Acronis

acronis.com

Acronis Cyber Protect 15

Update 6

Guide de l'utilisateur

RÉVISION : 15/06/2023

Table des matières

Déclaration de copyright

Technologies Acronis brevetées

Les technologies utilisées dans ce produit sont couvertes et protégées par un ou plusieurs brevets américains : 7 047 380 ; 7 246 211 ; 7 275 139 ; 7 281 104 ; 7 318 135 ; 7 353 355 ; 7 366 859 ; 7 383 327 ; 7 475 282 ; 7 603 533 ; 7 636 824 ; 7 650 473 ; 7 721 138 ; 7 779 221 ; 7 831 789 ; 7 836 053 ; 7 886 120 ; 7 895 403 ; 7 934 064 ; 7 937 612 ; 7 941 510 ; 7 949 635 ; 7 953 948 ; 7 979 690 ; 8 005 797 ; 8 051 044 ; 8 069 320 ; 8 073 815 ; 8 074 035 ; 8 074 276 ; 8 145 607 ; 8 180 984 ; 8 225 133 ; 8 261 035 ; 8 296 264 ; 8 312 259 ; 8 347 137 ; 8 484 427 ; 8 645 748 ; 8 732 121 ; 8 850 060 ; 8 856 927 ; 8 996 830 ; 9 213 697 ; 9 400 886 ; 9 424 678 ; 9 436 558 ; 9 471 441 ; 9 501 234 ; et d'autres demandes de brevet déposées.

Éditions Acronis Cyber Protect 15

Acronis Cyber Protect 15 est disponible dans les éditions suivantes :

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

Pour obtenir des informations détaillées sur les fonctionnalités incluses dans chaque édition, consultez la section Comparaison des éditions Acronis Cyber Protect 15 incluant le déploiement dans le cloud.

Toutes les éditions de Acronis Cyber Protect 15 sont sous licence en fonction du nombre de charges de travail protégées et de leur type (poste de travail, serveur et hôte virtuel). Les éditions de Cyber Protect sont disponibles uniquement avec des licences d'abonnement. Les éditions Cyber Backup sont disponibles à la fois avec des licences par abonnement et avec des licences perpetuelles. Pour plus d'informations sur les options disponibles, reportez-vous à "Licence" (p. 22).

Les clés de licence perpétuelle pour la version 15 ne peuvent pas être utilisées avec les agents de sauvegarde d'Acronis Cyber Backup 12.5. Toutefois, ces agents continueront à fonctionner avec leur ancienne licence, même si leur serveur de gestion est mis à niveau à la version 15.

Les licences d'abonnement de sauvegarde peuvent être utilisées avec les agents de la version 12.5, même lorsque les agents sont mis à niveau à la version 15. Les licences d'abonnement Cyber Protect ne peuvent être utilisées que par les agents de la version 15.

Les agents de sauvegarde de la version 12.5 qui sont enregistrés sur un serveur de gestion version 15 ne peuvent pas réaliser d'opérations de traitement des données hors hôte, telles que la réplication de sauvegarde, la validation de sauvegarde, le nettoyage ou la conversion vers une machine virtuelle.

Remarque
Les fonctionnalités entre les différentes éditions varient. Certaines des fonctionnalités décrites dans cette section peuvent être indisponibles avec votre licence. Pour obtenir des informations détaillées sur les fonctionnalités incluses dans chaque édition, consultez la section Comparaison des éditions Acronis Cyber Protect 15 incluant le déploiement dans le cloud.

Fonctionnalités Cyber Protect prises en charge par système d'exploitation.

Les fonctionnalités de Cyber Protect sont prises en charge sur les systèmes d'exploitation suivants :

- Windows : Windows 7 et versions ultérieures, Windows Server 2008 R2 et versions ultérieures.
  La gestion de l'antivirus Windows Defender est prise en charge sur Windows 8.1 et versions ultérieures.
- Linux : CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.
  Il se peut que d'autres distributions et versions de Linux prennent également en charge les fonctionnalités Cyber Protect, mais elles n'ont pas été testées.
- macOS : 10.13.x et versions ultérieures (seule la protection contre les virus et les malwares est prise en charge).

Important
Les fonctionnalités de Cyber Protect ne sont prises en charge que pour les machines sur lesquelles un agent de protection est installé. Pour les machines virtuelles protégées en mode sans agent, par exemple par l'agent pour Hyper-V, l'agent pour VMware ou l'agent pour Scale Computing, seule la sauvegarde est prise en charge.

