activés, mais que la combinaison **Reconnaissance optique des caractères**, **Transfert des données protégées par mot de passe** et **Empêcher le transfert de données en cas d'erreur** n'est pas activée.
- **Strict** indique qu'au moins la combinaison **Reconnaissance optique des caractères**, **Transfert des données protégées par mot de passe** et **Empêcher le transfert de données en cas d'erreur** est activée.

Détection automatique de la destination

En mode d'observation mixte, Data Loss Prevention applique des règles différentes en fonction de la destination du transfert de données détecté (interne ou externe). La logique permettant de

© Acronis International GmbH, 2003-2026

déterminer qu'une destination est interne est décrite ci-dessous. Toutes les autres destinations sont considérées comme externes.

Pour chaque transfert de données intercepté, Data Loss Prevention détecte automatiquement si le serveur HTTP, FTP ou SMB de destination est interne en effectuant une requête DNS et en comparant les noms FQDN de l'ordinateur sur lequel s'exécute l'agent Data Loss Prevention et du serveur distant. Si la requête DNS échoue, il vérifie également si la ressource protégée et le serveur distant se trouvent dans le même réseau. Les serveurs ayant le même nom de domaine (ou se trouvant dans le même sous-réseau) que l'ordinateur sur lequel s'exécute l'agent Data Loss Prevention sont considérés comme internes.

Pour la communication par e-mail, le module Data Loss Prevention traite comme étant des transferts internes tous les e-mails envoyés à partir d'une adresse e-mail d'entreprise à l'aide du serveur de messagerie d'entreprise si l'adresse e-mail du destinataire se trouve sur le même domaine que l'adresse e-mail de l'expéditeur, et que le nom du serveur de messagerie du destinataire est le même.

Les e-mails autres que ceux de l'entreprise sont traités comme étant des communications externes, sauf si le compte du destinataire est connu. Les adresses e-mail connues sont mises à jour, car la prévention des pertes de données surveille l'activité des utilisateurs sur le réseau et met à jour la base de données du backend à l'aide des données des adresses associées à l'utilisateur.

Les communications par Messenger sont traitées comme étant des communications externes, sauf si le compte du destinataire est connu. Les comptes connus sont mis à jour, car la prévention de la perte de données surveille l'activité des utilisateurs sur le réseau et met à jour la base de données du backend à l'aide des données des comptes associés à l'utilisateur.

Définitions des données sensibles

Cette rubrique décrit la logique d'identification des données sensibles lors de l'analyse de contenu.

Pour réduire le nombre de faux positifs, les correspondances identiques sont comptabilisées comme une seule correspondance pour tous les groupes des expressions logiques décrites.

Important
Les expressions logiques utilisées pour l'identification de contenu sont fournies à titre d'information uniquement et ne décrivent pas la solution en détail.

Informations de santé protégées (PHI)

Langues prises en charge

- Anglais américain, anglais britannique, anglais international
- Finlandais
- Italien

© Acronis International GmbH, 2003-2026

- Français
- Polonais
- Russe
- Hongrois
- Norvégien
- Espagnol

Données considérées comme des informations de santé protégées

Les données suivantes sont considérées comme des informations de santé protégées.

- Prénoms et noms
- Adresse (rue, ville, comté, circonscription, code postal et leurs codes géographiques équivalents)
- Numéros de téléphone
- Adresses e-mail
- Numéros de sécurité sociale
- Numéros de bénéficiaires de la couverture santé
- Numéros de compte bancaire
- URL
- Numéros d'adresse IP
- Codes ICD-10-CM
- ICD-10-PCS-and-GEMs
- HIPAA
- Autre élément relatif aux soins de santé
- Numéros de carte de crédit

Expression logique utilisée pour la détection de contenu

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR. L'opérateur OR est utilisé pour rejoindre différents groupes de données dans la liste ci-dessus si l'opérateur logique AND n'est pas spécifié explicitement. Les numéros entre parenthèses représentent le nombre d'instances détectées qui renverraient un résultat de détection positif.

- **Numéros de sécurité sociale** (5)
- (Prénoms et noms (3) OR Adresse (3) OR Numéros de téléphone (3) OR Adresse e-mail (3) OR Numéros de compte bancaire (3) OR Numéros de carte de crédit (3)) AND (Numéros de sécurité sociale (3) OR Numéros de bénéficiaires de la couverture santé (3) * OR Codes ICD-10-CM (3) OR PCS et GEM ICD-10 (3) OR HIPAA (3) OR * Autre élément relatif aux soins de santé (3))

© Acronis International GmbH, 2003-2026

Informations personnelles identifiables (PII)

Langues prises en charge

- Anglais américain, anglais britannique, anglais international
- Bulgare
- Chinois
- Tchèque
- Danois
- Néerlandais
- Finlandais
- Français
- Allemand
- Hongrois
- Indonésien
- Italien
- Coréen
- Malais
- Norvégien
- Polonais
- Portugais (Brésil)
- Portugais (Portugal)
- Roumain
- Russe
- Serbe
- Singapour
- Espagnol
- Suédois
- Taïwan
- Turc
- Thaï
- Japonais

© Acronis International GmbH, 2003-2026

Données considérées comme informations personnelles identifiables (PII)

- Prénoms et noms
- Adresse (rue, ville, comté, code postal)
- Numéros de compte bancaire
- Numéros personnels et identifiants fiscaux
- Numéros de passeport
- Numéros de sécurité sociale
- Numéros de téléphone
- Numéros de plaque d'immatriculation
- Numéros de permis de conduire
- Identifiants et numéros de série
- Adresses IP
- Adresses e-mail
- Numéros de carte de crédit

Expression logique utilisée pour la détection de contenu

Expression logique pour toutes les langues prises en charge, à l'exception du japonais

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR ou AND. Les numéros entre parenthèses représentent le nombre d'instances détectées qui renverraient un résultat de détection positif.

- Numéros personnels et identifiants fiscaux (5)
- Prénoms et noms (3) AND **(**Numéro de carte de crédit (3) OR Numéro de sécurité sociale (3) OR Numéro de compte bancaire (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3) OR Adresses IP (3) OR Numéros de plaque d'immatriculation (3) OR Identifiants et numéros de série**)**
- Numéros de téléphone (3) AND **(**Numéro de carte de crédit (3) OR Numéro de sécurité sociale (3) OR Numéro de compte bancaire (3) OR Adresse (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3) OR Numéros de plaque d'immatriculation (3) OR Identifiants et numéros de série (3)**)**
- **(**Prénoms et noms (30) OR Adresse (30)**)** AND **(**Adresses e-mail (30) OR Numéros de téléphone (30) OR Adresses IP (30)**)**
- Adresses e-mail (3) AND **(**Numéro de carte de crédit (3) OR Numéro de sécurité sociale (3) OR Numéro de compte bancaire (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3) OR Numéros de plaque d'immatriculation (3) OR Identifiants et numéros de série (3)**)**

© Acronis International GmbH, 2003-2026

- Adresse e-mail (30) AND **(**Adresse (30) OR Numéros de téléphone (30)**)**
- Prénoms et noms (30) AND adresse (30)
- Numéros de téléphone (30) AND adresse (30)
- Prénoms et noms (3) AND Numéros de compte bancaire (3)
- Numéros de téléphone (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de sécurité sociale (3) OR Numéros personnels et identifiants fiscaux (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3)**)**

Expression logique pour le japonais

Remarque
La détection de contenu ne comptabilise que les correspondances uniques.

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR. L'opérateur OR est utilisé pour rejoindre différents groupes si l'opérateur logique AND n'est pas spécifié explicitement.

- Numéros de sécurité sociale (5)
- Prénoms et noms (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3)**)**
- Prénoms et noms (30) AND **(**Adresses e-mail (30) OR Numéros de téléphone (30) OR Adresses IP (30) OR Adresse (30)**)**
- Adresse (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de permis de conduire (3) OR Numéros de passeport (3) OR Numéros de sécurité sociale (3)**)**
- Adresse e-mail (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Numéros de sécurité sociale (3) OR Numéros de permis de conduire (3)**)**
- Adresse (5) AND **(**Adresse e-mail (5) OR Prénoms et noms (5) OR Numéros de téléphone (5) OR Adresses e-mail (5)**)**
- Prénoms et noms (3) AND Numéros de compte bancaire (3)
- Numéros de téléphone (3) AND **(**Numéro de carte de crédit (3) OR Numéro de compte bancaire (3) OR Adresse (3) OR Numéros de sécurité sociale (3) OR Numéros de permis de conduire (3)**)**

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

Langues prises en charge

Ce groupe de sensibilité ne dépend pas de la langue. Les données PCI DSS sont en anglais dans tous les pays.

© Acronis International GmbH, 2003-2026

Données considérées comme données PCI DSS

- Données du détenteur de la carte
  - Numéro de compte principal (PAN)
  - Nom du détenteur de la carte
  - Date d'expiration
  - Code du service
- Données d'authentification sensibles
  - Données de piste complète (données d'une bande magnétique ou équivalent sur une puce)
  - CAV2/CVC2/CVV2/CID
  - Codes PIN/Blocs PIN

Expression logique utilisée pour la détection de contenu

L'expression logique se compose des chaînes suivantes rejointes par l'opérateur logique OR. Les numéros entre parenthèses représentent le nombre d'instances détectées qui renverraient un résultat de détection positif.

- Numéro de carte de crédit (5)
- Numéro de carte de crédit (3) AND (Nom américain (Ex) (3) OR Nom américain (3) OR Mots-clés DSS PCI (3) OR Date (mois/an) (3))
- Vidage de carte de crédit (5)

Marqué confidentiel

Des données marquées comme confidentielles sont détectées dans le groupe de mots-clés.

La condition de correspondance est pondérée et chaque mot a une pondération égale à 1. La détection de contenu est considérée comme positive lorsque la condition de correspondance est remplie si la pondération est supérieure à 3.

Langues prises en charge

- Anglais
- Bulgare
- Chinois simplifié
- Chinois traditionnel
- Tchèque
- Danois
- Néerlandais
- Finlandais

© Acronis International GmbH, 2003-2026

- Français
- Allemand
- Hongrois
- Indonésien
- Italien
- Japonais
- Coréen
- Malais
- Norvégien
- Polonais
- Portugais - Brésil
- Portugais - Portugal
- Russe
- Serbe
- Espagnol
- Suédois
- Turc

Groupes de mots-clés

Le groupe de mots-clés de chaque langue contient les équivalents propres au pays des mots-clés suivants qui sont utilisés pour la langue anglaise (non sensible à la casse).

- confidentiel
- distribution interne
- non destiné à la distribution
- ne pas distribuer
- non adapté au public
- non destiné à la distribution externe
- à usage interne uniquement
- documentation hautement qualifiée
- privé
- informations privilégiées
- à usage interne uniquement
- à usage officiel uniquement

© Acronis International GmbH, 2003-2026

Événements de prévention des pertes de données

Data Loss Prevention génère des événements dans la vue des événements DLP comme suit.

- En mode d'observation, les événements sont générés pour tous les transferts de données justifiés.
- En mode d'application, les événements sont générés en fonction de l'action **Écrire dans un journal** configurée pour chaque règle déclenchée.

Pour afficher les événements d'une règle dans la règle de flux de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Règle de flux de données**.
3. Localisez la règle pour laquelle vous souhaitez visualiser les événements, puis cliquez sur le bouton représentant des points de suspension à la fin de la ligne de la règle.
4. Sélectionnez **Afficher les événements**.

Pour afficher les détails concernant un événement dans la vue des événements DLP

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Événements DLP**.
3. Cliquez dans la liste sur un événement pour en voir les détails.
   Le panneau détails de l'événement se développe vers la droite.
4. Faites défiler l'affichage du panneau détails de l'événement vers le haut ou vers le bas pour afficher les informations disponibles.
   Les détails affichés dépendent du type de règle et des paramètres de règle qui ont déclenché l'événement.

Pour filtrer les événements de la liste des événements DLP

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Événements DLP**.
3. En haut à gauche, cliquez sur **Filtrer**.
4. Sélectionnez dans les menus déroulants la catégorie de sensibilité, la ressource, le type d'action, l'utilisateur et le canal.
   Vous pouvez sélectionner plusieurs éléments dans les menus déroulants. Le filtrage applique l'opérateur logique OR entre les éléments du même menu. Quant à l'opérateur logique AND, il est utilisé entre des éléments de menus différents.
   Par exemple, si vous sélectionnez la catégorie de sensibilité **PHI** et **PII**, le résultat renvoie tous les événements contenant PHI ou PII, ou les deux. Si vous sélectionnez la catégorie de sensibilité **PHI** et l'action **Accès en écriture**, seuls les événements correspondant aux deux catégories apparaissent dans le résultat filtré.
5. Cliquez sur **Appliquer**.

© Acronis International GmbH, 2003-2026

6. Pour afficher de nouveau tous les événements, cliquez sur **Filtre**, **Réinitialiser au défaut** et **Appliquer**.

Pour rechercher des événements dans la liste des événements DLP

1. Répétez les étapes 1-2 de la procédure ci-dessus.
2. Dans la liste déroulante située à droite de Filtre, sélectionnez une catégorie dans laquelle vous souhaitez effectuer une recherche : **Expéditeur**, **Destination**, **Processus**, **Objet du message** ou **Motif**.
3. Dans la zone de texte, saisissez l'expression qui vous intéresse et confirmez en appuyant sur la touche Entrée du clavier.
   Seuls les événements correspondant à l'expression que vous avez saisie apparaît dans la liste.
4. Pour réinitialiser la liste des événements, cliquez sur le **X**, connectez-vous à la zone de texte de recherche, puis appuyez sur Entrée.

Pour afficher la liste des événements liés à des règles spécifiques de flux de données

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Règle de flux de données**.
3. Cochez la case figurant devant le nom de la règle qui vous intéresse.
   Vous pouvez sélectionner plusieurs règles si nécessaire.
4. Cliquez sur **Afficher les événements**.
   L'affichage passe à **Protection** > **Événements DLP** et la liste affiche les événements liés aux règles que vous avez sélectionnées.

Widgets Data Loss Prevention dans le tableau de bord Vue d'ensemble

Le tableau de bord **Vue d'ensemble** fournit un certain nombre de widgets personnalisables qui offrent une vue d'ensemble des opérations liées au service Cyber Protection, y compris le module Data Loss Prevention. Vous trouverez les widgets Data Loss Prevention suivants dans le tableau de bord **Vue d'ensemble**, sous **Surveillance**.

- **Transferts de données sensibles** - affiche le nombre total d'opérations de transfert de données sensibles aux destinataires internes et externes. Le graphique est divisé par le type d'autorisation : autorisées, justifiées ou bloquées. Vous pouvez personnaliser ce widget en sélectionnant la plage souhaitée (1 jour, 7 jours, 30 jours ou ce mois).
- **Catégories de données sensibles sortantes** - affiche le nombre total de transferts de données sensibles aux destinataires externes. Le graphique est divisé par les catégories sensibles : Informations de santé protégées (PHI), Informations personnelles identifiables (PII), PCI DSS et Marqué confidentiel (Confidentiel).
- **Principaux émetteurs de données sensibles sortantes** - affiche le nombre total de transferts de données sensibles depuis l'organisation vers des destinataires externes, ainsi que la liste des 5 utilisateurs ayant le plus de transferts (avec ces nombres). Cette statistique inclut les transferts

© Acronis International GmbH, 2003-2026

autorisés et justifiés. Vous pouvez personnaliser ce widget en sélectionnant la plage souhaitée (1 jour, 7 jours, 30 jours ou ce mois).

- **Principaux émetteurs de transferts de données sensibles bloqués** - affiche le nombre total de transferts de données sensibles bloqués et la liste des 5 utilisateurs ayant le plus de tentatives de transferts (avec ces nombres). Vous pouvez personnaliser ce widget en sélectionnant la plage souhaitée (1 jour, 7 jours, 30 jours ou ce mois).
- **Événements DLP récents** - affiche les détails des événements récents de prévention de la perte de données sur la période donnée. Vous pouvez personnaliser ce widget à l'aide des options suivantes :
  - **Plage (date de publication)** (1 jour, 7 jours, 30 jours ou ce mois).
  - Nom de la **ressource**
  - **État de l'opération** (autorisée, justifiée ou bloquée)
  - **Sensibilité** (PHI, PII, Confidentiel, DSS PCI)
  - **Type de destination** (externe, interne)
  - **Regroupement** (ressource, utilisateur, canal, type de destination)

Les widgets sont mis à jour toutes les cinq minutes. Les widgets disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Vous pouvez télécharger l'état actuel du tableau de bord ou bien l'envoyer par e-mail au format .pdf et/ou .xlsx.

Catégories personnalisées de sensibilité

Les catégories personnalisées de données sensibles peuvent aider une organisation à protéger sa propriété intellectuelle et ses données confidentielles propres en élargissant le catalogue intégré de DLP des définitions de contenu liées à la conformité réglementaire.

Pour créer une catégorie personnalisée de données sensibles

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Sélectionnez **Catégorie de sensibilité**.
   La liste des catégories de sensibilité s’affiche.
4. Cliquez sur **Ajouter** en haut à droite de la fenêtre.
5. Dans la fenêtre qui s'ouvre, entrez un nom pour la nouvelle catégorie de sensibilité et cliquez sur **Créer**.
   Par défaut, les catégories nouvellement créées ou clonées sont désactivées. Vous pouvez les activer une fois que vous avez configuré tous leurs paramètres.
6. Dans la liste déroulante à droite de la ligne, cliquez sur **Modifier**.
7. Dans la boîte de dialogue **Modifier la sensibilité**, cliquez sur **Ajouter une ligne** pour développer la liste des détecteurs de contenu.

© Acronis International GmbH, 2003-2026

8. Sélectionnez les détecteurs de contenu à ajouter.
   - Pour ajouter des détecteurs de contenu existants, sélectionnez les cases à cocher à côté de leurs noms, puis cliquez sur **Ajouter** dans le coin inférieur droit.
   - Pour définir un nouveau détecteur de contenu, cliquez sur **Ajouter**, et configurez le détecteur dont vous avez besoin.
     Au lieu de partir de zéro, vous pouvez cloner un détecteur de contenu existant et l'éditer.
9. Vérifiez que vous avez ajouté tous les détecteurs de contenu nécessaires, puis cliquez sur **Terminé** dans le coin inférieur droit.
10. Activez votre catégorie de sensibilité personnalisée.

Au lieu de créer une nouvelle catégorie de sensibilité de toutes pièces, vous pouvez également cloner une catégorie existante (intégrée ou personnalisée) et ajuster ses paramètres.

1. Pour cloner une sensibilité existante, sélectionnez **Cloner** dans la liste déroulante à la fin de sa ligne.
2. Modifiez la catégorie clonée pour ajouter ou supprimer des détecteurs de contenu si nécessaire, puis cliquez sur **Terminé** pour enregistrer vos modifications.

Remarque
Le clonage d'une catégorie de sensibilité intégrée à l'intérieur d'un tenant crée une nouvelle sensibilité qui contient les mêmes détecteurs qui deviennent Personnalisés une fois copiés.

Consultez "Détecteurs de contenu personnalisés" (p. 1607).

Détecteurs de contenu personnalisés

Les détecteurs de contenu permettent de définir de manière centralisée les types de contenu pour lesquels un contrôle d'accès est souhaité. Les détecteurs de contenu spécifient les critères de filtrage de contenu pour identifier les données auxquelles des règles basées sur le contenu doivent être appliquées.

Type de fichier

Pour créer un détecteur de contenu de type de fichier

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Cliquez sur **Détecteurs de contenu**.
   La liste des détecteurs de contenu s'ouvre.
4. Dans le coin supérieur droit de l'écran, cliquez sur **Ajouter**.
5. Dans la liste déroulante, sélectionnez **Type de fichier**.
6. Configurer le détecteur de contenu.
   a. Saisissez un nom et une description pour le détecteur de contenu.
   b. [Facultatif] Sélectionnez une catégorie de sensibilité dans la liste.

© Acronis International GmbH, 2003-2026

c. Dans la liste **Types de fichiers pris en charge** cliquez sur l'icône plus pour déplacer le type sélectionné vers la liste **Types de fichiers sélectionnés**. En cliquant sur l'icône « plus » située à droite d'un type de fichier pris en charge, vous le déplacez vers la liste des types de fichiers sélectionnés. Vous pouvez également sélectionner plusieurs types de fichiers pris en charge en cochant les cases situées à côté de leur nom, puis en utilisant le bouton **Ajouter la sélection** en haut à droite.

d. Pour supprimer un type de fichier de la liste **Types de fichiers sélectionnés**, cliquez sur l'icône de la corbeille à droite de son nom. Vous pouvez également supprimer plusieurs types de fichiers en cochant les cases correspondantes et en cliquant sur le bouton **Retirer la sélection**.

7. Dans l'angle inférieur droit, cliquez sur **Enregistrer**.

Mots-clés

Pour créer un détecteur de contenu de mots-clés

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Cliquez sur **Détecteurs de contenu**.
   La liste des détecteurs de contenu s'ouvre.
4. Dans le coin supérieur droit de l'écran, cliquez sur **Ajouter**.
5. Dans la liste déroulante, cliquez sur **Mots-clés**.
6. Configurer le détecteur de contenu.
   a. Saisissez les mots-clés manuellement, un à la fois, ou importez-les à partir d'un fichier CSV ou TXT.

      Remarque
      Chaque mot-clé ou phrase dans le fichier doit être spécifié sur une nouvelle ligne.

      Une fois l'importation effectuée, vous pouvez soit fusionner les nouveaux mots-clés avec la liste existante, soit remplacer cette liste par les mots-clés importés.

   b. Configurez si le détecteur de contenu doit correspondre à tous les mots-clés de la liste, à un seul mot-clé de la liste, ou à un nombre personnalisé de mots-clés.
7. Dans l'angle inférieur droit, cliquez sur **Enregistrer**.

Motif

Pour créer un détecteur de contenu de modèle

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Cliquez sur **Détecteurs de contenu**.
   La liste des détecteurs de contenu s'ouvre.
4. Dans le coin supérieur droit de l'écran, cliquez sur **Ajouter**.

© Acronis International GmbH, 2003-2026

5. Dans la liste déroulante, cliquez sur **Motif**.
6. Configurer le détecteur de contenu.
   a. **Nom** - Spécifiez le nom du groupe.
   b. **Description** - Spécifiez une description pour le groupe.
   c. **Expression régulière** - Entrez une expression régulière.
   d. **Valider** - Vérifiez la syntaxe de l'expression régulière.
   e. **Vérifier maintenant** - Entrez des chaînes de test et consultez le résultat. DLP prend en charge la mise en surbrillance colorée en temps réel des tests. Toutes les correspondances sont mises en surbrillance.
   f. **Validation** - Lorsqu'il est configuré pour effectuer une validation, le groupe détecte une correspondance uniquement en cas de correspondance avec le type de validation sélectionné en plus de l'expression spécifiée. Pour correspondre au groupe, les données doivent correspondre à l'expression et en outre passer la validation.
      Si **Aucune validation** n'est sélectionnée dans ce champ, le groupe ne réalise pas de validation. Pour correspondre au groupe dans ce cas, les données doivent uniquement correspondre à l'expression spécifiée.
      Pour configurer la validation, sélectionnez le type souhaité dans la liste déroulante dans ce champ.
   g. **Nombre minimum de correspondances** - Entrez le nombre de correspondances qui déclencheront la règle d'inspection du contenu.

      Important
      Le détecteur vérifie la correspondance exacte d'au plus le premier mégaoctet du contenu fourni pour inspection. Si le contenu dépasse 1 Mo, la règle avec la condition **Correspondance exacte** n'est pas déclenchée même si le premier mégaoctet du contenu correspond à l'expression régulière du détecteur.

   h. **Sensible à la casse** - Lorsque cette case à cocher est sélectionnée, le groupe fait la distinction entre les caractères minuscules et majuscules. Par exemple, les mots `Term` et `term` seront traités différemment, de sorte que le groupe peut être configuré pour correspondre au mot `Term` mais pas `term`.
      Lorsque cette case à cocher est désactivée, le groupe ne fait pas de distinction entre les majuscules et les minuscules. Par exemple, si `Term` correspond au groupe, alors `term` ou même `tErM` lui correspondra également.
   i. **Compter les correspondances identiques comme une seule correspondance** - Combinez les correspondances en double renvoyées par l'expression régulière en une seule correspondance. Pour ce faire, sélectionnez la case à cocher **Compter les correspondances identiques comme une seule correspondance**.
7. Dans l'angle inférieur droit, cliquez sur **Enregistrer**.

Complexe

Pour créer un détecteur de contenu complexe

© Acronis International GmbH, 2003-2026

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Protection** > **Prévention des pertes de données** > **Classifieurs de données**.
3. Cliquez sur **Détecteurs de contenu**.
   La liste des détecteurs de contenu s'ouvre.
4. Dans le coin supérieur droit de l'écran, cliquez sur **Ajouter**.
5. Dans la liste déroulante, cliquez sur **Complexe**.
6. Configurer le détecteur de contenu.
   Le détecteur de contenu complexe vous permet de créer des combinaisons logiques de plusieurs détecteurs de contenu. Vous pouvez parcourir la base de données des détecteurs disponibles et les combiner à l'aide des opérateurs logiques AND, OR et NOT.
7. Dans l'angle inférieur droit, cliquez sur **Enregistrer**.

Au lieu de créer un nouveau détecteur de contenu à partir de zéro, vous pouvez également cloner un détecteur de contenu intégré ou personnalisé existant et ajuster ses paramètres.

Pour cloner un détecteur de contenu existant

1. Dans la liste des détecteurs de contenu, sélectionnez celui que vous souhaitez cloner, puis cliquez sur **Cloner** dans la liste déroulante à la fin de sa ligne.
2. Modifiez le détecteur de contenu cloné pour ajouter ou supprimer des paramètres si nécessaire et cliquez sur **Terminé** pour enregistrer vos modifications.

Remarque
Le clonage d'un détecteur de contenu intégré crée un détecteur de contenu personnalisé.

Carte de l'organisation

Remarque
Cette fonctionnalité n'est accessible qu'aux administrateurs de l'entreprise.

La carte de l'organisation est une base de données qui contient les données des utilisateurs et de tous leurs comptes utilisés pour transférer des données via la messagerie instantanée, la messagerie électronique ou tout autre moyen, et qui ont été interceptées par DLP.

La carte de l'organisation permet de créer et de gérer des groupes d'utilisateurs dans DLP, ainsi que de gérer les utilisateurs et les comptes associés aux utilisateurs dans DLP. Les groupes d'utilisateurs peuvent ensuite être utilisés pour la gestion des règles DLP basées sur les groupes.

Pour localiser la carte de l'organisation

- Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.

© Acronis International GmbH, 2003-2026

Comment cela fonctionne-t-il ?

Remarque
La carte de l'organisation est remplie lorsque le module DLP (Data Loss Prevention) fonctionne en mode Observation.

Pour chaque transfert de données intercepté par l'agent DLP, les attributs suivants sont collectés en amont.

Attribut	Description	Étiquette dans l'interface utilisateur
Unité d'organisation	Groupe créé manuellement. L'unité d'organisation peut avoir une ou plusieurs unités d'organisation imbriquées.	Nom du groupe, tel que défini
ID de sécurité	Identificateur de sécurité unique.	Sur la page des détails de l'utilisateur > **SID**
	Nom affiché convivial dérivé des noms de comptes utilisateur. Ce nom n'est pas toujours disponible dans la carte de l'organisation.	**Nom**
PC\Nom de l'utilisateur	Nom de l'utilisateur du terminal (ressource). Un nom d'utilisateur ne peut être attribué qu'à une seule unité d'organisation.	**Nom de l'utilisateur**
Terminal (ressource)	Nom du terminal (ressource).	**Ressource**
Compte	Comptes utilisés par un utilisateur pour communiquer via la messagerie électronique et la messagerie instantanée, et qui ont été interceptés par l'agent DLP. Par exemple, si l'agent détecte que le nom d'utilisateur « PC\Jean » utilise jean@gmail.com pour envoyer un e-mail, ce compte est lié au nom d'utilisateur PC\Jean.	**Comptes**

Dans la carte de l'organisation, vous pouvez afficher et rechercher des comptes, des utilisateurs et des groupes, et créer, modifier et supprimer des groupes.

Pour rechercher des comptes spécifiques

Dans le cadre d'une enquête sur un incident, les administrateurs peuvent avoir besoin de trouver le propriétaire d'un compte spécifique impliqué dans une violation potentielle de données.

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.

© Acronis International GmbH, 2003-2026

2. Dans la zone de texte **Recherche** située au-dessus de la liste des utilisateurs, commencez à taper le nom du compte ou collez-le.
   La liste est filtrée au fur et à mesure de la saisie.

Pour rechercher un nom d'utilisateur spécifique

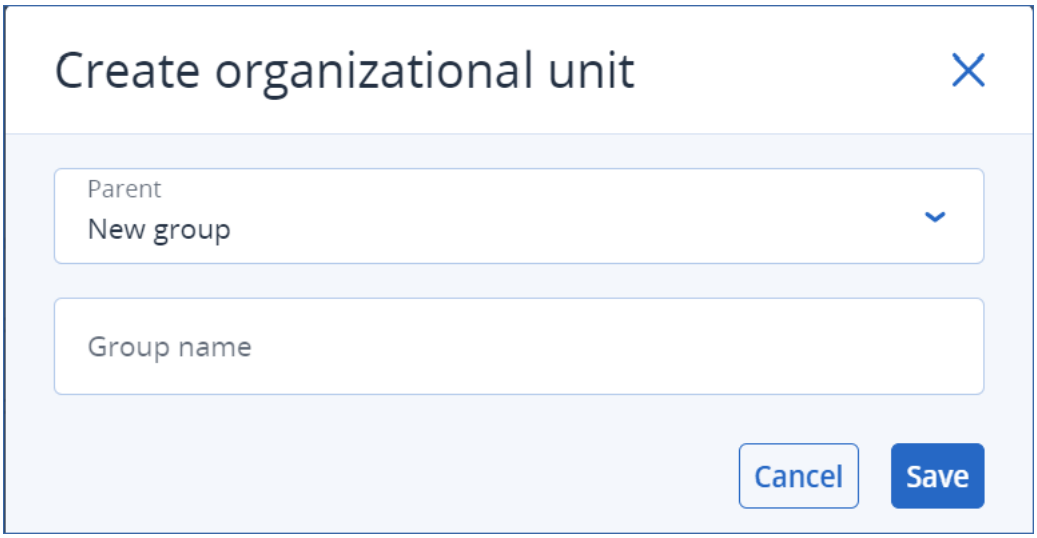
1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Pour effectuer une recherche dans un groupe spécifique, cliquez sur le nom du groupe dans la liste.
3. Dans la zone de texte **Recherche** située au-dessus de la liste des utilisateurs, commencez à taper le nom du compte ou collez-le.
   La liste est filtrée au fur et à mesure de la saisie.

Pour afficher les comptes utilisés par un nom d'utilisateur particulier

1. Localisez l'utilisateur souhaité dans la liste.
2. Cliquez sur les trois points situés à l'extrémité de la ligne de l'utilisateur et sélectionnez **Afficher**.
3. Dans la boîte de dialogue des détails de l'utilisateur, localisez la section **Comptes associés**.
4. Vous pouvez ajouter des commentaires dans la zone de texte Description.

Pour créer un groupe d'utilisateurs

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Dans la partie inférieure gauche de la liste des groupes, cliquez sur **Créer un groupe**.
   La boîte de dialogue Créer une entité d'organisation s'ouvre.



3. Dans le menu déroulant Parent, sélectionnez le contexte du nouveau groupe.

Remarque
Vous ne pourrez pas modifier le parent ultérieurement. Le groupe restera imbriqué dans ce contexte.

© Acronis International GmbH, 2003-2026

4. Saisissez un nom de groupe et cliquez sur **Enregistrer**.

Pour ajouter un utilisateur à un groupe

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Dans la liste des utilisateurs, localisez l'utilisateur que vous souhaitez ajouter et cochez la case au début de sa ligne.
   Les boutons **Déplacer la sélection** et **Supprimer la sélection** apparaissent au-dessus de la liste des utilisateurs.
3. Cliquez sur **Déplacer la sélection**.
   La boîte de dialogue Déplacer l'utilisateur s'ouvre.
4. Sélectionnez un nouveau parent pour l'utilisateur sélectionné et cliquez sur **Enregistrer**.

Remarque
Un utilisateur ne peut appartenir qu'à un seul groupe.

Pour supprimer un compte associé à un utilisateur

1. Localisez l'utilisateur souhaité dans la liste.
2. Cliquez sur les trois points situés à l'extrémité de la ligne de l'utilisateur et sélectionnez **Afficher**.
3. Dans la boîte de dialogue des détails de l'utilisateur, localisez la section **Comptes associés**.
4. Localisez le compte que vous souhaitez supprimer et cliquez sur les trois points situés à côté.
5. Dans la liste déroulante, sélectionnez **Supprimer**.

Pour renommer un groupe d'utilisateurs

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Cliquez sur les trois points situés à côté du nom du groupe et cliquez sur **Renommer**.

Pour supprimer un groupe d'utilisateurs

1. Dans la console Cyber Protect Cloud, accédez à **Protection** > **Prévention des pertes de données** > **Carte de l'organisation**.
2. Cliquez sur les trois points situés à côté du nom du groupe et cliquez sur **Supprimer**.
   Tous les utilisateurs du groupe sont déplacés vers l'entité parent.

Problèmes connus et limites

- [DEVLOCK-4028] Aucun contrôle des chats de groupe dans l'agent Zoom pour ordinateur.
- [DEVLOCK-4016] Le nom convivial et l'identifiant d'expéditeur ne sont pas capturés pour GMX Web Mail et Web.de Mail en cas de création de brouillon.

© Acronis International GmbH, 2003-2026

- [DEVLOCK-4447] Aucune boîte de dialogue de justification pour WebMail naver.com en cas de création de brouillon.

© Acronis International GmbH, 2003-2026

Autres outils Cyber Protection

Mode de conformité

Le mode de Conformité est conçu pour les clients ayant des exigences de sécurité élevées. Ce mode exige un chiffrement obligatoire pour toutes les sauvegardes et n'autorise que les mots de passe de chiffrement définis localement.

Avec le mode de Conformité, toutes les sauvegardes créées dans un tenant client et dans ses unités sont chiffrées automatiquement avec l'algorithme AES et une clé de chiffrement 256 bits. Les utilisateurs peuvent définir leur mot de passe de chiffrement uniquement sur les terminaux protégés et ne peuvent pas les définir dans les plans de protection.

Important
Vous ne pouvez pas désactiver le mode de Conformité.

Limites

- Le mode de Conformité n'est compatible qu'avec les agents de la version 15.0.26390 ou supérieure.
- Le mode de Conformité n'est pas disponible pour les terminaux exécutant Red Hat Enterprise Linux 4.x ou 5.x et leurs dérivés.
- Les services cloud ne peuvent pas accéder aux mots de passe de chiffrement. En raison de cette limitation, certaines fonctionnalités ne sont pas disponibles pour les tenants en mode de Conformité.

Fonctionnalités non prises en charge

Les fonctionnalités suivantes ne sont pas disponibles pour les tenants en mode de Conformité :

- Restauration depuis la console Cyber Protect
- Navigation de niveau fichier dans les sauvegardes depuis la console Cyber Protect
- Accédez à la console Web Restore
- Sauvegarde de Cloud à Cloud
- Sauvegarde des sites Web
- Sauvegarde d'applications
- Sauvegarde des terminaux mobiles
- Analyse antimalware des sauvegardes
- Restauration sûre
- Création automatique de listes d’autorisation d’entreprise
- Carte de la protection des données

© Acronis International GmbH, 2003-2026

- Reprise d'activité après sinistre
- Rapports et tableaux de bord liés aux fonctionnalités non disponibles

Définition du mot de passe de chiffrement

Vous devez définir le mot de passe de chiffrement localement sur le terminal protégé. Vous ne pouvez pas définir le mot de passe de chiffrement dans le plan de protection. Sans mot de passe, la création de sauvegardes échouera.

Avertissement !
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Vous pouvez définir le mot de passe de chiffrement de l'une des manières suivantes :

1. Lors de l'installation de l'agent de protection (pour Windows, macOS et Linux).
2. À l'aide de la ligne de commande (pour Windows et Linux).
   C'est la seule façon de définir un mot de passe de chiffrement sur une appliance virtuelle.
   Pour plus d'informations sur la manière de définir un mot de passe de chiffrement avec l'outil **Acropsh**, voir "Chiffrement" (p. 596).
3. Dans l'application Cyber Protect Monitor (pour Windows and macOS).

Pour définir le mot de passe de chiffrement dans Cyber Protect Monitor

1. Sur le terminal protégé, connectez-vous en tant qu'administrateur.
2. Cliquez sur l'icône de Cyber Protect Monitor dans la zone de notification (sous Windows) ou dans la barre des menus (sous macOS).
3. Cliquez sur l'icône en forme d'engrenage.
4. Cliquez sur **Chiffrement**.
5. Définissez le mot de passe de chiffrement.
6. Cliquez sur **OK**.

Modification du mot de passe de chiffrement

Vous pouvez modifier le mot de passe de chiffrement avant qu'un plan de protection ne crée la moindre sauvegarde.

Nous vous recommandons de ne pas modifier le mot de passe de chiffrement après la création des sauvegardes, car les sauvegardes ultérieures échoueront. Pour continuer à protéger le même ordinateur, vous devez lui créer un nouveau plan de protection. La modification du mot de passe de chiffrement et du plan de protection permettra la création de sauvegardes chiffrées avec le mot de passe modifié. Les sauvegardes qui ont été créées avant ces modifications ne seront pas affectées.

Si vous préférez, vous pouvez aussi conserver le plan de protection appliqué et modifier uniquement le nom du fichier de sauvegarde qu'il contient. Cela permettra aussi la création de

© Acronis International GmbH, 2003-2026

sauvegardes chiffrées avec le mot de passe modifié.Pour en savoir plus sur le nom du fichier de sauvegarde, reportez-vous à "Nom de fichier de sauvegarde" (p. 609).

Vous pouvez modifier le mot de passe de chiffrement de l'une des manières suivantes :

1. Dans l'application Cyber Protect Monitor (pour Windows and macOS).
2. À l'aide de la ligne de commande (pour Windows et Linux).
   Pour en savoir plus sur la définition d'un mot de passe de chiffrement avec l'outil **Acropsh**, reportez-vous à "Chiffrement" (p. 596).

Restauration de sauvegardes dans les tenants en mode de conformité

En mode de conformité, vous ne pouvez pas restaurer les sauvegardes dans la console Cyber Protect.

Les options suivantes sont disponibles :

- Restauration d'un ordinateur complet, de ses disques ou de ses fichiers à l'aide d'un support de démarrage.
- Extraction de fichiers à partir de sauvegardes locales d'ordinateurs Windows avec l'agent installé, à l'aide de l'Explorateur de fichiers Windows.

Stockage immuable

Le stockage immuable fournit une couche de protection critique pour les données de sauvegarde en empêchant la suppression ou la modification des points de restauration jusqu'à l'expiration de leur période de rétention. Cette protection garantit que les sauvegardes restent intactes même si les identifiants sont compromis, le ransomware désactive les outils de sécurité, ou des erreurs administratives se produisent. Bien que l'activation de l'immuabilité puisse légèrement augmenter les coûts de stockage parce que les anciens points de restauration ne peuvent pas être supprimés avant l'expiration de leur période de rétention, cette dépense prévisible est minime comparée à l'impact financier et opérationnel de la perte de données critiques. Des incidents réels ont démontré que l'immuabilité peut faire la différence entre une restauration complète et une perte de données catastrophique.

Le stockage immuable est disponible pour toutes les sauvegardes dans le cloud stockées dans une instance de stockage dans le cloud prise en charge. Voir "Stockages et agents pris en charge" (p. 1618).

Grâce au stockage immuable, vous pouvez accéder à des sauvegardes supprimées pendant la période de rétention spécifiée. Vous pouvez restaurer des contenus depuis ces sauvegardes, mais vous ne pouvez ni les modifier, ni les déplacer, ni les supprimer. À la fin de la période de rétention, les sauvegardes supprimées sont définitivement supprimées.

Le stockage immuable contient les sauvegardes suivantes :

© Acronis International GmbH, 2003-2026

- Sauvegardes supprimées manuellement.
- Sauvegardes supprimées automatiquement, conformément aux paramètres de la section **Durée de conservation** d'un plan de protection ou de la section **Règles de rétention** d'un plan de nettoyage.

Les sauvegardes supprimées du stockage immuable utilisent toujours de l'espace de stockage et sont facturées en conséquence.

Les tenants supprimés ne sont facturés pour aucun stockage, pas même le stockage immuable.

Modes de stockage immuable

Le stockage immuable est disponible dans les modes suivants :

- **Mode de gouvernance**
  Dans ce mode, toutes les sauvegardes supprimées restent dans le stockage immuable pendant la période de rétention spécifiée. Cela empêche les ransomwares ou les acteurs malveillants de manipuler ou d'effacer les données de sauvegarde et garantit l'intégrité des sauvegardes, ce qui est essentiel pour une reprise d'activité après sinistre fiable.
  Dans ce mode, vous pouvez changer la période de rétention ou passer en mode Conformité. Le stockage immuable ne peut être désactivé qu'en contactant l'équipe de Support.
- **Mode de conformité**
  En plus des avantages du mode Gouvernance, le mode Conformité aide les organisations à répondre aux exigences réglementaires en matière de rétention des données et de sécurité en empêchant les modifications de la stratégie de rétention, y compris le changement de la période de rétention ou sa désactivation.

  Important
  La sélection du mode Conformité est irréversible. Après avoir sélectionné ce mode, vous ne pouvez pas changer la période de rétention ou revenir au mode Gouvernance. Le stockage immuable ne peut pas être désactivé dans ce mode.

Stockages et agents pris en charge

- Le stockage immuable n'est pris en charge que pour le stockage dans le cloud.
  - Le stockage immuable est disponible pour les stockages dans le cloud hébergés par Acronis et ses partenaires qui utilisent Acronis Cyber Infrastructure version 4.7.1 ou ultérieure.
  - Tous les systèmes de stockage pouvant être utilisés avec Acronis Cyber Infrastructure Backup Gateway sont pris en charge. Par exemple, le stockage Acronis Cyber Infrastructure, les stockages Amazon S3 et EC2, et le stockage Microsoft Azure.
  - Le stockage immuable nécessite que le port TCP 40440 soit ouvert pour le service Backup Gateway dans Acronis Cyber Infrastructure. Dans les versions 4.7.1 et ultérieure, le port TCP 40440 est automatiquement ouvert avec le type de trafic **public Backup (ABGW)**. Pour plus d'informations sur les types de trafic, consultez la documentation d'Acronis Cyber Infrastructure.

© Acronis International GmbH, 2003-2026

- Le stockage immuable nécessite un agent de protection version 21.12 (15.0.28532) ou ultérieure.
- Seules les sauvegardes TIBX (version 12) sont prises en charge.

Activation du stockage immuable

Depuis septembre 2024, le stockage immuable en mode Gouvernance est activé par défaut, avec une période de rétention de 14 jours.

Vous pouvez activer le stockage immuable pour les tenants où il n'est pas encore activé en utilisant soit la console Cyber Protect, soit le Portail de gestion. Les deux offrent les mêmes paramètres. Les étapes ci-dessous utilisent la Cyber Protect console. Pour plus d'informations, voir Configuration du stockage immuable dans le guide de l'administrateur.

Pour activer le stockage immuable

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Paramètres** > **Paramètres du système**.
3. Faites défiler la liste des options de sauvegarde par défaut, puis cliquez sur **Stockage immuable**.
4. Activez le commutateur **Stockage immuable**.
5. Spécifiez une période de rétention comprise entre 14 et 3 650 jours.

   Par défaut, la période de rétention est de 14 jours. Une période de rétention plus longue augmentera l'utilisation du stockage.
6. Sélectionnez le mode de stockage immuable et, si vous y êtes invité, confirmez votre choix.
   - **Mode de gouvernance**
     Dans ce mode, toutes les sauvegardes supprimées restent dans le stockage immuable pendant la période de rétention spécifiée. Cela empêche les ransomwares ou les acteurs malveillants de manipuler ou d'effacer les données de sauvegarde et garantit l'intégrité des sauvegardes, ce qui est essentiel pour une reprise d'activité après sinistre fiable.

     Dans ce mode, vous pouvez changer la période de rétention ou passer en mode Conformité. Le stockage immuable ne peut être désactivé qu'en contactant l'équipe de Support.
   - **Mode de conformité**

     En plus des avantages du mode Gouvernance, le mode Conformité aide les organisations à répondre aux exigences réglementaires en matière de rétention des données et de sécurité en empêchant les modifications de la stratégie de rétention, y compris le changement de la période de rétention ou sa désactivation.

     Important
     La sélection du mode Conformité est irréversible. Après avoir sélectionné ce mode, vous ne pouvez pas changer la période de rétention ou revenir au mode Gouvernance. Le stockage immuable ne peut pas être désactivé dans ce mode.
7. Cliquez sur **Enregistrer**.

© Acronis International GmbH, 2003-2026

8. Pour ajouter une archive existante au stockage non modifiable, créez une nouvelle sauvegarde dans cette archive en exécutant le plan de protection correspondant manuellement ou sur un calendrier.

Remarque
Si vous supprimez une sauvegarde avant d'ajouter l'archive au stockage immuable, elle est supprimée définitivement.

Désactivation du stockage immuable

Avertissement !
Nous déconseillons fortement de désactiver le stockage immuable :

- Le stockage immuable est la dernière ligne de défense contre la suppression accidentelle ou malveillante des sauvegardes.
- La protection contre les ransomwares seule ne suffit pas—l'immuabilité garantit la récupérabilité même si les identifiants sont compromis.
- L'impact sur les coûts est prévisible et limité, tandis que le risque de perte de données sans immuabilité est élevé et imprévisible.
- Les bonnes pratiques de l'industrie et les exigences d'assurance imposent de plus en plus des sauvegardes immuables.
- Désactiver l'immuabilité expose votre organisation à des violations d'accord de niveau de service (SLA), des risques de conformité et des dommages à la réputation.

Important
Le stockage immuable peut être désactivé uniquement en mode Gouvernance et uniquement par l'équipe de support.

Après que le stockage immuable est désactivé, toutes les sauvegardes que vous supprimez seront définitivement supprimées. Les sauvegardes déjà stockées dans le stockage immuable resteront disponibles pendant jusqu'à 14 jours (336 heures), ou jusqu'à la fin de leur période de rétention, selon la première éventualité.

Par exemple :

Il y a deux sauvegardes supprimées dans le stockage immuable :

- Sauvegarde A avec une période de rétention de 7 jours.
- Sauvegarde B avec une période de rétention de 1 an.

Le stockage immuable est désactivé.

- Si vous supprimez une sauvegarde maintenant, elle est définitivement supprimée.
- Le jour 7, la Sauvegarde A est définitivement supprimée (selon sa période de rétention originale).

© Acronis International GmbH, 2003-2026

- Le jour 14, la Sauvegarde B est définitivement supprimée (selon la période de grâce du stockage immuable, car la période de rétention originale dépasse 14 jours).

Accès aux sauvegardes supprimées dans le stockage immuable

Pendant la période de rétention, vous pouvez accéder aux sauvegardes supprimées stockées dans le stockage immuable et restaurer les données qu'elles contiennent.

Une sauvegarde supprimée peut faire partie d'une archive supprimée ou d'une archive non supprimée.

Remarque
Pour permettre l'accès aux sauvegardes supprimées, le port 40440 sur le stockage des sauvegardes doit être activé pour les connexions entrantes.

Pour accéder à une sauvegarde supprimée

Dans une archive supprimée

1. Dans l'onglet **Stockage de sauvegarde**, sélectionnez le stockage dans le cloud qui contient la sauvegarde supprimée.
2. Pour voir les archives supprimées, cliquez sur **Afficher les éléments supprimés**.
3. Sélectionnez l'archive qui contient la sauvegarde que vous souhaitez restaurer.
4. Cliquez sur **Afficher les sauvegardes**.
5. Sélectionnez la sauvegarde que vous voulez restaurer.
6. Effectuez l'opération de restauration décrite dans "Restauration" (p. 664).

Dans une archive non supprimée

1. Dans l'onglet **Stockage de sauvegarde**, sélectionnez le stockage dans le cloud qui contient la sauvegarde supprimée.
2. Sélectionnez l'archive qui contient la sauvegarde que vous souhaitez restaurer.
3. Cliquez sur **Afficher les sauvegardes**, puis sur **Afficher les éléments supprimés**.
4. Sélectionnez la sauvegarde que vous voulez restaurer.
5. Effectuez l'opération de restauration décrite dans "Restauration" (p. 664).

Affichage de l'utilisation du stockage immuable

Vous pouvez voir combien d'espace de stockage immuable est utilisé dans la console Cyber Protect.

Limites

- La valeur indiquée comprend la taille totale de toutes les sauvegardes supprimées, ainsi que les métadonnées des archives de sauvegarde dans le stockage. Les métadonnées peuvent représenter jusqu'à 10 % de la valeur indiquée.

© Acronis International GmbH, 2003-2026

- La valeur affiche les données d'utilisation d'il y a jusqu'à 24 heures.
- Si l'utilisation réelle est inférieure à 0,01 Go, elle est affichée sous la forme 0,0 Go.

Pour afficher l'utilisation du stockage immuable

Dans la console Cyber Protect

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Stockage des sauvegardes** > **Sauvegardes**, puis sélectionnez un emplacement de stockage dans le cloud qui prend en charge le stockage immuable.
3. Vérifiez la colonne **Stockage immuable et métadonnées**.

Stockage géoredondant

Avec le stockage géoredondant, vos données sauvegardées sont copiées de manière asynchrone dans un emplacement de réplication éloigné géographiquement de l'emplacement de sauvegarde principal. De cette manière, les données restent durables et accessibles, même si l'emplacement principal devient indisponible.

Les données répliquées occupent la même quantité d'espace de stockage que les données d'origine.

Limites

- Le stockage géoredondant peut ne pas être disponible dans tous les centres de données.
- La géoredondance est prise en charge uniquement avec le stockage dans le cloud. Elle n'est pas prise en charge avec des stockages tiers tels que des stockages hébergés par des partenaires ou des stockages dans le cloud public.
- L'emplacement des données répliquées dépend de votre centre de données. Pour plus d'informations, consultez cet article de la base de connaissances.
- Des limitations supplémentaires s'appliquent lorsque vous utilisez le stockage géoredondant avec Disaster Recovery.

  Pour plus d'informations, voir "Limites d'utilisation du stockage géoredondant dans le cloud" (p. 1021).

Activation du stockage géoredondant

Prérequis

- Un stockage qui prend en charge la géoredondance est affecté au tenant du client.
- Un stockage géoredondant est provisionné pour le tenant du client dans le portail de gestion.

  Le stockage géoredondant ne peut pas être provisionné si un stockage non compatible est affecté (par exemple, un stockage hébergé par un partenaire).

© Acronis International GmbH, 2003-2026

Vous pouvez activer le stockage géoredondant dans l'écran principal de la console Cyber Protect ou dans l'onglet **Paramètres**. Le résultat des deux procédures est le même.

Pour activer le stockage géoredondant

Dans l'écran principal

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
   Un message d'avertissement apparaît en haut de la console Cyber Protect.
2. Dans le message d'avertissement, cliquez sur **Activer le stockage dans le cloud géoredondant**.
3. Pour confirmer que vous avez bien compris les emplacements et les frais de réplication, cochez la case.
4. Pour confirmer votre choix, cliquez sur **Activer**.

Le stockage géoredondant est activé et les données sauvegardées seront copiées dans l'emplacement de réplication.

Dans l'onglet Paramètres

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Réglages** > **Paramètres du système**.
3. Fermez la liste des options de sauvegarde par défaut, puis cliquez sur **Stockage dans le cloud géoredondant**.
4. Activez le commutateur **Stockage dans le cloud géoredondant**.
5. Cliquez sur **Enregistrer**.
6. Pour confirmer que vous avez bien compris les emplacements et les frais de réplication, cochez la case.
7. Pour confirmer votre choix, cliquez sur **Activer**.

Le stockage géoredondant est activé et les données sauvegardées seront copiées dans l'emplacement de réplication.

Désactivation du stockage géoredondant

Vous pouvez désactiver le stockage géoredondant dans la console Cyber Protect.

Pour désactiver le stockage géoredondant

1. Connectez-vous à la console Cyber Protect en tant qu'administrateur.
2. Accédez à **Réglages** > **Paramètres du système**.
3. Fermez la liste des options de sauvegarde par défaut, puis cliquez sur **Stockage dans le cloud géoredondant**.
4. Désactivez le commutateur **Stockage dans le cloud géoredondant**.

© Acronis International GmbH, 2003-2026

5. Cliquez sur **Enregistrer**.
6. Pour confirmer votre choix, saisissez **Désactiver**, puis cliquez sur **Désactiver**.

   Le stockage géoredondant est désactivé. Les données répliquées seront supprimées dans un délai d'un jour.

Affichage du statut de la géoréplication

Le statut de la géoréplication indique si les données de l'emplacement de sauvegarde principal est copié vers l'emplacement de réplication.

Les statuts suivants sont possibles :

- **Synchronisé** : les données ont été copiées dans l'emplacement de réplication.
- **Synchronisation** : les données sont en cours de copie dans l'emplacement de réplication. La durée de cette opération dépend du volume des données.
- **En attente** : la réplication des données est suspendue temporairement.
- **Désactivé** : la réplication des données est désactivée.

Pour vérifier le statut de validation

1. Connectez-vous à la console Cyber Protect.
2. Dans l'onglet **Stockage de sauvegarde**, sélectionnez l'emplacement de sauvegarde, puis l'archive de sauvegardes.
3. Cliquez sur **Détails**, puis sur le statut dans la section **Statut de géoréplication**.

Stockage d'archives

Le stockage d’archive est un stockage d’objets sécurisé, évolutif et rentable pour la rétention de données à long terme. Vous pouvez l’utiliser pour des données qui doivent répondre aux exigences de conformité ou pour des données qui sont rarement consultées, mais qui doivent être conservées.

Remarque
Vous ne pouvez pas utiliser le stockage d’archive comme destination de sauvegarde dans un plan de protection ou un plan de sauvegarde cloud à cloud.

Pour utiliser le stockage d’archive, vous devez créer un ou plusieurs compartiments dans la console Cyber Protect. Pour accéder aux compartiments, visualiser et gérer leur contenu, ou transférer des données, vous devez utiliser un client compatible S3.

Le stockage d’archive nécessite que le quota de **Stockage d’archives** soit activé dans Portail de gestion.

© Acronis International GmbH, 2003-2026

Fonctionnalités compatibles avec S3

Le stockage d'archive est compatible avec S3 et supporte les fonctionnalités standard de S3.

Versions

Vous pouvez activer la gestion des versions au niveau du compartiment :

- Dans un compartiment versionné, plusieurs versions d'un objet peuvent exister. Une nouvelle version est créée lorsqu'un objet est transféré, écrasé ou supprimé. Par exemple, lorsqu'un objet est supprimé, il n'est pas physiquement retiré du stockage. Au lieu de cela, un marqueur de suppression est ajouté à la version actuelle de l'objet, et la version précédente reste accessible.
- Dans un compartiment non versionné, chaque objet n'a qu'une seule version à la fois. Les écrasements et les suppressions sont permanents.

La versionnage empêche la suppression accidentelle ou malveillante, ou l'écrasement d'objets, mais cela entraîne une augmentation de l'espace de stockage. Pour réduire un compartiment versionné, vous pouvez utiliser une stratégie de cycle de vie.

La versionnage est automatiquement activée lorsque vous activez le verrouillage d'objet.

Mode d'accès

Dans le stockage d'archive, vous pouvez contrôler l'accès aux données et la sécurité en configurant les compartiments comme publics ou privés.

- Le mode public rend un compartiment et son contenu accessibles à toute personne disposant de l'URL correcte.
  Vous pouvez utiliser ce mode pour partager des fichiers non sensibles.
- Le mode privé restreint l'accès au compartiment aux utilisateurs autorisés.
  Vous pouvez utiliser ce mode pour les données sensibles ou critiques pour l'entreprise.

Verrouillage d'objet

Le verrouillage d'objet permet des capacités Write-Once Read-Many (WORM) pour les compartiments. Avec cela, vous pouvez configurer un compartiment où les données peuvent être écrites et lues, mais ne peuvent pas être supprimées ou écrasées.

Le verrouillage d'objet est uniquement disponible pour les compartiments versionnés.

Vous pouvez configurer le paramètre de verrouillage d'objet uniquement lors de la création d'un compartiment, et il ne peut pas être modifié par la suite.

Pour atteindre l'immuabilité de l'objet, vous devez ajouter une stratégie de rétention (mode de rétention et période de rétention) aux capacités de verrouillage d'objet. Dans la console Cyber Protect, vous pouvez configurer une stratégie de rétention au niveau du compartiment, de sorte que tous les objets dans ce compartiment utilisent le même mode et la même période de rétention.

© Acronis International GmbH, 2003-2026

Configurer une stratégie de rétention au niveau du compartiment est facultatif. Par exemple, vous pouvez créer un compartiment avec verrouillage d'objet et sans stratégie de rétention. Dans ce cas, assurez-vous que l'immuabilité de l'objet est configurée au niveau de l'objet.

Stratégie de rétention

Une stratégie de rétention assure l'immuabilité des objets en empêchant la suppression des versions d'objets pendant une période spécifiée. Cette fonctionnalité est couramment utilisée pour répondre aux exigences de conformité réglementaire ou pour protéger les données critiques contre une suppression accidentelle ou non autorisée.

Dans la console Cyber Protect, vous pouvez configurer une stratégie de rétention au niveau du compartiment. La stratégie s'applique à tous les objets placés dans le compartiment.

Vous pouvez configurer une stratégie de rétention lors de la création du compartiment ou plus tard, lorsque vous modifiez un compartiment.

Remarque
Configurer une stratégie de rétention nécessite que le verrouillage des objets soit activé pour le compartiment.

Une stratégie de rétention se compose des éléments suivants :

- Période de rétention
- Mode de rétention

Une période de rétention a une durée fixe comprise entre 1 jour et 100 ans, pendant laquelle une version d'objet reste verrouillée. Lorsque cette période se termine, la version de l'objet peut être supprimée.

La période de rétention s'applique aux versions individuelles des objets. C'est-à-dire que différentes versions du même objet peuvent avoir des durées de rétention différentes.

Par exemple :

- Vous configurez une période de rétention de 10 jours pour un compartiment et transférez l'objet X dans celui-ci. Cette version de l'objet X ne peut pas être supprimée pendant 10 jours.
- Le jour suivant, vous changez la période de rétention à 20 jours et transférez à nouveau l'objet X. La nouvelle version de l'objet X ne peut pas être supprimée pendant 20 jours, tandis que la version initiale reste verrouillée pour sa période de rétention initiale de 10 jours.

Cyber Protect supporte les modes de rétention suivants :

- Mode de gouvernance : Les versions d'objets sont protégées contre la suppression ou la modification par la plupart des utilisateurs. Cependant, les utilisateurs avec des autorisations spéciales peuvent outrepasser les paramètres de rétention, si nécessaire. Par exemple, vous pouvez demander l'assistance de l'équipe de support pour supprimer un objet. Ce mode est utile pour tester les stratégies de rétention avant de les appliquer en mode conformité.

© Acronis International GmbH, 2003-2026

- Mode de conformité : Les versions d'objets ne peuvent pas être supprimées ou écrasées par un utilisateur, y compris les administrateurs. Le mode de rétention ne peut pas être modifié, et la période de rétention ne peut pas être raccourcie. Ce mode est utilisé pour appliquer une stricte conformité réglementaire.

Stratégie de cycle de vie

Une stratégie de cycle de vie supprime automatiquement les objets dont vous n'avez plus besoin.

Vous pouvez configurer une stratégie de cycle de vie au niveau du compartiment pour les types d'objets suivants :

- Versions actuelles des objets

  Dans un compartiment versionné, la version actuelle de l'objet est marquée comme supprimée après la période spécifiée. Les versions précédentes (non actuelles) restent disponibles.

  Dans un compartiment non versionné, l'objet est définitivement supprimé après la période spécifiée.
- Versions non actuelles des objets

  Après la période spécifiée, ces versions sont définitivement supprimées. Cette option permet une gestion efficace de l'espace de stockage utilisé.

Remarque
Les stratégies de cycle de vie ne peuvent pas remplacer les stratégies de rétention. Si un objet est protégé par une période de rétention, il ne peut pas être supprimé avant l'expiration de cette période. Cependant, vous pouvez configurer une stratégie de cycle de vie avec une durée plus longue que la période de rétention, garantissant que les objets sont automatiquement supprimés après qu'ils ne sont plus protégés.

Gestion des compartiments dans le stockage d'archive

Vous pouvez gérer vos compartiments dans la console Cyber Protect.

Génération d'une paire de clés d'accès

Une paire de clés d'accès est utilisée pour authentifier les applications tierces qui peuvent accéder au stockage d'archive. Par exemple, vous avez besoin d'une paire de clés pour configurer un client compatible S3. Pour plus d'informations, voir "Accéder au stockage d'archive via des clients tiers" (p. 1631).

Une paire de clés d'accès se compose des composants suivants :

- Identifiant de la clé d'accès
- Clé d'accès secrète

Vous ne pouvez utiliser la paire de clés d'accès qu'avec une URL de terminal spécifique. Par exemple : `s3-us-central-2.acronis.storage`. Cette URL dépend de l'emplacement du centre de données pour votre compte, et vous ne pouvez pas la modifier.

© Acronis International GmbH, 2003-2026

Pour générer une paire de clés d'accès

Paire initiale

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Cliquez sur **Générer une paire de clés d'accès**.

   Important
   Vous pouvez voir, copier ou télécharger l'identifiant de la clé d'accès, la clé d'accès secrète et l'URL du terminal uniquement lorsque vous générez la paire de clés d'accès. Si vous perdez ou oubliez ces données, vous ne pouvez pas les récupérer, et vous devez générer une nouvelle paire de clés.

3. Cochez la case **Je comprends et j'accepte**.
4. Cliquez sur **Générer**.
5. Copiez la paire de clés d'accès et l'URL du terminal ou téléchargez-les sous forme de fichier CSV, puis cliquez sur **Fermer**.
   Assurez-vous de stocker ces données en toute sécurité.

Nouvelle paire

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Cliquez sur **Générer une nouvelle paire de clés d'accès**.

   Important
   Vous pouvez voir, copier ou télécharger l'identifiant de clé d'accès, la clé d'accès secrète et l'URL du terminal uniquement lorsque vous générez la paire de clés d'accès. Si vous perdez ou oubliez ces données, vous ne pouvez pas les récupérer et vous devez générer une nouvelle paire de clés.
   Générer une nouvelle paire de clés désactive automatiquement la précédente.

3. Cochez la case **Je comprends et j'accepte**.
4. Cliquez sur **Générer**.
5. Copiez la paire de clés d'accès et l'URL du terminal ou téléchargez-les sous forme de fichier CSV, puis cliquez sur **Fermer**.
   Assurez-vous de stocker ces données en toute sécurité.

Création de compartiments

Vous pouvez créer des compartiments dans la console Cyber Protect.

Prérequis

- Vous avez une paire de clés d'accès. Voir "Génération d'une paire de clés d'accès" (p. 1627).

Pour créer un compartiment

© Acronis International GmbH, 2003-2026

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Cliquez sur **Ajouter un compartiment**.
3. Spécifiez le nom du compartiment.

   Le nom du compartiment doit être globalement unique. Il doit contenir entre 3 et 63 caractères, et peut inclure des lettres minuscules (a-z de l'alphabet anglais), des chiffres (0–9), des tirets et des points. Il ne peut pas commencer par un tiret ou un point. Si le nom ne répond pas à ces exigences, le bouton **Ajouter** sur cet écran est désactivé.
4. Sous **Mode d'accès**, sélectionnez **Public** ou **Privé**.

   Pour plus d'informations, voir "Mode d'accès" (p. 1625).

   Vous pouvez changer le mode d'accès plus tard, en modifiant les propriétés du compartiment.
5. Sous **Versionnage**, sélectionnez **Activer** ou **Désactiver**.

   Pour plus d'informations, voir "Versions" (p. 1625).

   Si vous créez un compartiment non versionné, vous pouvez activer le versionnage à tout moment.

   Si vous créez un compartiment versionné, vous ne pouvez pas désactiver le versionnage, mais vous pouvez le suspendre. Si vous suspendez le versionnage, les versions d'objet existantes restent intactes. Cependant, les nouveaux objets transférés ne seront pas versionnés, et la suppression d'un objet ne créera pas une nouvelle version. En conséquence, vous ne pourrez pas restaurer les objets supprimés en utilisant l'historique des versions.
6. Sous **Verrouillage d'objet**, sélectionnez **Activer** ou **Désactiver**.

   Vous ne pouvez pas modifier ce paramètre plus tard.

   Le verrouillage d'objet est uniquement disponible pour les compartiments versionnés. Pour plus d'informations, voir "Verrouillage d'objet" (p. 1625).

   Le verrouillage d'objet est une condition préalable pour une stratégie de rétention. Pour plus d'informations, voir "Configurer une stratégie de rétention" (p. 1630).
7. Cliquez sur **Ajouter**.

En conséquence, un compartiment vide est créé. Pour transférer et gérer des objets dans le compartiment, connectez-vous au stockage via un client tiers. Pour plus d'informations, voir "Accéder au stockage d'archive via des clients tiers" (p. 1631).

Visualisation des compartiments

Vous pouvez visualiser tous les compartiments que vous avez créés dans la console Cyber Protect.

Prérequis

- Vous avez une paire de clés d'accès. Voir "Génération d'une paire de clés d'accès" (p. 1627).

Pour visualiser vos compartiments

1. Connectez-vous à la console Cyber Protect.
2. Allez à **Stockage de sauvegardes** > **Stockage d'archives**.

© Acronis International GmbH, 2003-2026

Édition des compartiments

Vous pouvez éditer un compartiment pour modifier les propriétés suivantes :

- Mode d'accès
- [Uniquement pour les compartiments versionnés où le verrouillage des objets est activé] Stratégie de rétention
- Stratégie de cycle de vie

Changer le mode d'accès

Vous pouvez changer le mode d'accès pour un compartiment. Pour plus d'informations, voir "Mode d'accès" (p. 1625).

Pour changer le mode d'accès

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Cliquez sur le compartiment que vous souhaitez modifier.
3. Dans l'onglet **Compartiment**, sélectionnez le mode d'accès.
4. Cliquez sur **Enregistrer**.

Configurer une stratégie de rétention

Dans les compartiments où le verrouillage des objets est activé, vous pouvez configurer une stratégie de rétention. Pour plus d'informations, voir "Stratégie de rétention" (p. 1626).

Pour configurer une stratégie de rétention

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Cliquez sur le compartiment que vous souhaitez modifier.
3. Dans l'onglet **Verrouillage d'objet**, activez l'interrupteur **Rétention**.
4. Dans **Mode de rétention**, sélectionnez le mode.

   Avertissement !
   En mode de conformité, les objets ne peuvent pas être supprimés pendant leur période de rétention par un utilisateur, y compris les administrateurs.

5. Dans **Période de rétention**, spécifiez la période en jours ou en années.
   Vous pouvez spécifier une période comprise entre 1 jour et 100 ans.
6. Cliquez sur **Enregistrer**.

Configurer une stratégie de cycle de vie

Pour supprimer automatiquement les fichiers inutiles, vous pouvez configurer une stratégie de cycle de vie au niveau du compartiment. Pour plus d'informations, voir "Stratégie de cycle de vie" (p.

© Acronis International GmbH, 2003-2026

1627).

Pour configurer une stratégie de cycle de vie

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Cliquez sur le compartiment que vous souhaitez modifier.
3. Dans l'onglet **Cycle de vie**, activez l'interrupteur **Cycle de vie**.
4. [Pour les compartiments versionnés] Sélectionnez les versions auxquelles vous souhaitez appliquer la stratégie de cycle de vie.
5. Configurez la période après laquelle la stratégie de cycle de vie sera appliquée aux objets dans le compartiment.

   Remarque
   Une stratégie de cycle de vie ne sera pas appliquée aux objets en rétention. Configurez une période de cycle de vie qui est plus longue que la période de rétention pour les objets que vous souhaitez supprimer.

6. Cliquez sur **Enregistrer**.

Suppression des compartiments

Vous pouvez supprimer des compartiments dans la console Cyber Protect.

Prérequis

- Le compartiment est vide.

Remarque
Vous ne pouvez pas supprimer un objet du compartiment tant que la période de rétention pour cet objet n'est pas expirée.

Pour supprimer des compartiments

1. Dans la console Cyber Protect, accédez à **Stockage de sauvegarde** > **Stockage d'archives**.
2. Sélectionnez la case des compartiments que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Cochez la case pour confirmer votre choix.
5. Saisissez votre identifiant pour confirmer votre compte.
6. Cliquez sur **Supprimer**.

Accéder au stockage d'archive via des clients tiers

Vous pouvez gérer les objets dans le stockage d'archive en utilisant un client compatible S3. Les options populaires incluent :

© Acronis International GmbH, 2003-2026

- Cyberduck
- S3 Browser
- Mountain Duck
- Rclone

Avec un client compatible S3, vous pouvez effectuer les actions suivantes :

- Transférer des fichiers vers un compartiment
- Créer des dossiers dans un compartiment
- Télécharger des fichiers ou des dossiers vers le stockage local
- Supprimer des fichiers et des dossiers d'un compartiment

Remarque
Le stockage d'archive prend en charge les noms d'objets qui incluent des caractères alphanumériques et spéciaux. Vérifiez la documentation de votre client compatible S3 pour toute restriction sur le nommage des objets.

Pour accéder au stockage d'archive, vous devez fournir :

- Identifiant de la clé d'accès
- Clé d'accès secrète
- Terminal de stockage d'objets S3
  Par exemple : `s3-us-central-2.acronis.storage`
- [Si non rempli automatiquement] Port
  Le stockage d'archives prend en charge le port 443 avec TLS v1.2 ou ultérieur.

Important
L'identifiant de clé d'accès, la clé d'accès secrète et l'URL du terminal sont affichés uniquement lorsque vous créez une nouvelle paire de clés d'accès. Copiez ou téléchargez ces éléments sous forme de fichier CSV. Si vous les perdez, créez une nouvelle paire de clés et reconfigurez votre client compatible S3. Pour plus d'informations, voir "Génération d'une paire de clés d'accès" (p. 1627).

Remarque
Les clients compatibles S3 doivent utiliser des URL de type chemin. Par exemple :

```
https://s3-eu-central-1.acronis.storage/mybucket/myfolder/file.txt
```

Les URL de type hébergé virtuellement ne sont pas prises en charge. Par exemple :

```
https://mybucket.s3-eu-central-1.acronis.storage/myfolder/file.txt
```

Pour des informations détaillées sur la configuration d'un client compatible S3, voir la documentation du client.

© Acronis International GmbH, 2003-2026

Par exemple :

- Cyberduck : https://docs.cyberduck.io/cyberduck
- S3 Browser : https://s3browser.com/help.aspx
- Mountain Duck : https://docs.cyberduck.io/mountainduck
- Rclone : https://rclone.org/docs

Tableau de bord de sensibilisation

Ce tableau de bord est disponible si le fournisseur de services a activé le service de formation Sensibilisation à la sécurité.

Le tableau de bord est accessible au niveau client pour les utilisateurs ayant les rôles suivants : administrateur partenaire, administrateur client, administrateur de la protection ou cyberadministrateur.

Le tableau de bord indique l'avancement dans la formation et la sensibilisation à la sécurité en entreprise. Il permet également d'accéder à la console d'administration de la formation à la sécurité en entreprise dans Wizer.

Utilisation du service de formation et de sensibilisation à la sécurité

Pour gérer les utilisateurs et le contenu de formation disponibles pour votre organisation, cliquez sur **Console d'administration** dans l'angle supérieur gauche du tableau de bord Sensibilisation pour ouvrir la console d'administration Wizer.

Pour obtenir des instructions détaillées, consultez la documentation de Wizer.

© Acronis International GmbH, 2003-2026

OpenVPN de site à site – Informations complémentaires

Quand vous créez un serveur de restauration, vous configurez son **adresse IP dans le réseau de production** et son **adresse IP test**.

Quand vous aurez réalisé le basculement (exécuté la machine virtuelle dans le cloud), et que vous vous serez connecté à la machine virtuelle pour consulter l'adresse IP du serveur, vous verrez l'**adresse IP dans le réseau de production**.

Quand vous réalisez le basculement test, vous pouvez joindre le serveur de test uniquement en utilisant l'**adresse IP test**, visible uniquement dans la configuration du serveur de restauration.

Pour accéder à un serveur de test depuis votre site local, vous devez utiliser l'**adresse IP de test**.

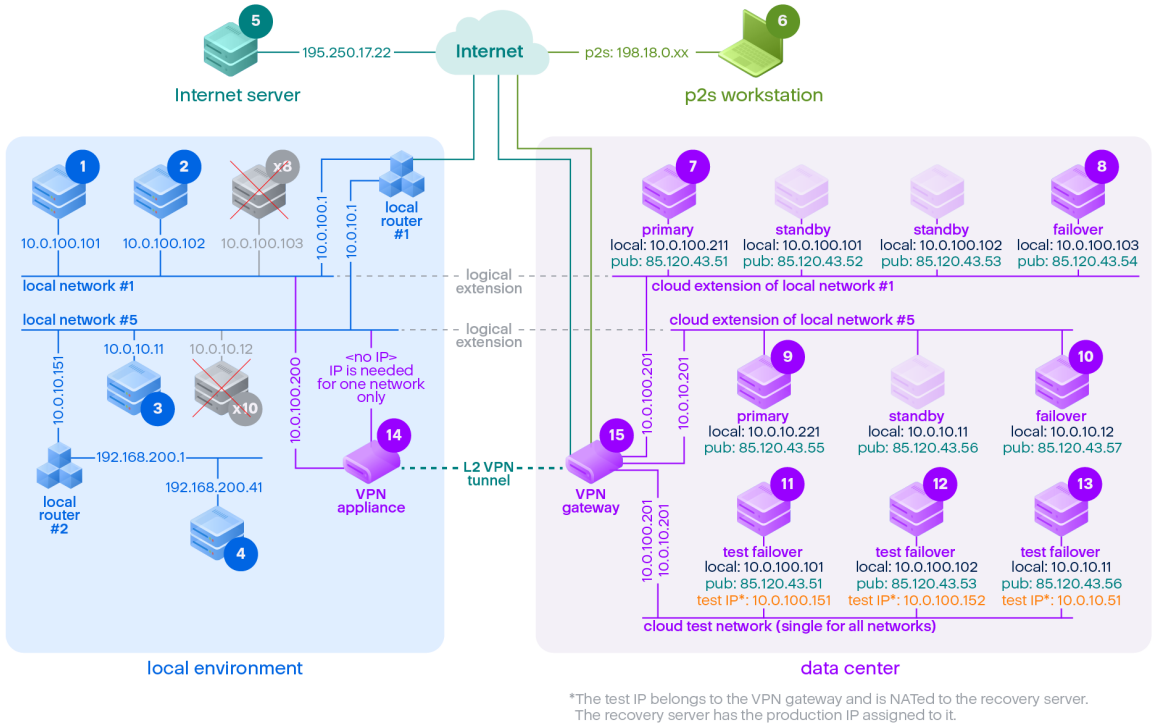
Remarque
La configuration réseau du serveur indique toujours l'**adresse IP dans le réseau de production** (car le serveur de test illustre le serveur de production). En effet, l'adresse IP test n'appartient pas au serveur de test, mais à la passerelle VPN, et elle est convertie en adresse IP de production à l'aide d'une mise en réseau partagé (NAT).

Le diagramme ci-dessous montre un exemple de configuration Open VPN de site à site. Certains serveurs de l'environnement local sont restaurés dans le Cloud au moyen du basculement (tandis que l'infrastructure réseau est OK).

1. Le client a activé Disaster Recovery :
   a. en configurant l'appliance VPN (14) et en la connectant au serveur VPN Cloud dédié (15)
   b. en protégeant certains des serveurs locaux à l'aide de Disaster Recovery (1, 2, 3, x8 et x10)
      Certains serveurs sur le site local (comme le 4) sont connectés à des réseaux qui ne sont pas connectés à l'appliance VPN. Ces serveurs ne sont pas protégés par Disaster Recovery.
2. Une partie des serveurs (connectés à des réseaux différents) fonctionne sur le site local : (1, 2, 3 et 4)
3. Les serveurs protégés (1, 2 et 3) sont testés au moyen d'un basculement test (11, 12 et 13)
4. Certains serveurs sur le site local sont indisponibles (x8, x10). Après le basculement, ils deviennent disponibles dans le Cloud (8 et 10)

© Acronis International GmbH, 2003-2026

5. Certains serveurs primaires (7 et 9), connectés à des réseaux différents, sont disponibles dans l'environnement Cloud
6. Le (5) est un serveur sur Internet avec une adresse IP publique
7. Le (6) est un poste de travail connecté au Cloud à l'aide d'une connexion VPN de point à site (p2s)



Dans cet exemple, la configuration de connexion suivante est disponible (par exemple, « ping ») depuis un serveur de la rangée **De :** vers un serveur de la colonne **À :**.

© Acronis International GmbH, 2003-2026

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
de :		locale	locale	locale	locale	internet	p2s	primaire	basculement	primaire	basculement	basculement test	basculement test	basculement test	application VPN	serveur VPN
1	locale		direct	via routeur local 1	via routeur local 2	via routeur local 1 et Internet	non	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via local routeur 1 et tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	direct	non
2	locale	direct		via routeur local 1	via routeur local 2	via routeur local 1 et Internet	non	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : local via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	via local routeur 1 et tunnel : NAT (serveur VPN) via routeur local 1 et Internet : pub	direct	non
3	locale	via routeur	via routeur		via routeur	via routeur local 1	non	via tunnel : local	via tunnel : local	via tunnel : local	via tunnel : local	via tunnel : NAT	via tunnel : NAT	via local routeur 1 et tunnel :	via routeur local	non

© Acronis International GmbH, 2003-2026

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		local 1	local 1		local 2	et Internet		via router local 1 et Internet : pub	via router local 1 et Internet : pub	via router local 1 et Internet : pub	via router local 1 et Internet : pub	(serveur VPN) via router local 1 et Internet : pub	(serveur VPN) via router local 1 et Internet : pub	NAT (serveur VPN) via router local 1 et Internet : pub		
4	locale	via router local 2 et router 1	via router local 2 et router 1	via router local 2		via router local 2, router 1 et Internet	non	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via router local 2 et tunnel : local via router local 2, router local 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 2, router 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 2, router 1 et Internet : pub	via tunnel : NAT (serveur VPN) via router local 2, router 1 et Internet : pub	via router local 2	non
5	internet	non	non	non	non		N/D	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	via Internet : pub	non	non
6	p2s	non	non	non	non	via		via	via VPN	via	via VPN	via VPN	via VPN	via VPN	non	non

© Acronis International GmbH, 2003-2026

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						Internet		VPN p2s (serveur VPN) : local via Internet : pub	p2s (serveur VPN) : local via Internet : pub	VPN p2s (serveur VPN) : local via Internet : pub	p2s (serveur VPN) : local via Internet : pub	p2s – NAT (serveur VPN) via Internet : pub	p2s – NAT (serveur VPN) via Internet : pub	p2s – NAT (serveur VPN) via Internet : pub		
7	primaire	via tunnel	via tunnel	via tunnel et router local 1	via tunnel et router local 1 et 2	via Internet (via serveur VPN)	non		direct dans le Cloud : local	via tunnel et router local 1 : local	via tunnel et router local 1 : local	via serveur VPN : NAT	via serveur VPN : NAT	via tunnel et router local 1 : NAT	non	Protocoles DHCP et DNS seulement
8	basculement	via tunnel	via tunnel	via tunnel et router local 1	via tunnel et router local 1 et 2	via Internet (via serveur VPN)	non	direct dans le Cloud : local		via tunnel et router local 1 : local	via tunnel et router local 1 : local	via serveur VPN : NAT	via serveur VPN : NAT	via tunnel et router local 1 : NAT	non	Protocoles DHCP et DNS seulement
9	primaire	via tunn	via tunn	via tunnel	via tunnel	via Intern	non	via tunnel	via tunnel et router		direct dans le	via tunnel et router	via tunnel et router	via serveur VPN : NAT	non	Protocoles

© Acronis International GmbH, 2003-2026

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		el et router local 1	el et router local 1			et (via serveur VPN)		et router local 1 : local	local 1 : local		Cloud : local	local 1 : NAT	local 1 : NAT			DHCP et DNS seulement
10	basculement	via tunnel et router local 1	via tunnel et router local 1	via tunnel	via tunnel	via Internet (via serveur VPN)	non	via tunnel et router local 1 : local	via tunnel et router local 1 : local	direct dans le Cloud : local		via tunnel et router local 1 : NAT	via tunnel et router local 1 : NAT	via serveur VPN : NAT	non	Protocoles DHCP et DNS seulement
11	basculement test	non	non	non	non	via Internet (via serveur VPN)	non	non	non	non	non		direct dans le Cloud : local	via serveur VPN : local (routage)	non	Protocoles DHCP et DNS seulement
12	basculement test	non	non	non	non	via Internet (via serveur VPN)	non	non	non	non	non	direct dans le Cloud : local		via serveur VPN : local (routage)	non	Protocoles DHCP et DNS seulement
13	basculem	non	non	non	non	via	no	non	non	non	non	via	via		non	Protocol

© Acronis International GmbH, 2003-2026

	À :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	ent test					Internet (via serveur VPN)	n					serveur VPN : local (routage)	serveur VPN : local (routage)			es DHCP et DNS seulement
14	application VPN	direct	direct	via router local 1	via router local 2	via Internet (router local 1)	non	non	non	non	non	non	non	non		non
15	serveur VPN	non	non	non	non	non	non	non	non	non	non	non	non	non	non	

© Acronis International GmbH, 2003-2026

Glossaire

A

Adresse IP publique

[Disaster Recovery] Une adresse IP nécessaire pour rendre les serveurs Cloud disponibles depuis Internet.

Adresse IP test

[Disaster Recovery] Une adresse IP nécessaire en cas de basculement test, pour éviter la duplication de l'adresse IP de production.

Agent de prévention des pertes de données

Un composant client du système de prévention des pertes de données qui protège son ordinateur hôte contre l'utilisation, la transmission et le stockage non autorisés de données confidentielles, protégées ou sensibles en appliquant une combinaison de techniques d'analyse de contexte et de contenu et en mettant en œuvre des politiques de prévention des pertes de données gérées de manière centralisée. Cyber Protection propose un agent de prévention des pertes de données complet. Toutefois, la fonctionnalité de l'agent sur un ordinateur protégé est limitée à l'ensemble de fonctionnalités de prévention des pertes de données disponibles sous licence dans Cyber Protection, et dépend du plan de protection appliqué à cet ordinateur.

Agent de protection

Un agent de protection est l'agent à installer sur les machines à des fins de protection des données.

Application VPN

[Disaster Recovery] Une machine virtuelle spéciale qui connecte le réseau local et le site dans le Cloud via un tunnel VPN sécurisé. Le matériel VPN est déployé sur le site local.

B

Basculement

Rebasculement d'une ressource d'un serveur de production vers un serveur de secours (tel qu'un réplica de machine virtuelle ou un serveur de restauration s'exécutant dans le Cloud).

Base de données des périphériques USB

[Contrôle des terminaux] Le module de contrôle des terminaux tient à jour une base de données des périphériques USB depuis laquelle ils peuvent être ajoutés à la liste des exclusions du contrôle d'accès aux terminaux. La base de données enregistre les périphériques USB par identifiants de périphérique, qui peuvent être entrés manuellement ou sélectionnés à partir des terminaux connus dans la console Cyber Protect.

C

Connexion de point à site (P2S)

[Disaster Recovery] Une connexion VPN sécurisée extérieure en utilisant vos terminaux (comme un ordinateur de bureau ou un ordinateur portable) vers le site local et dans le Cloud.

© Acronis International GmbH, 2003-2026

Connexion de site à site (S2S)

[Disaster Recovery] Connexion qui étend le réseau local au Cloud via un tunnel VPN sécurisé.

F

Finalisation

L'opération qui consiste à faire d'une machine virtuelle temporaire s'exécutant depuis une sauvegarde une machine virtuelle permanente. Physiquement, cela signifie restaurer l'ensemble des disques de la machine virtuelle, y compris les modifications effectuées lors de l'exécution de la machine, dans le magasin de données stockant ces modifications.

Format de sauvegarde sous forme d'un fichier unique

Format de sauvegarde, pour lequel les sauvegardes complètes et incrémentielles suivantes sont enregistrées sous forme d'un fichier .tibx unique. Ce format accélère la vitesse de la méthode de sauvegarde incrémentielle, tout en évitant ses principaux inconvénients et la suppression complexe de sauvegardes ayant expiré. Le logiciel définit les blocs de sauvegarde utilisés par des sauvegardes ayant expiré comme étant « libres » et y inscrit les nouvelles sauvegardes. Ce procédé permet un nettoyage extrêmement rapide et une consommation minimale des ressources. Le format de sauvegarde sous forme de fichier unique n'est pas disponible lorsque la sauvegarde est effectuée sur des emplacements qui ne prennent pas en charge les lectures et écritures en accès aléatoire.

J

Jeu de sauvegardes

Il s'agit d'un groupe de sauvegardes auquel il est possible d'appliquer une règle individuelle de rétention. Pour le modèle de sauvegarde Personnalisé, les jeux de sauvegardes correspondent aux méthodes de sauvegarde (Complète, Différentielle et Incrémentielle). Dans tous les autres cas de figure, les jeux correspondent à une sauvegarde : Mensuelle, Quotidienne, Hebdomadaire et Par heure. Une sauvegarde mensuelle correspond à la première sauvegarde créée dès qu'un mois commence. Une sauvegarde hebdomadaire correspond à la première sauvegarde créée le jour de la semaine sélectionné dans l'option Sauvegarde hebdomadaire (cliquez sur l'icône en forme d'engrenage, puis sur Options de sauvegarde > Sauvegarde hebdomadaire). Si une sauvegarde hebdomadaire correspond à la première sauvegarde créée dès qu'un mois commence, cette sauvegarde est considérée comme étant mensuelle. Dans ce cas, une sauvegarde hebdomadaire sera créée lors du jour de la semaine sélectionné. Une sauvegarde quotidienne correspond à la première sauvegarde créée dès qu'un jour commence, sauf si elle répond à la définition d'une sauvegarde mensuelle ou hebdomadaire. Une sauvegarde par heure correspond à la première sauvegarde créée dès qu'une heure commence, sauf si elle répond à la définition d'une sauvegarde mensuelle, hebdomadaire ou quotidienne.

M

Machine physique

Une machine sauvegardée par un agent installé sur le système d'exploitation.

© Acronis International GmbH, 2003-2026

Machine virtuelle

Une machine virtuelle sauvegardée au niveau de l'hyperviseur par un agent externe tel que l'agent pour VMware ou l'agent pour Hyper-V. Une machine virtuelle avec un agent interne est traitée comme une machine physique au niveau de la sauvegarde.

Module

Un module est un élément du plan de protection, fournissant une fonctionnalité de protection particulière, par exemple le module de sauvegarde, le module de protection contre les virus et les malwares, etc.

Module de contrôle des terminaux

Dans le cadre d'un plan de protection, le module de contrôle des terminaux tire parti d'un sous-ensemble fonctionnel de l'agent de prévention des pertes de données sur chaque ordinateur protégé afin de détecter et de prévenir la consultation et la transmission non autorisées de données via les canaux de l'ordinateur local. Cela comprend l'accès de l'utilisateur aux ports et périphériques, l'impression de documents, les opérations de copier-coller, le formatage des supports et les opérations d'éjection, ainsi que les synchronisations aux terminaux mobiles connectés localement. Le module de contrôle des terminaux offre un contrôle granulaire et contextuel sur les types de terminaux et de ports auxquels les utilisateurs peuvent accéder sur l'ordinateur protégé, ainsi que les actions que ces utilisateurs peuvent réaliser sur ces terminaux.

O

Objectif de point de restauration (RPO)

[Disaster Recovery] Quantité de données perdues à cause d'une panne, mesurée en termes de temps à partir d'une panne ou d'un sinistre programmés. Le seuil des objectifs de point de restauration définit l'intervalle de temps maximum autorisé entre le dernier point de restauration pour un basculement et l'heure actuelle.

P

Passerelle VPN (anciennement serveur VPN ou passerelle de connectivité)

[Disaster Recovery] Une machine virtuelle spéciale qui connecte les réseaux du site local et du site dans le Cloud via un tunnel VPN sécurisé. La passerelle VPN est déployée dans le site dans le Cloud.

Plan de protection

Un plan de protection est un plan qui combine des modules de protection des données, notamment les modules suivants : sauvegarde, protection contre les virus et les malwares, filtrage d'URL, Windows Defender Antivirus, Microsoft Security Essentials, évaluation des vulnérabilités, gestion des correctifs, carte de protection de données, contrôle des terminaux.

Prévention des pertes de données (anciennement, prévention des fuites de données)

Un système de technologies intégrées et de mesures organisationnelles destinées à détecter et à prévenir la divulgation/consultation accidentelle ou intentionnelle de données confidentielles,

© Acronis International GmbH, 2003-2026

protégées ou sensibles par des entités non autorisées, au sein ou en dehors de l'organisation, ou le transfert de telles données vers des environnements non dignes de confiance.

R

Réseau de production

[Disaster Recovery] Le réseau interne étendu au moyen d'une transmission tunnel VPN, et qui couvre aussi bien les sites locaux et dans le Cloud. Les serveurs locaux et les serveurs dans le Cloud peuvent communiquer entre eux dans le réseau de production.

Réseau de test

[Disaster Recovery] Réseau virtuel isolé, utilisé pour tester le processus de basculement.

Restauration automatique

Rebasculement d'une ressource d'un serveur de secours (tel qu'un réplica de machine virtuelle ou un serveur de restauration s'exécutant dans le Cloud) vers un serveur de production.

Runbook

[Disaster Recovery] Scénario planifié composé d'étapes configurables qui automatisent les actions de reprise d'activité après sinistre.

S

Sauvegarde complète

Sauvegarde autonome contenant toutes les données choisies pour la sauvegarde. Vous n'avez pas besoin d'accéder à une autre sauvegarde pour récupérer les données à partir d'une sauvegarde complète.

Sauvegarde différentielle

Une sauvegarde différentielle stocke les modifications apportées à des données par rapport à la dernière sauvegarde complète. Vous devez avoir accès à la sauvegarde complète correspondante pour récupérer les données à partir d'une sauvegarde différentielle.

Sauvegarde incrémentielle

Sauvegarde qui stocke les modifications apportées aux données par rapport à la dernière sauvegarde. Vous avez besoin d'accéder à d'autres sauvegardes pour récupérer les données à partir d'une sauvegarde incrémentielle.

Sauvegarde orpheline

Une sauvegarde orpheline est une sauvegarde qui n'est plus associée à un plan de protection.

Serveur Cloud

[Disaster Recovery] Référence générale vers un serveur primaire ou de restauration.

Serveur de restauration

[Disaster Recovery] Un réplica en MV de la machine d'origine, basé sur les sauvegardes de serveur protégées stockées dans le Cloud. Les serveurs de restauration sont utilisés pour remplacer les ressources depuis les serveurs originaux en cas de sinistre.

Serveur primaire

[Disaster Recovery] Une machine virtuelle qui ne possède pas de machine associée sur le site local (tel qu'un serveur de restauration). Les serveurs primaires servent à protéger une

© Acronis International GmbH, 2003-2026

application ou à exécuter divers services auxiliaires (tels qu'un service Web).

Site dans le Cloud (ou site de RAS)

[Disaster Recovery] Site distant hébergé dans le Cloud et servant à exécuter l'infrastructure de restauration, en cas de sinistre.

Site local

[Disaster Recovery] L'infrastructure locale déployée sur les locaux de l'entreprise.

V

Validation

Opération qui vérifie la possibilité de restauration de données à partir d'une sauvegarde. La validation d'une sauvegarde de fichiers imite la restauration de tous les fichiers à partir de la sauvegarde vers une destination factice. La validation d'une sauvegarde de disque calcule une somme de contrôle pour chaque bloc de données enregistré dans la sauvegarde. Les deux procédures nécessitent beaucoup de ressources. Même si une validation réussie signifie qu'il existe une forte probabilité de réussite de la restauration, elle ne vérifie pas tous les facteurs ayant une incidence sur le processus de restauration.

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Index

3

32 bits ou 64 bits ? 992

A

À propos d'Acronis Disaster Recovery 1016

À propos de la planification de sauvegarde 918

À propos de Secure Zone 563

À propos du service d'envoi de données physiques 649

Accéder à une appliance virtuelle via un client SSH 181

Accéder au stockage d'archive via des clients tiers 1631

Accès à un site Web malveillant 1199

Accès au service Cyber Protection 24

Accès aux sauvegardes supprimées dans le stockage immuable 1621

Accès VPN à distance de point à site 1052

Accès VPN au site local 1055

Action lors de la détection 1189

Actions 1590

Actions avec plans de protection 245

Actions de workflow 1231

Actions par défaut 1210

Actions supplémentaires avec la console de ligne de commande à distance 1497

Actions supplémentaires avec les chats dans Cyber Protect Monitor 376

Actions supplémentaires avec les messages de chat 1522

Actions supplémentaires avec les sessions de chat 1520

Actions supplémentaires avec plans de surveillance 1567

Activation d'une règle de rétention 793

Activation d'un workflow 1234

Activation de Data Loss Prevention dans les plans de protection 1593

Activation de la connexion de site à site 1032

Activation de la fonctionnalité EDR (Endpoint Detection and Response) 1255

Activation de la fonctionnalité XDR (Extended Detection and Response) 1243

Activation de la recherche améliorée dans les sauvegardes chiffrées 944

Activation de la restauration en un clic 641

Activation de Startup Recovery Manager 1014

Activation des services d'emplacement dans le système d'exploitation 1513

Activation du compte 21

Activation du mode compatible FIPS pour une appliance virtuelle 64

Activation du mode de surveillance pour EDR (Endpoint Detection and Response) 1339

Activation du stockage géoredondant 1622

Activation du stockage immuable 1619

Activation et désactivation de la gestion du pare-feu 1212

Activation ou désactivation d'un plan de protection 250

Activation ou désactivation de l'analyse de l'inventaire logiciel 1386

© Acronis International GmbH, 2003-2026

Activation ou désactivation de l'analyse de l'inventaire matériel 1380

Activation ou désactivation de la correction automatique des écarts par rapport aux références 1367

Activation ou désactivation des notifications de chat dans Cyber Protect Monitor 377

Active Protection 29, 1167, 1170

Active Protection dans l'édition Cyber Backup Standard 1188

Activer l'utilisation du module de contrôle de terminaux sur macOS 452

Activer la sauvegarde complète VSS 661

Activer ou désactiver le contrôle des terminaux 451

Activer ou désactiver les notifications du système d'exploitation et les alertes de service 455

Administration d'organisations Microsoft 365 organisations ajoutées à différents niveaux 854

Adresses IP publique et de test 1057

Adresses IP publiques 1122

Advanced 1211

Affectation d'identifiants à une ressource 1482

Affectation des workflows 1235

Affecter des sessions de chat à vous-même 1517

Affectés récemment 357

Affichage de l'emplacement d'un terminal 1513

Affichage de l'état de la sauvegarde dans vSphere Client 976

Affichage de l'état de protection d'une ressource Microsoft 365 par service 860

Affichage de l'historique d'exécution 1110

Affichage de l'inventaire du logiciel d'un seul terminal 1389

Affichage de l'utilisation du stockage immuable 1621

Affichage de la liste des correctifs disponibles 1409

Affichage des activités d'archivage des e-mails 773

Affichage des alertes d'archivage des e-mails 773

Affichage des archives de sauvegarde contenant des données d'investigation numérique 631

Affichage des correctifs au niveau du partenaire 1423

Affichage des détails d'un goulot d'étranglement 742

Affichage des détails sur les serveurs cloud 1076

Affichage des erreurs d'intégration XDR 1249

Affichage des incidents non atténués 1262

Affichage des informations sur les terminaux découverts 195

Affichage des ressources gérées par les intégrations RMM 478

Affichage des vulnérabilités au niveau du partenaire 1422

Affichage des workflows actuels 1226

Affichage du journal des alertes de surveillance 1579

Affichage du matériel d'un seul terminal 1384

Affichage du résultat de la distribution 973

Affichage du statut de la géoréplication 1624

© Acronis International GmbH, 2003-2026

Affichage du statut du basculement test automatisé 1086, 1138

Affichage et compréhension des résultats de requête 1269

Affichage et mise à jour d'un agent pour Azure déployé 165

Affichage et mise à jour des emplacements de sauvegarde dans le cloud public 756

Afficher les alertes de contrôle des terminaux 458

Afficher les détails à propos des éléments de la liste blanche 1217

Agent pour Azure 523

Agent pour empêcher les pertes de données 516

Agent pour Exchange (pour la sauvegarde de boîte aux lettres) 517

Agent pour File Sync & Share 517

Agent pour Hyper-V 522

Agent pour Linux 518

Agent pour Mac 520

Agent pour Microsoft 365 518

Agent pour MySQL/MariaDB 518

Agent pour Nutanix 523

Agent pour Office 365 installé localement 912

Agent pour Oracle 518

Agent pour oVirt 523

Agent pour oVirt - Rôles et ports requis 162

Agent pour Scale Computing HC3 523

Agent pour Scale Computing HC3 – Rôles requis 145

Agent pour SQL, agent pour Active Directory, agent pour Exchange (pour la sauvegarde de bases de données et la sauvegarde reconnaissant les applications) 516

Agent pour Synology 523

Agent pour Virtuozzo 522

Agent pour Virtuozzo Hybrid Infrastructure 523

Agent pour VMware - Sauvegarde sans réseau local 967

Agent pour VMware (appliance virtuelle) 521

Agent pour VMware (Windows) 521

Agent pour Windows 513

Agent pour Windows (hérité) 514

Agents dans Microsoft Azure 1159

Aide-mémoire pour la sauvegarde 549

Ajout automatique à la liste blanche 1216

Ajout d'identifiants 1482

Ajout d'un accès à une connexion au cloud public 766

Ajout d'un réseau de restauration de production à partir de Microsoft Azure 1125

Ajout d'un réseau de restauration de test à partir de Microsoft Azure 1125

Ajout d'un serveur de messagerie 772

Ajout d'une organisation Microsoft 365 853, 912

Ajout d'une ressource à un plan de déploiement de logiciel 1455

Ajout d'une ressource à un plan de gestion à distance 1477

Ajout de fichiers mis en quarantaine à la liste blanche 1216

Ajout de l'accès à un abonnement Microsoft Azure 762

© Acronis International GmbH, 2003-2026

Ajout de la variable AR_RETENTION_LOCK_SUPPORT 538

Ajout de packages logiciels à partir de la bibliothèque 1433

Ajout de plusieurs terminaux 184

Ajout de ressources à des plans de surveillance 1563

Ajout de ressources à la console Cyber Protect 398

Ajout de ressources à un groupe statique 423

Ajout de VLAN 1007

Ajout manuel à la liste blanche 1216

Ajout ou suppression de colonnes dans la vue de disposition en tableau 1270

Ajouter des références aux modèles 1371

Ajouter ou supprimer le terminal USB de la base de données 456

Ajouter ou supprimer un processus, un fichier ou un réseau dans la liste de blocage ou la liste d'autorisation du plan de protection 1331

Ajouter une organisation Google Workspace 919

Ajouter une règle de conservation légale 797

Ajustement des autorisations dans les règles de flux de données 1588

Alertes 606

Alertes de connexion au cloud public 333

Alertes de contrôle des terminaux 329, 473

Alertes de déploiement logiciel 336

Alertes de filtrage 303

Alertes de filtrage d'URL 325

Alertes de licence 326

Alertes de protection antimalware 320

Alertes de reprise d'activité après sinistre 310

Alertes de sauvegarde 306

Alertes de surveillance 1571

Alertes du serveur dans le cloud 1162

Alertes EDR 328

Alertes relatives à l'état de santé du disque 350

Alertes système 330

Algorithme de distribution 972

Amorçage d'un réplica initial 966

Analyse antimalware des boîtes aux lettres 869

Analyse antimalware des sauvegardes 1217

Analyse planifiée 1169

Analyser les détails de l'incident 1265

Annulation de l'affectation d'identifiants d'une ressource 1483

Annuler la suppression d'e-mails dans le stockage immuable 802

Antivirus Microsoft Defender 1208

Antivirus Microsoft Defender et Microsoft Security Essentials 1208

Application d'un plan à un groupe 446

Application d'un plan de protection à une ressource 246

Application d'un plan de sauvegarde 906

Application des mesures d'intervention 1248

Application potentiellement indésirable 1187

Application VPN 1032

Applications dans le Cloud 358

Approbation automatique des correctifs 1412

Approbation manuelle des correctifs 1417

Archivage d'e-mails 771

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Archivage des e-mails dans des tenants désactivés ou supprimés 774

Arguments de commande 1437

Arrêt d'un basculement 1091

Arrêt de l'exécution d'un runbook 1109

Arrêt du basculement 964

Association de ressources à des utilisateurs spécifiques 481

Attacher des bases de données SQL Server 828

Attendre que les conditions de la planification soient remplies 659

Atténuation d'incidents 1304

Atténuer l'intégralité d'un incident 1305

Atténuer un incident faux positif 1309

Attribution des autorisations système requises à Agent Connect 57

Aucune sauvegarde réussie sur plusieurs jours d'affilée 606

Authentification à deux facteurs 21

Autoprotection 1173, 1189

Autorisations 1589

Autorisations de politiques 759

Autorisations de stratégies 758

Autorisations nécessaires à l'installation sans assistance sous macOS 101

Autoriser le trafic DHCP via un VPN de couche 2 1039

Autres actions pouvant être effectuées dans le cadre de plans de gestion à distance existants 1478

Autres outils Cyber Protection 1615

Avant de commencer 37, 138, 141, 145, 157, 163, 167, 171

Azure Bastion 1122

Azure ExpressRoute 1122

Azure VPN site à site 1122

B

Basculement dans Microsoft Azure 1131

Basculement de la production 1087, 1131

Basculement pour Disaster Recovery 1324

Basculement sur un réplica 964

Basculement test 1083, 1132

Basculement test automatisé 1085, 1132, 1160

Basculement test automatisé dans Microsoft Azure 1136

Basculement test dans Microsoft Azure 1133

Base de données des périphériques USB 467

Basé sur Linux 990

Basé sur WinPE/WinRE 990

Bibliothèque 1429

Bonnes pratiques pour la Disaster Recovery configuration réseau 1123

Bootable Media Builder 992

C

calculer le hachage 636

Capture des paquets réseau 1066

Caractères génériques 622

Carte de l'organisation 1610

Carte de la protection des données 367

Cas d'utilisation d'approbation automatique des correctifs sans test 1417

Cas d'utilisation de l'approbation et du test automatiques des correctifs 1413

Catégories à filtrer 1199

Catégories personnalisées de sensibilité 1606

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Ce qu'un réplica vous permet de faire 962

Ce que vous devez savoir 841

Ce que vous devez savoir à propos de la conversion 269

Ce que vous devez savoir à propos de la finalisation 960

Ce que vous pouvez sauvegarder 840

Champ d'application de la protection 1221

Champs d'événements 1278

Changer le compte de connexion sur les machines Windows 66

Changer le mode d'accès 1630

Chat d'assistance 1515

Chats dans Monitor 375

Chemin de désinstallation 1437

Chiffrement 596

Chiffrement de lecteur BitLocker Microsoft 546

Citrix Hypervisor/XenServer 533

Classes de stockage prises en charge 758

Clés d'accès 759, 761

Clonage d'un script 499

Clonage d'un workflow 1236

Clonage d'une version de workflow 1240

Clouds publics 529

Codec adaptatif 1464

Collecte automatique de données de performances 212

Collecte des informations système 215

Combien d'agents sont nécessaires pour la sauvegarde et la restauration de données de cluster ? 811

Combien d'agents sont nécessaires pour la sauvegarde et la restauration prenant en charge les clusters ? 813

Combien d'appliances virtuelles me faut-il ? 168

Combinaison de règles de flux de données 1589

Commande après la capture de données 655

Commande après la restauration 729

Commande après la sauvegarde 653

Commande avant la capture de données 654

Commande avant la restauration 728

Commandes avant la sauvegarde 651

Commandes d'installation 1437

Commandes de capture de données Pré/Post 653

Commandes de désinstallation 1437

Commandes et arguments d'installation et de désinstallation 1436

Commandes Pré/Post 651, 728, 966

Comment analyser les incidents de sécurité nécessitant une attention immédiate 1261

Comment attribuer les droits d'utilisateur 67

Comment cela fonctionne-t-il ? 1611

Comment commencer à sauvegarde vos données 842

Comment créer Secure Zone 564

Comment créer, configurer et activer un workflow 1223

Comment enquêter sur des incidents dans la cyber kill chain 1287

Comment examiner des données à partir de la console Cyber Protect 843

Comment exécuter un basculement à l'aide

© Acronis International GmbH, 2003-2026

d'un serveur DHCP 1090

Comment exécuter un basculement des serveurs à l'aide d'un DNS local 1090

Comment fonctionne le filtrage d'URL 1197

Comment la création de Secure Zone transforme le disque 564

Comment les fichiers arrivent-ils dans le dossier de quarantaine ? 1213

Comment parcourir les phases d'une attaque 1293

Comment réduire les goulots d'étranglement ? 742

Comment restaurer les données vers un terminal mobile 842

Comment supprimer Secure Zone 565

Comment utiliser la notarisation 601, 940

Comparaison de versions de script 501

Comparaison des solutions de sauvegarde pour les données Microsoft 365 845

Compatibilité avec le logiciel de chiffrage 545

Compatibilité avec les disques durs Advanced Format (secteurs 4 K) 546

Compatibilité avec les stockages Data Domain Dell EMC 538

Compatibilité de Disaster Recovery avec le logiciel de chiffrement 1162

Compatibilité des formats de sauvegarde dans différentes versions de solution 615

Composants d'agent 188

Composants d'une installation sans assistance (EXE) 82

Composants d'une installation sans assistance (MSI) 91

Composants et modèles de workflow 1231

Compréhension de la détection des goulots d'étranglement 740

Compréhension de la portée et de l'impact des incidents 1263

Compréhension et personnalisation de la vue de la cyber kill chain 1290

Comprendre les actions entreprises pour réduire un incident 1297

Conditions de démarrage 507, 580

Conditions de démarrage de tâche 659

Configuration d'un VPN IPsec multi-site 1042

Configuration d'un workflow automatisé EDR (Endpoint Detection and Response) 1336

Configuration d'une connexion OpenVPN de site à site 1033

Configuration d'une sauvegarde CDP 569

Configuration d'une sauvegarde reconnaissant les applications 947

Configuration de l'accès VPN à distance de point à site 1053

Configuration de l'appliance virtuelle 139, 143, 155, 160

Configuration de l'appliance virtuelle Nutanix 169

Configuration de l'approbation automatique des correctifs 1412

Configuration de l'archivage des e-mails 772

Configuration de l'authentification à deux facteurs pour votre compte 22

Configuration de l'objet de stratégie de groupe 137

Configuration de la collecte de données d'investigation numérique 629

Configuration de la découverte passive de

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

terminaux 191

Configuration de la durée de vie des correctifs dans la liste 1411

Configuration de la fréquence des sauvegardes Google Workspace 925

Configuration de la fréquence des sauvegardes Microsoft 365 858

Configuration de la méthode par défaut pour mettre à jour les agents 122

Configuration de la protection antivirus et antimalware 1164

Configuration de la sauvegarde reconnaissant les applications des machines virtuelles exécutant Windows Server 2022 et versions ultérieures 816

Configuration de la sécurité de votre intelligence artificielle générative 1220

Configuration de serveurs DNS personnalisés 1062

Configuration des alertes de surveillance 1571

Configuration des connexions Microsoft 365 1345

Configuration des filtres de fichiers 622

Configuration des mesures d'intervention automatiques 1564

Configuration des paramètres Connect Client 1509

Configuration des paramètres de correctif au niveau du partenaire 1427

Configuration des paramètres de serveur proxy 52

Configuration des paramètres de serveur proxy dans Cyber Protect Monitor 375

Configuration des paramètres du VPN IPsec multi-site 1043

Configuration des paramètres RDP 1484

Configuration des paramètres réseau 1007

Configuration des règles de rétention 593

Configuration des serveurs de restauration 1067

Configuration des serveurs primaires 1072

Configuration des stratégies de notification par e-mail 1579

Configuration du basculement test automatisé 1086

Configuration du basculement test automatisé dans Microsoft Azure 1137

Configuration du chiffrement dans le plan de protection 597

Configuration du chiffrement en tant que propriété de l'ordinateur 598

Configuration du mode « sur Cloud uniquement » 1028

Configuration du nombre de nouvelles tentatives en cas d'erreur 263

Configuration du plan de protection Correctifs Production 1416

Configuration du plan de protection Correctifs Test 1415

Configuration du réseau de restauration de test 1125

Configuration du routage local 1063

Configuration OpenVPN de site à site 1032

Configuration requise 713, 734, 1032, 1139

Configuration réseau de la passerelle VPN 1031

Configuration réseau requise pour Agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) 147

Configuration système de l'appliance virtuelle 167

© Acronis International GmbH, 2003-2026

Configuration système requise pour l'agent 138, 141, 146, 157, 163

Configuration système requise pour les agents 45

Configurations de cluster prises en charge 811-812

Configurations de comptes utilisateur dans Virtuozzo Hybrid Infrastructure 147

Configurations de réseaux dans Virtuozzo Hybrid Infrastructure 147

Configurer le filtrage d'URL 1199

Configurer une stratégie de cycle de vie 1630

Configurer une stratégie de rétention 1630

Connectivité et réseaux 1026

Connectivité et réseaux dans Microsoft Azure 1120

Connexion à des ressources de type Bureau ou assistance à distance 1459

Connexion à des ressources gérées de type bureau ou assistance à distance 1485

Connexion à des ressources non gérées via Acronis Assistance rapide 1502

Connexion à des ressources non gérées via une adresse IP 1503

Connexion à distance à la ligne de commande 1495

Connexion à distance à une ressource 1322

Connexion à un compte Microsoft 1346

Connexion à un ordinateur démarré à partir d'un support de démarrage 1007

Connexion à une ressource gérée via un client Web 1488

Connexion aux terminaux découverts à distance 205

Connexion locale 1007

Connexion OpenVPN de site à site 1029

Connexion VPN IPsec multi-site 1041

Connexions à des ressources distantes de type bureau ou assistance à distance 1466

Connexions de point à site actives 1056

Connexions SSH à une appliance virtuelle 180

Conseils importants 589

Conseils utiles 920

Consolidation de sauvegarde 608

Consultation du dernier utilisateur connecté 482

Consulter les attaques dévoilées publiquement sur vos ressources à l'aide de flux d'informations sur les menaces 1254

Consulter ou modifier les paramètres d'accès 454

Conteneur Proxmox 673

Conteneur Virtuozzo Hybrid Server 670

Contrôleur de domaine Active Directory pour la connectivité OpenVPN de couche 2 1056

Contrôleur de domaine Active Directory pour la connectivité VPN IPsec de couche 3 1057

Conversion en une machine virtuelle 267

Conversion régulière en machine virtuelle ou exécution d'une machine virtuelle depuis une sauvegarde 270

Copier les bibliothèques Microsoft Exchange Server 839

Correction de ressource 1317

Correction des risques liés aux utilisateurs 1376

Correction manuelle des références des tenants 1366

Création d'un groupe dynamique 424

© Acronis International GmbH, 2003-2026

Création d'un groupe dynamique de terminaux au niveau du partenaire 390

Création d'un groupe statique 422

Création d'un groupe statique de terminaux au niveau du partenaire 390

Création d'un plan d'archivage 776-777

Création d'un plan de création de scripts 504

Création d'un plan de déploiement de logiciels 1446

Création d'un plan de gestion à distance 1467

Création d'un plan de protection 244

Création d'un plan de protection de reprise d'activité après sinistre 1022

Création d'un plan de protection de reprise d'activité après sinistre avec Microsoft Azure 1116

Création d'un plan de réplication 962

Création d'un plan de réplication de sauvegarde 255

Création d'un plan de surveillance 1561

Création d'un plan de validation 264

Création d'un plan SIEM pour un client individuel 282

Création d'un projet Google Cloud personnel 921

Création d'un runbook 1105

Création d'un runbook dans Microsoft Azure 1153

Création d'un script 493

Création d'un script à l'aide de l'intelligence artificielle 496

Création d'un serveur de restauration 1067

Création d'un serveur primaire 1072

Création d'un site de reprise d'activité après sinistre dans Microsoft Azure 1118

Création d'un support de démarrage afin de restaurer des systèmes d'exploitation 989

Création d'un support de démarrage physique 991

Création d'un support de démarrage WinPE ou WinRE 1002

Création d'un ticket de service d'assistance à partir d'une alerte 305

Création d'une règle de conservation légale 795

Création d'une règle de rétention 791

Création d'une requête de recherche enregistrée 785, 789

Création d'un plan global d'exclusions antivirus et antimalware 394

Création d'un workflow 1227

Création de compartiments 1628

Création de cyber-scripts 489

Création de sauvegardes dans une archive de sauvegarde existante 613

Création de serveurs de restauration dans Microsoft Azure 1127

Création des règles et des règles de flux de données 1583

Création du fichier de transformation et extraction des packages d'installation 136

Création et application d'un nouveau plan de sauvegarde 903

Créer et modifier des modèles de référence 1370

Créer un plan de transfert SIEM pour plusieurs clients 280

© Acronis International GmbH, 2003-2026

Créer une appliance virtuelle à partir d'un modèle OVA dans Proxmox 1040

Créer une nouvelle version d'un workflow 1239

Créneau de sauvegarde 646

Cyber Protect Monitor 372, 524

Cyber Protection 339

D

Dans Cyber Protect Cloud 851

Dans Cyber Protection 918

Dans Google Workspace 918

Dans Microsoft 365 851

Date et heure des fichiers 725

De combien d'agents ai-je besoin ? 138, 141, 146, 157

De quel agent ai-je besoin ? 41

De quel type de sauvegarde ai-je besoin ? 40

De quoi ai-je besoin pour utiliser la sauvegarde reconnaissant les applications ? 815

Déclencheurs de workflow 1231

Découverte active de terminaux à l'aide de Device Sense ™ 192

Découverte automatique des ordinateurs au niveau du partenaire 391

Découverte de plusieurs terminaux 182

Découverte de terminaux à l'aide de Device Sense ™ 189

Découverte passive de terminaux à l'aide de Device Sense ™ 191

Déduplication dans l'archive 615

Déduplication des données 543

Définir des mesures d'intervention pour un fichier suspect 1329

Définir des mesures d'intervention pour un processus suspect 1325

Définir des mesures d'intervention pour une entrée de registre suspecte 1330

Définir des mesures d'intervention pour une ressource affectée 1312

Définir la version par défaut d'un workflow 1240

Définir les paramètres de flux d'informations sur les menaces 1301

Définir un emplacement de sauvegarde dans Amazon S3 748

Définir un emplacement de sauvegarde dans IONOS Cloud, Impossible Cloud ou un stockage compatible S3 752

Définir un modèle de référence par défaut 1369

Définition d'un emplacement de sauvegarde dans Microsoft Azure 745

Définition d'un mode d'affichage 1008

Définition de l'ordre des plans favoris 237

Définition de plans en tant que favori 235

Définition de règles de pare-feu pour les serveurs Cloud 1078

Définition des plans par défaut 232

Définition du mot de passe de chiffrement 1616

Définition du mot de passe root sur une appliance virtuelle 181

Définitions des données sensibles 1597

Démarrage du démon Secure Shell 180

Démarrage manuel d'une analyse de l'inventaire logiciel 1387

Démarrage manuel d'une analyse de l'inventaire matériel 1381

© Acronis International GmbH, 2003-2026

Démarrer la machine virtuelle cible lorsque la restauration est complétée 730

Démarrer un chat avec un utilisateur distant 1516

Démarrer un chat dans Cyber Protect Monitor 375

Dépannage 718

Dépannage de la configuration VPN IPsec 1049

Dépannage de la connectivité VPN site à site OpenVPN 1040

Dépannage de la découverte de terminaux 206

Dépannage des problèmes d'autorisation sur macOS 109

Dépannage des problèmes de configuration VPN IPsec 1049

Dépendance Internet 1139

Déplacement des ressources vers un autre tenant 121

Déploiement d'agents de protection via la stratégie de groupe 135

Déploiement d'appliances virtuelles 138

Déploiement de l'agent pour Azure 162

Déploiement de l'agent pour Nutanix AHV 167

Déploiement de l'agent pour oVirt (appliance virtuelle) 157

Déploiement de l'agent pour Scale Computing HC3 (appliance virtuelle) 141

Déploiement de l'agent pour Synology 171

Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle) 145

Déploiement de l'agent pour VMware (appliance virtuelle) 138

Déploiement de l'appliance virtuelle Agent pour Azure 163

Déploiement des modèles de référence 1373

Déploiement du modèle OVA 158

Déploiement du modèle OVF 139

Déploiement du modèle QCOW2 142, 154, 168

Désactivation d'une règle de rétention 794

Désactivation de l'attribution automatique pour un agent 973

Désactivation de la connexion de site à site 1040

Désactivation de la recherche d'événements 1268

Désactivation de la recherche en texte intégral pour les sauvegardes Gmail 945

Désactivation de la Restauration en un clic 643

Désactivation de Startup Recovery Manager 1014

Désactivation du basculement test automatisé 1086, 1138

Désactivation du service de gestion de Microsoft 365 1348

Désactivation du stockage géoredondant 1623

Désactivation du stockage immuable 1620

Désactiver le planificateur de ressources partagées (PRP) automatique pour l'agent 138

Désactiver une règle de conservation légale 798

Description des options 636

Désenregistrement des ressources 120

Désinstallation d'agents 72

Désinstallation du logiciel 1442

Destinations prises en charge 569

Détails de l'analyse de la sauvegarde 357

Détails de l'utilisation de l'intelligence artificielle générative (7 derniers jours) 351

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Détecteurs de contenu personnalisés 1607

Détection automatique de la destination 1596

Détection d'un processus de cryptominage 1175

Détection de cryptominage 1192

Détection des terminaux 182

Détection par tactique 344

Différentes options de connexion 1465

Disaster Recovery vers Cyber Protect Cloud 1016

Disaster Recovery vers Microsoft Azure 1111

Disponibilité des options de restauration 721

Disponibilité des options de sauvegarde 602

Distribution des principaux incidents par ressource 342

Données considérées comme des informations de santé protégées 1598

Données considérées comme données PCI DSS 1602

Données considérées comme informations personnelles identifiables (PII) 1600

Données d'investigation 628

Données rapportées en fonction du type de widget 382

Dossier personnalisé en libre-service et à la demande 1215

Droits utilisateur requis pour les sauvegardes reconnaissant les applications 816

Droits utilisateurs requis 819, 851, 918

Durée de conservation des sauvegardes 552

E

Économiser de la batterie 584

Édition des compartiments 1630

Édition des références dans les modèles 1372

Effacement des données d'une ressource gérée 476

Effectuer un basculement permanent 965

Éléments à analyser 1394

Empêcher la désinstallation ou la modification non autorisée d'agents 207

Emplacement de quarantaine sur les machines 1215

Emplacements pris en charge 266, 595

Emplacements pris en charge pour la validation 259

Emplacements pris en charge pour le traitement des données hors hôte 258

En utilisant Universal Restore 718

Endpoint Detection and Response (EDR) 1251

Enquête sur les incidents 1286

Enregistrement des ressources 110

Enregistrement des ressources à l'aide d'un jeton d'enregistrement 112, 118

Enregistrement des ressources à l'aide de l'interface utilisateur graphique 110

Enregistrement des ressources à l'aide de la console Cyber Protect 110

Enregistrement des ressources à l'aide des identifiants utilisateur 112, 115

Enregistrement du support de démarrage 1005

Enregistrement et désenregistrement de ressources à l'aide de l'interface de ligne de commande 115

Enregistrement et lecture de sessions à distance 1508

Enregistrer des informations système au cas où

© Acronis International GmbH, 2003-2026

une restauration avec un redémarrage échouerait 726

Environnements de restauration 716

Envoi d'e-mails archivés 801

Envoi de données physiques 649

Espace disque libre nécessaire pour la mise à jour 122

Espace disque nécessaire 717, 1013

Est-ce que les paquets requis sont déjà installés ? 49

Etape 1 37

Etape 2 37

Etape 3 37

Etape 4 38

Etape 5 38

Étape 6 39

État de protection 340

État du plan 242

Éteindre les machines virtuelles cibles lors du démarrage de la restauration 730

Évaluation des vulnérabilités 1391

Évaluation des vulnérabilités et gestion des correctifs 1390

Évaluation des vulnérabilités et gestion des correctifs au niveau partenaire 1421

Évaluation des vulnérabilités pour les machines sous Linux 1397

Évaluation des vulnérabilités pour les machines Windows 1397

Évaluation des vulnérabilités pour les terminaux macOS 1398

Événements de prévention des pertes de données 1604

Éviter les sauvegardes en double des groupes Microsoft 365 862

Examen des incidents 1259

Examen du niveau de sécurité 1349

Examen du tableau de bord Risque 1349

Examen et gestion des stratégies 1590

Examiner des nœuds de la cyber kill chain 1295

Examiner et analyser les indicateurs de compromission découverts 1303

Examiner et atténuer les indicateurs de compromission sur les ressources affectées 1302

Examiner les phases d'attaque d'un incident 1292

Exclure des sous-classes de terminaux du contrôle d'accès 455

Exclure des terminaux USB particuliers du contrôle d'accès 456

Exclusion d'utilisateurs 1379

Exclusion de processus du contrôle d'accès 471

Exclusion des terminaux de la découverte 205

Exclusions 1193, 1212

Exclusions d'URL 1206

Exclusions de fichiers 726

Exclusions de protection 1182

Exécuter une sauvegarde de données d'investigation à la demande sur une ressource 1321

Exécution automatique de scripts pre-freeze et post-thaw 974

Exécution d'un basculement test dans Microsoft Azure 1134

Exécution d'un runbook 1109

© Acronis International GmbH, 2003-2026

Exécution d'une analyse active à la recherche de terminaux à l'aide de Device Sense ™ 192

Exécution d'une machine virtuelle à partir d'une sauvegarde (restauration instantanée) 957

Exécution d'une requête de recherche enregistrée 788

Exécution d'une restauration automatique avec agent via un support de démarrage 1094

Exécution d'une restauration automatique sans agent via un agent d'hyperviseur 1098

Exécution d'une sauvegarde à partir d'une planification 574

Exécution d'un basculement de production dans Microsoft Azure 1133

Exécution d'une restauration automatique manuelle à partir de Microsoft Azure 1150

Exécution de la ligne de commande à distance 1322

Exécution de la machine 958

Exécution du plan de protection Correctifs Test et refus des correctifs non sécurisés 1417

Exécution manuelle d'une sauvegarde 588

Exécution manuelle de sauvegardes de cloud à cloud 273

Exécution rapide du script 510

Exemple 76, 86, 101, 581-586, 592

- Installation manuelle des paquets sous Fedora 14 51
- Sauvegarde d'urgence en cas de blocs défaillants sur le disque dur 579

Exemple d'audit JSON 295

Exemple de contenu Debian 297

Exemple de contenu Red Hat 296

Exemples 75, 77, 85, 87, 99, 149, 153

Exemples d'utilisation 594, 957, 961, 974

Exemples d'activité CEF 289

exemples d'activité JSON 294

Exemples d'alerte CEF 287

Exemples d'alerte JSON 293

Exemples d'événement CEF 289

Exemples d'événements JSON 293

Exemples de filtres 623

Exemples de journal d'audit CEF 291

Exemples de requêtes 1275

Exemples de types de données 1277

Exigences communes 805

Exigences d'accès pour la sauvegarde dans le stockage dans le cloud public 757

Exigences de découverte de terminaux 183

Exigences et limitations pour le basculement de machines virtuelles Linux vers Microsoft Azure 1138

Exigences logicielles pour Disaster Recovery vers Cyber Protect Cloud 1017

Exigences logicielles pour Disaster Recovery vers Microsoft Azure 1112

Exigences logicielles pour Endpoint Detection and Response 1255

Exigences pour le contrôle de compte d'utilisateur (UAC) 187

Exigences pour les machines virtuelles ESXi 806

Exigences pour les machines virtuelles Hyper-V 807

© Acronis International GmbH, 2003-2026

Exigences relatives à l'appliance VPN 1032

Exigences relatives au mot de passe 21

Exigences supplémentaires pour les machines virtuelles 817

Exigences supplémentaires pour les ordinateurs exécutant Windows 817

Exigences supplémentaires pour les sauvegardes reconnaissant les applications 805-806

Exigences sur les comptes d'utilisateur 832

Exportation de chats 1518

Exportation de sauvegardes 736

Exporter des bases de référence vers un fichier CSV 1372

Exporter un plan de protection 248

Expression logique pour le japonais 1601

Expression logique pour toutes les langues prises en charge, à l'exception du japonais 1600

Expression logique utilisée pour la détection de contenu 1598, 1600, 1602

Extensions et règles d'exception 371

Extraction de fichiers à partir de sauvegardes locales 713

Extraction des fichiers MSI, MST et CAB 83

F

Façon d'utiliser Secure Zone 545

Fichiers d'un script 997

Fichiers journaux VPN IPsec multi-site 1052

Filtrage d'URL 1197

Filtrage des sessions de chat 1519

Filtres de fichiers (Inclusions/Exclusions) 620

Finalisation de la machine 959

Finalisation des machines exécutées depuis des sauvegardes Cloud 960

Finalisation vs. restauration normale 960

Flashback 726

Flux de menaces 364

Fonctionnalités antimalware 1168

Fonctionnalités compatibles avec S3 1625

Fonctionnalités de protection prises en charge par système d'exploitation 27

Fonctionnalités EDR 1252

Fonctionnalités non prises en charge 1615

Fonctionnalités prises en charge de bureau et assistance à distance 1460

Fonctionnalités prises en charge par plate-forme 1165

Fonctionnement 347, 364, 367, 483, 566, 601, 632, 940, 1188

Fonctionnement dans VMware vSphere 961

Fonctionnement de la conversion régulière vers une machine virtuelle 271

Fonctionnement du routage 1027, 1031, 1042

Format de sauvegarde 614

Format et exemples de données SIEM 286

Format et fichiers de sauvegarde 614

Fractionnement 658

G

Génération d'un jeton d'enregistrement 112

Génération d’une paire de clés d’accès 1627

Gérer l'isolation réseau d'une ressource 1313

Gérer vos incidents dans la page Incident 1253

Gestion 337

© Acronis International GmbH, 2003-2026

Gestion de l'accès à d'autres services de stockage dans le cloud public 765

Gestion de l'accès à votre abonnement Microsoft Azure 1115

Gestion de l'accès aux abonnements Microsoft Azure 761

Gestion de l'accès du compte dans le cloud public 757

Gestion de l'alimentation des MV 730, 966

Gestion de la mise en réseau dans Microsoft Azure 1123

Gestion de la sauvegarde et de la restauration des ressources et fichiers 513

Gestion de logiciels 1385

Gestion de vos workflows 1233

Gestion de votre inventaire de logiciels 1386

Gestion de votre inventaire matériel 1379

Gestion des compartiments dans le stockage d'archive 1627

Gestion des conflits d'adresse IP dans le basculement 1132

Gestion des correctifs 1401

Gestion des fichiers mis en quarantaine 1214

Gestion des fichiers non protégés détectés 368

Gestion des jetons d'enregistrement 114

Gestion des licences pour les serveurs de gestion sur site 215

Gestion des modèles de référence du tenant 1368

Gestion des paramètres de l'appliance VPN 1034

Gestion des paramètres de la connexion de point à site 1055

Gestion des réseaux en mode Cloud uniquement 1028

Gestion des réseaux pour OpenVPN site à site 1035

Gestion des ressources cibles pour un plan 508

Gestion des ressources dans la console Cyber Protect 385

Gestion des utilisateurs Microsoft 365 1375

Gestion des vulnérabilités trouvées 1398

Gestion du pare-feu 1212

Gestion du réseau 1057

Gestion du site de reprise d'activité après sinistre dans Microsoft Azure 1117

Gestion erreurs 618, 725, 966

Gestion et affectation des workflows d'automatisation 1223

Gestion et surveillance de l'environnement Microsoft 365 1345

Groupes de cloud à cloud et groupes autres que de cloud à cloud 421

Groupes de mots-clés 1603

Groupes de sécurité réseau (NSG) 1121

Groupes du terminal 419

Groupes dynamiques 420

Groupes par défaut 419

Groupes par défaut et groupes personnalisés 419

Groupes personnalisés 420

Groupes statiques 420

Groupes statiques et dynamiques 420

H

H.264 1464

Haute disponibilité d'une machine restaurée 985

© Acronis International GmbH, 2003-2026

Historique d'installation des correctifs 356

Historique de gravité de l'incident 343

I

Icônes du graphique XDR 1249

Identifiants de la ressource 1481

Ignorer les enregistreurs VSS échoués 660

Ignorer les erreurs 725

Ignorer les secteurs défectueux 619

Images WinPE 1002

Images WinRE 1001

Implémentation de la reprise d'activité après sinistre 1016

Importation de plans de création de scripts 510

Importation des e-mails à partir de fichiers PST 778

Importer des références dans des modèles 1371

Importer un plan de protection 248

Index de recherche 942

Informations de santé protégées (PHI) 1597

Informations personnelles identifiables (PII) 1599

Informations pour les administrateurs partenaires 403

Infrastructure par défaut du réseau cloud 1025

Installation à distance des agents 196

Installation d'agents à distance 200

Installation de correctifs à la demande 1418

Installation de l'agent de machine virtuelle Azure avec accès Internet 1139

Installation de l'agent de machine virtuelle Azure sans accès Internet 1139

Installation de l'agent pour Linux en mode compatible FIPS 63

Installation de l'agent pour Proxmox 955

Installation de l'agent pour Synology 173

Installation de l'agent pour Windows en mode compatible FIPS 60

Installation de la fonctionnalité SIEM 275

Installation de la fonctionnalité SIEM à l'aide de l'interface graphique 275

Installation de la fonctionnalité SIEM sans surveillance 278

Installation des agents de protection à l'aide de l'interface utilisateur graphique 64

Installation des agents de protection sous Linux 69

Installation des agents de protection sous macOS 71

Installation des agents de protection sous Windows 64

Installation des agents et des composants (combinaison MSI et MST) 84

Installation des paquets à partir de la base de données de référentiel. 50

Installation du logiciel 1438

Installation dynamique des composants 56

Installation et déploiement d'agents Cyber Protection 37

Installation et désinstallation d'agents de protection à l'aide de l'interface de ligne de commande 74

Installation et désinstallation d'agents de protection dans macOS 99

Installation et désinstallation d'agents de protection sous Linux 92

© Acronis International GmbH, 2003-2026

Installation et désinstallation d'agents de protection sous Windows 74

Installation et désinstallation d'agents et de composants (MSI et sélection directe) 84

Installation et désinstallation des agents et des composants (EXE) 75

Installation et désinstallation sans assistance à l'aide d'un fichier EXE 74

Installation et désinstallation sans assistance à l'aide d'un fichier MSI 83

Installation manuelle des paquets 51

Instantané de sauvegarde de niveau fichier 627

Instantanés intermédiaires 271

Intégration d'utilisateurs 1375

Intégration de DirectAdmin, de cPanel et de Plesk 956

Interaction avec d'autres options de sauvegarde 654

J

Journal des événements Windows 664, 730

L

L'outil « tibxread » pour obtenir les données sauvegardées 633

L'utilisateur est inactif 581

L'hôte de l'emplacement de la sauvegarde est disponible 582

La console Cyber Protect 385

Lancer une analyse du Score #CyberFit 487

Langage d'interrogation XDR d'Acronis (XQL) 1272

Langues prises en charge 1597, 1599, 1601-1602

Le modèle par défaut 1368

Le tableau de bord Activités 299

Le tableau de bord des alertes 300

Les fonctionnalités clés 1016

Liaison de machine virtuelle 972

Liaison manuelle 973

Licence de Disaster Recovery pour Microsoft Azure 1114

Limitations et problèmes connus 901

Limitations pour les ressources Proxmox 954

Limite le nombre total de machines virtuelles sauvegardées simultanément. 986

Limites 59, 146, 158, 168, 172, 270, 346, 490, 528, 531-532, 535-538, 552-553, 558, 560, 563, 674, 689, 709, 717, 724, 731, 772, 779, 850, 870, 881, 886, 891, 919, 927, 930-931, 935-936, 947, 962, 969, 1014, 1019, 1113, 1139, 1218, 1615, 1621-1622

Limites d'utilisation du stockage géoredondant dans le cloud 1021

Limites de la restauration des fichiers dans la console Cyber Protect 713

Limites des noms de fichier de sauvegarde 610

Linux 555

list backups 634

list content 635

Liste blanche d'entreprise 1215

Liste d'autorisation des périphériques USB 466

Liste d'autorisation des types de terminaux 464

Liste des terminaux USB sur un ordinateur 470

Listes de plans de transfert SIEM 279

Lors d'un événement du Journal des événements Windows 579

© Acronis International GmbH, 2003-2026

M

Ma boîte de réception 26

Mac 555

Machine physique 667

Machine virtuelle Broadcom VMware ESXi 668

Machine virtuelle Microsoft Azure 668

Machine virtuelle Microsoft Hyper-V 669

Machine virtuelle Nutanix 672

Machine virtuelle Proxmox 672

Machine virtuelle Red Hat Virtualization/oVirt 671

Machine virtuelle Scale Computing HyperCore 671

Machine virtuelle Virtuozzo Hybrid Infrastructure 670

Machine virtuelle Virtuozzo Hybrid Server 669

Machines vulnérables 354

Mappage de client 1347

Marqué confidentiel 1602

McAfee Endpoint Encryption et PGP Whole Disk Encryption 546

Mécanisme de notation #CyberFit 483

Mémoire en cache 213

Mes packages 1430

Mesures d'intervention manuelles 1575

Mesures d'intervention pour les différents nœuds de la cyber kill chain 1310

Méthode d'utilisation de la fonctionnalité EDR (Endpoint Detection and Response) 1258

Méthode de suivi de géolocalisation prise en charge par le système d'exploitation 1512

Méthode de transfert des fichiers 286

Méthode de transfert via serveur syslog 286

Méthodes de transfert SIEM 286

Méthodes de validation 259

Microsoft 529

Microsoft 365 Business – Sauvegarde 859

Microsoft Exchange Server 617

Microsoft Security Essentials 1209

Microsoft SQL Server 616

Mise à jour automatique des agents de protection 131

Mise à jour d'un workflow 1237

Mise à jour de l'agent pour Synology 178

Mise à jour des agents de protection 121

Mise à jour des agents de protection sur les ressources chiffrées par BitLocker 134

Mise à jour des définitions de Cyber Protection à la demande 213

Mise à jour des définitions de Cyber Protection de façon planifiée 213

Mise à jour manuelle des agents de protection 129

Mise à jour, reconstruction ou suppression des index 943

Mises à jour automatiques pour les composants 211

Mises à jour manquantes, par catégorie 356

Mode « sur Cloud uniquement » 1027

Mode compatible FIPS 59

Mode d'accès 1625

Mode de conformité 1615

Mode de démarrage 723

© Acronis International GmbH, 2003-2026

Mode de sauvegarde de cluster 616

Modèles de sauvegarde 571

Modèles de workflow 1233

Modèles intégrés et personnalisés 1368

Modes de stockage immuable 1618

Modification d'un groupe dynamique 445

Modification d'un plan de protection 247

Modification d'un plan de sauvegarde 905

Modification d'une règle de conservation légale 797

Modification d'une règle de rétention 793

Modification d'un plan de transfert SIEM 285

Modification de l'adaptateur graphique d'une appliance virtuelle 161

Modification de l'environnement de restauration 718

Modification de l'état du script 501

Modification de l'inscription d'une ressource 120

Modification de SID 729

Modification des identifiants de Microsoft 365 914

Modification des informations d'identification de SQL Server ou d'Exchange Server 839

Modification des packages logiciels 1437

Modification des paramètres du serveur de restauration 1131

Modification des paramètres par défaut d'un serveur de restauration 1024

Modification des ports utilisés par l'agent de protection 40

Modification des références des tenants 1365

Modification du compte utilisateur de l'agent pour VMware 984

Modification du délai d'expiration de la validation du pouls et des captures d'écran d'une machine virtuelle 262

Modification du format de sauvegarde en version 12 (TIBX) 615

Modification du mot de passe de chiffrement 1616

Modification ou suppression d'un script 500

Modifier le quota du service pour les ressources 209

Moniteurs configurables 1525

Montage de bases de données Exchange Server 831

Montage de volumes à partir d'une sauvegarde 734

Moteur de comportement 1176

N

Navigateurs Web pris en charge 25

Navigation dans l'inventaire du logiciel 1387

Navigation dans l'inventaire du matériel 1381

Navigation dans les référentiels de logiciels 1431

Ne pas afficher les messages et dialogues pendant le traitement (mode silencieux) 619, 725

Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants 585

Ne pas démarrer pendant une connexion mesurée 584

NEAR 1464

Nettoyage 266

Niveau de compression 618

Niveaux d'administration dans la console Cyber Protect 387

© Acronis International GmbH, 2003-2026

Nom de fichier de sauvegarde 609

Nom de fichier de sauvegarde par défaut 611

Noms sans variables 612

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) 1601

Notarisation 601, 939

Notarisation des sauvegardes avec les données d'investigation 632

Notificateurs de Bureau à distance 1510

Notifications du système d'exploitation et alertes de service 463

Nouveautés de la console Cyber Protect 386

Nutanix 536

O

Objet de variable 998

Objet Toplevel 998

Observation simultanée de plusieurs ressources gérées 1500

Obtenir le certificat pour les sauvegardes avec données d'investigation 633

obtenir le contenu 635

Obtention de l'identifiant et du secret d'application 912

Octroi d'une autorisation d'accès au compte utilisateur 983

Onglet Activités 371

OpenVPN de site à site – Informations complémentaires 1634

Opérateurs de recherche 426

Opérations à distance avec un support de démarrage 1009

Opérations avec des runbooks dans Microsoft Azure 1156

Opérations avec des sauvegardes 731

Opérations avec des serveurs primaires 1075

Opérations avec les runbooks 1109

Opérations liées aux serveurs de restauration 1070

Opérations locales avec support de démarrage 1007

Opérations prises en charge pour les volumes logiques 543

Opérations réalisées avec les machines virtuelles Microsoft Azure 1020

Opérations spéciales avec les machines virtuelles 957

Opérations supplémentaires réalisables avec les plans de déploiement de logiciels 1456

Option de stockage avancée 562

Options de planification supplémentaires 587

Options de redémarrage 1407

Options de réplication 965

Options de restauration 721

Options de restauration automatique 966

Options de sauvegarde 602

Options de sauvegarde par défaut 602

Options supplémentaires 575

Oracle 535

Orchestration (runbooks) 1104

Où puis-je voir les noms des fichiers de sauvegarde ? 610

Où trouver l'application Acronis Cyber Protect 842

oVirt/Red Hat Virtualization 4.2 et 4.3/Oracle Virtualization Manager 4.3 162

oVirt/Red Hat Virtualization 4.4, 4.5 162

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

P

Packages Linux requis pour l'installation d'agents dans Linux 48

Packages logiciels 1429

Page de gestion de la base de données des terminaux USB 468

Parallels 535

Paramètres 993

Paramètres avancés 1595

Paramètres d'accès 459

Paramètres d'Active Protection dans Cyber Backup Standard 1188

Paramètres d'enregistrement 96

Paramètres d'évaluation des vulnérabilités 1394

Paramètres d'événement 579

Paramètres d'information 98

Paramètres d'installation 95

Paramètres d'installation ou de désinstallation sans assistance 95

Paramètres d'une installation sans assistance (EXE) 77

Paramètres d'une installation sans assistance (MSI) 87

Paramètres de base 95

Paramètres de compartiment 759, 761

Paramètres de confidentialité 24

Paramètres de désinstallation 98

Paramètres de gestion des correctifs dans le plan de protection 1402

Paramètres de la carte de protection des données 368

Paramètres de liste blanche 1216

Paramètres de protection 210

Paramètres de protection contre les virus et les malwares 1170

Paramètres de quarantaine 1175

Paramètres de runbook dans Microsoft Azure 1155

Paramètres de sécurité de l'intelligence artificielle générative 1220

Paramètres de sécurité IPsec/IKE 1046

Paramètres de Universal Restore 719

Paramètres du filtrage d'URL 1199

Paramètres du moniteur de statut de Windows Update 1556

Paramètres du moniteur de statut du service Windows 1552

Paramètres du moniteur Dernier redémarrage du système 1554

Paramètres du moniteur du journal des événements Windows 1554

Paramètres du moniteur Échecs de connexion 1557

Paramètres du moniteur Espace disque 1532

Paramètres du moniteur État de la fonctionnalité d'exécution automatique 1559

Paramètres du moniteur État du logiciel antimalware 1557

Paramètres du moniteur État du pare-feu 1557

Paramètres du moniteur État du processus 1552

Paramètres du moniteur Logiciel installé 1553

Paramètres du moniteur Modifications apportées au matériel 1538

Paramètres du moniteur personnalisé 1559

© Acronis International GmbH, 2003-2026

Paramètres du moniteur Taille des fichiers et dossiers 1555

Paramètres du moniteur Température du processeur 1535

Paramètres du moniteur Température du processeur graphique 1536

Paramètres du moniteur Utilisation de la mémoire 1540

Paramètres du moniteur Utilisation de la mémoire par processus 1548

Paramètres du moniteur Utilisation du processeur 1538

Paramètres du moniteur Utilisation du processeur par processus 1548

Paramètres du moniteur Utilisation du réseau 1545

Paramètres du moniteur Utilisation du réseau par processus 1550

Paramètres du moniteur Vitesse de transfert du disque 1542

Paramètres du moniteur Vitesse de transfert du disque par processus 1549

Paramètres du noyau 993

Paramètres du runbook 1107

Paramètres personnalisés 1186

Paramètres pour les fonctionnalités héritées 98

Paramètres réseau 1005

Paramètres supplémentaires 97

Pare-feu Azure 1121

Partage d'écran Apple 1465

Partage du contenu du Presse-papiers entre des ressources 1490

Passage d'OpenVPN site à site à un VPN IPsec multisite 1039

Passage d'un VPN IPsec multisite à un VPN OpenVPN site à site 1048

Passerelle VPN 1031, 1042

Performance 727, 966

Performance et créneau de sauvegarde 645

Personnalisation du tableau de bord Alertes 301

Pilotes de stockage de masse à installer de toutes façons 720

Plan d'analyse des sauvegardes 272

Planification 369, 506, 657, 1394, 1405

Planification de sauvegarde 570

Planification et conditions de démarrage 506

Planifier l'analyse 1179, 1209

Planifier par événement 576

Planifier selon l'horaire 574

Plans à différents niveaux d'administration 240

Plans d'archivage 775

Plans de création de scripts 503

Plans de déploiement de logiciels 1446

Plans de gestion à distance 1467

Plans de gestion à distance intégrés 230

Plans de protection des données hors hôte 255

Plans de protection individuels pour l'hébergement des intégrations du panneau de configuration 251

Plans de protection intégrés 219

Plans de sauvegarde appliqués et planifiés pour les ressources Microsoft 365 859

Plans de sauvegarde pour les applications dans le Cloud 273

Plans de surveillance 1523, 1561

© Acronis International GmbH, 2003-2026

Plans de surveillance intégrés 228

Plans de transfert SIEM 274

Plans et modules de protection 243

Plans favoris 234

Plans intégrés 219

Plans par défaut 231

Plans préselectionnés 238

Plans pris en charge pour les groupes de terminaux 421

Plates-formes de virtualisation prises en charge 526, 1018, 1112

Plates-formes prises en charge 490

Plates-formes prises en charge pour la surveillance 1524

Points de calcul 1082

Points de montage 639, 727

Points de restauration Azure 606

- gestion des disques non pris en charge 608
- niveau de cohérence 607
- rétention 606

Ports 1033

Ports requis 162

Ports requis par le composant Téléchargeur 39

Ports TCP requis pour la sauvegarde et la réplication de machines virtuelles VMware 38

Ports utilisés par Device Sense ™ 193

Pour rétablir le disque RAM initial d'origine 721

Pourquoi utiliser Bootable Media Builder ? 992

Pourquoi utiliser la sauvegarde reconnaissant les applications ? 814

Pourquoi utiliser Secure Zone ? 563

Pourquoi y a-t-il des sauvegardes mensuelles avec un modèle horaire ? 591

Préconfiguration de plusieurs connexions réseau 1006

Préparation 37, 719

- WinPE 2.x et 3.x 1004
- WinPE 4.0 et versions ultérieures 1004

Préparation des ordinateurs pour l'installation à distance manuelle 197

Préparation des ordinateurs pour une installation à distance à l'aide d'un objet de stratégie de groupe (GPO) 198

Préparez les pilotes 719

Prérequis 129, 135, 178, 180-181, 391, 479-481, 489, 560, 643, 713, 947, 958, 974, 1029, 1051, 1054, 1580

Présentation de votre niveau de protection actuel 298

Présentation des clusters Exchange Server 812

Présentation des plans 216

Présentation des solutions SQL Server haute disponibilité 810

Présentation du processus d'envoi de données physiques 650

Prévention des failles 1176

Prévention des pertes de données 1583

Prévention des pertes de données GenAI 1221

Prévisualisation des e-mails 798

Principales solutions d'intelligence artificielle (visites) 350

Prioriser les incidents nécessitant une attention immédiate 1261

Priorité de CPU 647

Prise d'instantanés LVM 638

© Acronis International GmbH, 2003-2026

Prise en charge de l'agrégation de cartes réseau 1011

Prise en main de Cyber Protection 21

Privilèges requis pour l'agent pour VMware 977

Privilèges requis pour le compte de connexion 67

Problèmes connus 947

Problèmes connus et limites 1613

Problèmes de compatibilité avec les plans 251

Problèmes de configuration inter-abonnements dans Microsoft Azure 1115

Procédure d'analyse du graphique XDR 1245

Procédures de restauration spécifiques au logiciel 546

Processus de basculement test 1133

Processus de sauvegarde de données d'investigation 629

Processus Universal Restore 720

Produits Apple pris en charge 1393

Produits Microsoft 1403

Produits Microsoft pris en charge 1391

Produits tiers pour macOS pris en charge 1393

Produits tiers pris en charge pour Windows 1393

Produits Windows tiers 1404

Protection antimalware Advanced 1171

Protection continue des données (CDP) 566

Protection contre l'injection de prompt 1222

Protection contre les virus et les malwares 30, 1165, 1168

Protection côté serveur 1172, 1191

Protection d'applications Microsoft 803

Protection d'un contrôleur de domaine 804

Protection de Microsoft SharePoint 804

Protection de SAP HANA 946

Protection de sites SharePoint Online 885

Protection des applications de collaboration et de communication 273

Protection des blocs-notes OneNote 900

Protection des boîtes aux lettres Exchange Online 915

Protection des données Exchange Online 864

Protection des données Google Workspace 917

Protection des données Microsoft 365 844

Protection des données Microsoft 365 Teams 890

Protection des données MySQL et MariaDB 946

Protection des environnements de virtualisation 976

Protection des fichiers de Drive partagés 935

Protection des fichiers OneDrive 880

Protection des groupes de disponibilité Always On (AAG) 810

Protection des groupes de disponibilité de la base de données (DAG) 812

Protection des machines virtuelles et des conteneurs Proxmox 953

Protection des postes avec application de collaboration Microsoft 365 901

Protection des serveurs Microsoft SQL Server et Microsoft Exchange Server 803

Protection des terminaux mobiles 840

Protection du dossier réseau 1171, 1191

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Protection du navigateur 1207

Protection en temps réel 1169, 1178, 1210

Protection intelligente 364

Protéger des données Gmail 926

Protéger des fichiers Google Drive 930

Protéger les serveurs d'hébergement Web 956

Protocoles de connexion à distance 1464

Provisionnement du disque 966

Proxmox VE 533

Q

Qu'est-ce qu'un fichier de sauvegarde ? 609

Qu'est-ce qu'un goulot d'étranglement ? 740

Qu'est-ce qui déclenche une règle ? 1587

Quarantaine 1213

Que faire ensuite 1024

Que répliquer 257

Que signifie la protection Google Workspace ? 917

Que sont les incidents exactement ? 1260

Que stocke une sauvegarde de disque ou de volume ? 554

Quelles sont les informations incluses dans une phase d'attaque ? 1293

Quels éléments de données peuvent être restaurés ? 864, 881, 886, 890, 915, 926, 931, 935

Quels éléments ne peuvent pas être restaurés ? 887

Quels éléments peuvent être sauvegardés ? 864, 880, 885, 890, 915, 926, 930, 935

Quotas 956

R

Rapport des licences de poste Microsoft 365 857

Rapports 378

RDP 1465

Réaffectation d'adresses IP 1061

Réaffectation de sessions de chat 1518

Réalisation d'actions de contrôle sur les ressources gérées 1492

Réalisation d'un basculement 1088

Réalisation d'un basculement test 1083

Réalisation d'une restauration automatique en mode manuel 1102

Recevoir des notifications d'alerte en cas de violation 1253

Recherche 338

Recherche d'e-mails 781

Recherche d'événements 1266

Recherche d'indicateurs de compromission (IoC) et d'activités suspectes 1266

Recherche dans les sauvegardes cloud à cloud 941

Recherche dans Ma boîte de réception 26

Recherche de messages dans les sessions de chat 1519

Recherche de nœuds individuels 1247

Recherche de pilote automatique 719

Recherche en texte intégral 942

Rechercher des attributs pour les ressources autres que cloud à cloud 430

Rechercher des attributs pour les ressources de cloud à cloud 429

© Acronis International GmbH, 2003-2026

Rechercher des indicateurs de compromission dans des attaques connues publiquement et visant vos ressources 1300

Recommandations 724, 1139

Recommandations et étapes de réparation 1253

Recommandations générales pour les sites locaux 1045

Recommandations pour la disponibilité d'AD DS sur le site DR dans Azure 1124

Recommandations pour la disponibilité des services de domaine Active Directory 1056, 1124

Reconfiguration d'une adresse IP 1059

Récupération des données d'investigation numérique 630

Récupération des routines stockées 952

Red Hat et Linux 534

Redémarrer une ressource 1319

Redirection du son à distance 1465

Redirection du son d'une ressource distante Linux 1466

Redirection du son d'une ressource distante macOS 1465

Redirection du son d'une ressource distante Windows 1465

Redistribution 972

Réessayer si une erreur se produit 618, 725

Réessayer si une erreur se produit lors de la création d'instantané de MV 620

Références de tenant 1352

Référentiel de scripts 502

Référentiels de logiciels 1429

Régénération de la configuration 1055

Règle commune d'installation 545

Règle de sauvegarde commune 546

Règles de conservation légale 794

Règles de pare-feu pour les serveurs Cloud 1078

Règles de rétention 589, 790

Règles de rétention en fonction du modèle de sauvegarde 590

Règles de stratégie pour les disques et les volumes 555

Règles de stratégie pour les fichiers et les dossiers 558

Réinitialisation des modèles d'apprentissage automatique 1570

Réinitialisation des mots de passe des utilisateurs 1378

Réinstallation de la passerelle VPN 1061

Remarque pour les utilisateurs Mac 666

Renommer un plan de transfert SIEM 285

Renouvellement de l'accès à un abonnement Microsoft Azure 763

Renouvellement de l'accès à une connexion au cloud public 770

Renouvellement de la règle d'un ou plusieurs utilisateurs de la société ou de l'unité 1591

Renouvellement de la règle d'une société ou d'une unité 1591

Renouvellement de la règle de flux de données 1590

Réplication 594

Réplication de machines virtuelles 961

Réplication de sauvegarde 255

Réplication vs. sauvegarde 961

© Acronis International GmbH, 2003-2026

Requêtes de recherche 781

Réseau de restauration de production 1123

Réseau de test de restauration 1123

Résolution des incidents de sécurité 344

Résolution des problèmes de compatibilité 253

Ressources 396

Ressources agrégées 479

Ressources CyberApp 479

Restauration 544, 664

Restauration à partir d'une sauvegarde 1323

Restauration à partir d'une sauvegarde reconnaissant les applications 948

Restauration automatique 965, 1091

Restauration automatique à partir de Microsoft Azure vers une machine virtuelle Azure 1152

Restauration automatique avec agent via un support de démarrage 1092

Restauration automatique avec agent via un support de démarrage à partir de Microsoft Azure 1140, 1142

Restauration automatique dans Microsoft Azure 1139

Restauration automatique depuis Cyber Protect Cloud vers une machine virtuelle Azure 1104

Restauration automatique en mode manuel 1102

Restauration automatique manuelle à partir de Microsoft Azure 1150

Restauration automatique sans agent via un agent d'hyperviseur 1096

Restauration automatique sans agent via un agent d'hyperviseur à partir de Microsoft Azure 1144

Restauration automatique sans agent via un agent d'hyperviseur à partir de Microsoft Azure 1146

Restauration avec redémarrage 716

Restauration d'applications 804

Restauration d'e-mails, de dossiers et de boîtes aux lettres 799

Restauration d'éléments de boîte aux lettres 835, 873, 916, 928

Restauration d'éléments de boîte aux lettres d'équipe vers des fichiers PST 896

Restauration d'éléments de boîte aux lettres vers des fichiers PST 876

Restauration d'éléments sauvegardés 907

Restauration d'instances 949

Restauration d'une configuration ESXi 715

Restauration d'une machine à l'aide de la restauration en un seul clic 643

Restauration d'une machine physique en tant que machine physique 675

Restauration d'une machine physique en tant que machine virtuelle 676

Restauration d'une machine virtuelle en tant que machine physique 690

Restauration d'une machine virtuelle en tant que machine virtuelle 691

Restauration de bases de données 950

Restauration de bases de données Exchange 828

Restauration de bases de données incluses dans un AAG 811

Restauration de bases de données SQL 819

Restauration de bases de données SQL sous forme de fichiers 824

© Acronis International GmbH, 2003-2026

Restauration de bases de données SQL vers l'ordinateur d'origine 820

Restauration de bases de données SQL vers un ordinateur différent de l'ordinateur d'origine 822

Restauration de blocs-notes OneNote sauvegardés 900

Restauration de boîtes aux lettres 833, 871, 916, 927

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres 871, 916, 927

Restauration de boîtes aux lettres et éléments de boîtes aux lettres Exchange 831

Restauration de chemin d'accès complet 727

Restauration de conteneurs 702

Restauration de disques via un support de démarrage 704

Restauration de données à partir d'une archive d'e-mails 798

Restauration de données de SharePoint Online 888

Restauration de dossiers publics et d'éléments de dossier 879

Restauration de fichiers dans la console Cyber Protect 707

Restauration de fichiers Google Drive 933

Restauration de fichiers OneDrive 883

Restauration de fichiers via un support de démarrage 712

Restauration de l'aide-mémoire 664

Restauration de l'état du système 714

Restauration de l'intégralité d'un Drive partagé 937

Restauration de l'intégralité d'une équipe 892

Restauration de l'intégralité d'une instance Google Drive 932

Restauration de l'intégralité de boîtes aux lettres dans des fichiers de données PST 875

Restauration de l'intégralité de OneDrive 882

Restauration de la base de données MASTER 827

Restauration de machines physiques 674

Restauration de machines virtuelles 689

Restauration de machines virtuelles Microsoft Azure et Amazon EC2 989

Restauration de OneDrive et de fichiers OneDrive 882

Restauration de sauvegardes dans les tenants en mode de conformité 1617

Restauration de serveur de restauration en basculement vers un moment donné précédent 1132

Restauration de tables 951

Restauration depuis un partage réseau 996

Restauration des bases de données système 827

Restauration des données à l'aide d'un support de démarrage local 1008

Restauration des données du cluster Exchange 814

Restauration des Drives partagés et des fichiers de Drive partagés 937

Restauration des fichiers 707

Restauration des fichiers de Drive partagés 938

Restauration du serveur tout entier 949

Restauration du stockage Cloud 996

Restauration en un seul clic 640

© Acronis International GmbH, 2003-2026

Restauration interplate-forme 666-667

Restauration interplate-forme via un support de démarrage 673

Restauration sur des conteneurs ou machines virtuelles Virtuozzo 714

Restauration sûre 730

Restaurer des canaux ou des fichiers d'équipe dans les canaux d'équipe 893

Restaurer des ressources Proxmox 955

Restaurer les messages électroniques et les réunions 898

Restaurer un site d'équipe ou des éléments précis d'un site 899

Restaurer une boîte aux lettres d'équipe 896

Restaurer une instance et des fichiers Google Drive 932

Résumé d'installation des correctifs 356

Résumé de l'utilisation de l'intelligence artificielle générative (clients) 351

Résumé de l'utilisation de l'intelligence artificielle générative (terminaux) 351

Révision des modèles de référence 1369

Révocation d'un plan à partir d'un groupe 447

Révocation d'un plan d'archivage 778

Révocation d'un plan de protection 249

Révocation d'un plan de sauvegarde pour Microsoft 365 Business – Sauvegarde 861

Révocation de plans de surveillance 1564

Révocation des droits d'accès de l'application de service de sauvegarde 857

Révocation des modèles de référence 1374

Révoquer un plan de sauvegarde pour la sauvegarde directe vers Microsoft 365 910

RMM 1344

Rôles d'utilisateur et droits de création de cyber-scripts 491

Rôles requis 162

Routage de sous-réseau (itinéraires définis par l'utilisateur) 1122

Runbooks dans Microsoft Azure 1153

S

Sauter l'exécution de la tâche 659

Sauvegarde 543, 547

Sauvegarde avec agent de machines virtuelles Microsoft Azure et Amazon EC2 988

Sauvegarde avec et sans agent 40

Sauvegarde d'Oracle Database 946

Sauvegarde dans Amazon S3 757

Sauvegarde dans Microsoft Azure 757

Sauvegarde de base de données 808

Sauvegarde de boîte de réception 817

Sauvegarde de machines Hyper-V en cluster. 985

Sauvegarde de ressources dans des clouds publics 745

Sauvegarde de serveurs cloud 1077

Sauvegarde des bases de données incluses dans un AAG 811

Sauvegarde des données de cluster Exchange 813

Sauvegarde des machines virtuelles Microsoft Azure et Amazon EC2 988

Sauvegarde des machines virtuelles Nutanix 171

Sauvegarde des ressources Proxmox 955

© Acronis International GmbH, 2003-2026

Sauvegarde directe dans le stockage de sauvegarde de Microsoft 365 902

Sauvegarde hebdomadaire 664

Sauvegarde incrémentielle/différentielle rapide 620

Sauvegarde pré-mise à jour 1409

Sauvegarde prenant en charge les clusters 812

Sauvegarde reconnaissant les applications 814

Sauvegarde secteur par secteur 657

Sauvegarde vers un stockage compatible S3 (inclut Wasabi, IONOS Cloud et Impossible Cloud) 759

Scale Computing 532

Scénarios d'utilisation 734

Score #CyberFit par machine 345

Score #CyberFit pour les machines 483

Scripts 493

Scripts personnalisés 997

Scripts prédéfinis 996

Scripts sur un support de démarrage 996

Sécurité 1465

Sécurité de niveau fichier 726

Sélection d'un niveau d'administration 387

Sélection d'un ordinateur complet 552

Sélection d'une destination 560

Sélection de boîtes aux lettres 865

Sélection de disques ou de volumes 553

Sélection de données Exchange Server 809

Sélection de données SharePoint Online 887

Sélection de dossiers publics 868

Sélection de fichiers de Drive partagés 936

Sélection de fichiers OneDrive 881

Sélection de fichiers ou de dossiers 556

Sélection de l'état du système 559

Sélection de la configuration ESXi 560

Sélection des bases de données SQL 808

Sélection des boîtes aux lettres Gmail 927

Sélection des boîtes aux lettres Microsoft 365 915

Sélection des données à sauvegarder 552

Sélection des équipes 891

Sélectionner des fichiers Google Drive 931

Sélectionner le fournisseur d'instantanés 661

Sélectionner les boîtes aux lettres Exchange Server 819

Serveurs Cloud 1066

Serveurs de restauration dans Microsoft Azure 1126

Serveurs de restauration en basculement 1161

Serveurs DNS 1121

Serveurs primaires 1161

Service de cliché instantané des volumes 660

Service de cliché instantané des volumes (VSS) pour les machines virtuelles 662, 966

Services Cyber Protection installés dans votre environnement 214

Services installés sous macOS 214

Services installés sous Windows 214

Si vous choisissez d'enregistrer la machine virtuelle comme un ensemble de fichiers 271

Si vous choisissez de créer la machine virtuelle sur un serveur de virtualisation 271

Signer un fichier avec ASign 710

Snapshot Multi-volume 640

© Acronis International GmbH, 2003-2026

Solutions Apple et tiers prises en charge pour l'évaluation des vulnérabilités 1393

Solutions Linux prises en charge pour l'évaluation des vulnérabilités 1394

Solutions Microsoft et tiers prises en charge pour l'évaluation des vulnérabilités 1391

Sources de données prises en charge 568

Startup Recovery Manager 1012

Statut d'installation des correctifs 355

Statut de l'activité de validation 264

Statut de la menace 342

Statut de validation 263

Statut réseau des ressources 345

Stockage d'archives 1624

Stockage de sauvegarde 731

Stockage géoredondant 1622

Stockage immuable 1617

Stockage immuable pour l'archivage des e-mails 802

Stockages et agents pris en charge 1618

Stocker les événements de sécurité pendant 180 jours 1254

Stratégie de cycle de vie 1627

Stratégie de rétention 1626

Structure d'autostart.json 998

Structure de la règle de flux de données 1585

Structure de règle 1586

Suivi de la géolocalisation 1512

Suivi des blocs modifiés (CBT) 616, 966

Support de démarrage basé sur Linux ou sur WinPE/WinRE ? 990

Support de démarrage basé sur un environnement Linux 992

Support de démarrage basé sur Windows 1001

Support de démarrage personnalisé ou tout prêt ? 990

Support pour la migration d'une machine virtuelle 975

Suppression automatique des environnements clients non utilisés sur un site dans le Cloud 1021

Suppression d'identifiants 1483

Suppression d'un groupe 446

Suppression d'un plan d'archivage 778

Suppression d'un plan de protection 250

Suppression d'un plan de sauvegarde 911

Suppression d'un serveur de messagerie 774

Suppression d'une connexion à un cloud public 770

Suppression d'une organisation Microsoft 365 856

Suppression d'une règle de rétention 794

Suppression d'un serveur de restauration 1131

Suppression d'un workflow 1237

Suppression d'une version de workflow 1241

Suppression de l'accès à un abonnement Microsoft Azure 764

Suppression de l'appliance virtuelle de l'agent pour Azure 167

Suppression de la machine 959

Suppression de packages logiciels 1438

Suppression de plans des favoris 236

Suppression de ressources d'un plan de gestion à distance 1478

Suppression de ressources de la console Cyber Protect 403

© Acronis International GmbH, 2003-2026

Suppression de ressources de plans de déploiement de logiciels 1456

Suppression de sauvegardes 737

Suppression de serveurs DNS personnalisés 1063

Suppression de toutes les alertes 367

Suppression des compartiments 1631

Suppression des modèles de référence 1374

Suppression des plans par défaut 233

Suppression des références d'un modèle 1372

Suppression des références des tenants 1367

Suppression des sauvegardes en dehors de la console Cyber Protect 739

Suppression douce des tenants disposant d'un site de reprise d'activité après sinistre dans Microsoft Azure 1158

Suppression du plan SIEM 285

Suppression du site de reprise d'activité après sinistre 1110

Suppression du site DR à partir de Microsoft Azure 1120

Supprimer la règle de conservation légale 798

Sur quels agents, ressources et emplacements de sauvegarde les goulots d'étranglement sont-ils affichés ? 744

Surveillance 298, 338

Surveillance basée sur une anomalie 1524

Surveillance de l'intégrité du disque 346

Surveillance de l'intégrité et des performances de la ressource 1523

Surveillance de l'utilisation 1220

Surveillance des références des tenants 1351

Surveillance des ressources par transmission de captures d'écran 1498

Surveillance étendue 1254

Syntaxe 1272

Systèmes d'exploitation et environnements pris en charge pour la sauvegarde et la restauration 513

Systèmes d'exploitation et versions pris en charge 27

Systèmes d'exploitation pris en charge 1017, 1112

Systèmes d'exploitation pris en charge pour la protection antivirus et antimalware 1164

Systèmes d'exploitation pris en charge pour le bureau à distance et l'assistance 1463

Systèmes d'exploitation Windows compatibles 1212

Systèmes de fichiers pris en charge 539

T

Tableau de bord de sensibilisation 1633

Tableau de bord Reprise d'activité après sinistre 1159

Tableau de bord Vue d'ensemble 298

Téléchargement d'adresses MAC 1064

Téléchargement d'agents de protection 47

Téléchargement d'un rapport de licence pour l'archivage des e-mails 774

Téléchargement de données pour les ressources récemment affectées 358

Téléchargement de fichiers dans la console Web Restore 709

Téléchargement de pièces jointes 802

Téléchargement des fichiers journaux VPN IPsec 1051

Téléchargement des journaux de l'appliance VPN 1065

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Téléchargement des journaux de la passerelle VPN 1065

Téléchargement du programme d'installation 173

Télécharger le résultat d'une opération de création de scripts 502

Téléchargez la configuration pour OpenVPN 1055

Temps moyen de réparation des incidents de sécurité 343

Tenants en mode de Conformité 713

Terminaux découverts 341

Terminaux éligibles à la reprise d'activité après sinistre 1159

Terminaux mobiles pris en charge 840

Test d'un réplica 963

Test du fonctionnement de la fonctionnalité EDR (Endpoint Detection and Response) 1341

Tient dans l'intervalle de temps 583

Traitement de l'échec de tâche 658

Transfert audio 1464

Transfert de fichiers 1489

Transfert de fichiers via Acronis Assistance rapide 1504

Transfert de packages logiciels 1434

Travail avec Disaster Recovery vers Cyber Protect Cloud 1022

Travail avec les références 1351

Travailler avec Disaster Recovery vers Microsoft Azure 1114

Tri des alertes 304

Tri des e-mails 783

Troncation de journal 638

Type de contrôle 999

Types d'analyses 1168

Types d'événements 1276

Types d'événements et champs 1276

Types de filtres de fichiers 621

Types de machine virtuelle pris en charge 269

Types de ressources 407

Types de sauvegarde 573

Types de surveillance 1523

Types et catégories d'alertes 305

U

Universal Restore sous Linux 721

Universal Restore sous Windows 719

Utilisateurs déconnectés 582

Utilisation d'un compte d'administrateur de projet 150

Utilisation d'un compte d'administrateur système 148

Utilisation d'un stockage localement connecté 970

Utilisation de caractères génériques pour définir des exclusions 395

Utilisation de comptes gMSA avec l'agent Cyber Protection 68

Utilisation de l'intelligence artificielle générative (visites par client) 352

Utilisation de l'intelligence artificielle générative (visites par terminal) 352

Utilisation de la barre d'outils dans la fenêtre de la visionneuse 1505

Utilisation de la console Cyber Protect au niveau Tous les clients 388

© Acronis International GmbH, 2003-2026

Utilisation de mots de passe comportant des caractères spéciaux ou des espaces vides 116

Utilisation de plans 216

Utilisation de ressources agrégées 480

Utilisation de ressources CyberApp 479

Utilisation de variables 612

Utilisation de variables pour définir des exclusions 396

Utilisation de workflows automatisés 1333

Utilisation des journaux 1064

Utilisation des points de calcul 1162

Utilisation des référentiels de logiciels et des packages logiciels 1429

Utilisation des requêtes enregistrées 1271

Utilisation des ressources gérées 1484

Utilisation des ressources non gérées 1502

Utilisation du contrôle des terminaux 451

Utilisation du graphique XDR 1244

Utilisation du mode d'application adaptative pour le renouvellement d'une règle utilisateur 1592

Utilisation du mode d'observation pour le renouvellement d'une règle utilisateur 1591

Utilisation du module de contrôle des terminaux 448

Utilisation du service de formation et de sensibilisation à la sécurité 1633

Utilité de la fonctionnalité EDR (Endpoint Detection and Response) 1251

Utilité de la fonctionnalité XDR (Extended Detection and Response) 1242

V

Valeurs de filtre de fichier 621

Valeurs du champ Action 474

Validation 259

Validation de la sauvegarde 615, 723

Validation des sauvegardes 736

Variables des alertes de surveillance 1572

Vérification de l'authenticité d'un fichier grâce à Notary Service 710, 940

Vérification de l'intégrité 1160

Vérification de la taille d'un index de recherche 943

Vérification de vos notifications 26

Vérification des activités de pare-feu dans le Cloud 1081

Vérification des détails sur une menace détectée 870

Vérification du statut de validation 263

Vérifier l’adresse IP du terminal 586

Vérifiez l'accès aux pilotes dans l'environnement de démarrage 719

Verrouillage d’objet 1625

Verrouillage de la rétention 538

Version d'évaluation Disaster Recovery 1020

Versions 1625

Versions de MariaDB prises en charge 526

Versions de Microsoft SharePoint prises en charge 525

Versions de Microsoft SQL Server prises en charge 524

Versions de MySQL prises en charge 526

Versions de Windows prises en charge 1430

© Acronis International GmbH, 2003-2026

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Versions de workflow 1237

Versions du script 500

Versions Microsoft Exchange Server compatibles 524

Versions Oracle Database prises en charge 525

Versions prises en charge 901

Versions SAP HANA prises en charge 525

Virtuozzo Hybrid Infrastructure 537

Virtuozzo Hybrid Server 536

Visualisation d'une version de workflow 1238

Visualisation de l'historique d'exécution d'un workflow 1236

Visualisation des alertes de surveillance pour une ressource 1578

Visualisation des compartiments 1629

Visualisation des données des moniteurs 1580

Visualisation des ressources de clients spécifiques 389

Visualisation facile à comprendre du scénario de l'attaque 1253

Vitesse de sortie au cours de la sauvegarde 649

VMware (Broadcom) 526

Vue d'ensemble 26

Vue d'ensemble dans le tableau de bord 1254

Vulnérabilités existantes 355

W

Widget d'inventaire du logiciel 359

Widget de carte de protection des données 352

Widget Sessions distantes 363

Widget Terminaux découverts 353

Widgets d'alerte 339

Widgets d'évaluation des vulnérabilités 354

Widgets d'installation de logiciels 360

Widgets d'installation des correctifs 355

Widgets d'inventaire du matériel 362

Widgets Data Loss Prevention dans le tableau de bord Vue d'ensemble 1605

Widgets de basculement 1132

Widgets de désinstallation des logiciels 361

Widgets de Endpoint Detection and Response (EDR) 341

Widgets de l'état de santé du disque 347

Widgets de logiciels 359

Widgets de moniteurs 1581

Widgets de protection de l'intelligence artificielle générative 350

Windows 554

Workflow Gestion des correctifs 1402

Workflows Endpoint Detection and Response (EDR) 1334

X

XDR (Extended Detection and Response) 1242

© Acronis International GmbH, 2003-2026