Cyber Protect fonctionnalités	Windows	Linux	macOS
Données d'investigation	Oui	Non	Non
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
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 périphériques	Oui	Non	Non
Protection Acronis contre les malwares			
Détection des ransomwares basée sur un comportement de processus (basé sur l'IA)	Oui	Non	Non
Détection de processus de cryptominage	Oui	Non	Non
Protection contre les malware en temps réel	Oui	Non	Oui
Restauration automatique de fichiers affectés depuis	Oui	Non	Non

le cache local			
Autoprotection pour les fichiers de sauvegarde Acronis	Oui	Non	Non
Autoprotection pour le logiciel Acronis	Oui	Non	Non
Analyse statique pour les fichiers exécutables portables	Oui	Non	Oui*
Protection des lecteurs externes (HDD, lecteurs flash, cartes SD)	Oui	Non	Non
Protection du dossier réseau	Oui	Non	Non
Protection côté serveur	Oui	Non	Non
Protection de Zoom, WebEx, Microsoft Teams et d'autres outils de travail à distance	Oui	Non	Non
Analyse anti-malware à la demande	Oui	Non	Oui
Analyser les fichiers d'archive	Oui	Non	Oui
Exclusions de fichier/dossier	Oui	Non	Oui**
Exclusions des processus	Oui	Non	Non
Liste blanche à l'échelle de l'entreprise	Oui	Non	Oui
Détection des comportements	Oui	Non	Non
Quarantaine	Oui	Non	Oui
Filtrage d'URL (http/https)	Oui	Non	Non
Gestion de l'antivirus Windows Defender	Oui	Non	Non
Gestion de Microsoft Security Essentials	Oui	Non	Non
Évaluation des vulnérabilités			
Évaluation des vulnérabilités du système d'exploitation et de ses applications natives	Oui	Oui**	Non
Évaluation des vulnérabilités pour les applications tierces	Oui	Non	Non
Gestion des correctifs			
Approbation manuelle des correctifs	Oui	Non	Non

Installation manuelle des correctifs	Oui	Non	Non
Planification de l'installation automatique de 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'un ordinateur si une sauvegarde est en cours d'exécution	Oui	Non	Non
Carte de la protection des données			
Analyse des machines pour trouver des fichiers non protégés	Oui	Non	Non
Aperçu des emplacements non protégés	Oui	Non	Non
Action protectrice dans la carte de la protection des données	Oui	Non	Non
État de santé du disque			
Contrôle de l'état de santé des HDD et SSD basés sur l'IA	Oui	Non	Non
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
Analyse de la sauvegarde			
Analyse des sauvegardes chiffrées	Oui	Non	Non
Analyse des sauvegardes de disque dans le stockage local, les partages réseau et le stockage Acronis Cloud Storage	Oui	Non	Non
Restauration sûre			
Analyse anti-malwares avec protection Acronis contre les virus et les malwares lors du processus de restauration	Oui	Non	Non
Bureau à distance			
Connexion via un client basé sur HTML5	Oui	Non	Non

Connexion via un client RDP Windows natif	Oui	Non	Non
Effacement à distance	Oui****	Non	Non
Moniteur Cyber Protect	Oui	Non	Oui

* Sous macOS, l'analyse statique pour les fichiers exécutables portables est prise en charge uniquement pour les analyses planifiées.

** Sous macOS, les exclusions vous permettent uniquement de spécifier les fichiers et les dossiers qui ne seront pas analysés par la protection en temps réel ni par les analyses planifiées.

*** 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, entre autres.

**** L'effacement à distance est uniquement disponible pour les machines exécutant Windows 10 ou une version ultérieure.

Licence

Pour protéger une charge de travail unique à l'aide de Acronis Cyber Protect, il vous faut une licence. Une licence n'est pas requise pour l'installation de Acronis Cyber Protect.

Types de licence

Acronis Cyber Protect est disponible avec des licences par abonnement. Au cours de la période de validité, qui commence à partir de la date d'achat, vous bénéficiez de mises à jour illimitées et d'une assistance technique gratuite. Une fois la période de validité terminée, les plans de protection existants cessent de fonctionner et aucun nouveau plan de protection ne peut être créé.

Des renouvellements des anciennes licences perpétuelles sont disponibles. Certaines fonctionnalités, telles que le déploiement dans le cloud ou les sauvegardes cloud à cloud ne sont pas disponibles avec une licence perpétuelle.

Une licence d'évaluation est également disponible. Elle vous fournit un accès à toutes les fonctionnalités du produit pendant 30 jours à partir de l'activation de la licence.

Pour en savoir plus sur les différentes options de licence, consultez Acronis Cyber Protect 15 : questions fréquentes concernant les licences et les mises à niveau/rétrogradations dans notre base de connaissances. Les règles de licence de Acronis sont disponibles sur https://www.acronis.com/company/licensing.html.

Important
Acronis Cyber Protect 15 Update 3 a introduit un nouveau modèle de licences. Il nécessite l'enregistrement des licences et leur activation sur les serveurs de gestion sur site.

Licences dans Acronis Cyber Protect 15 Update 3 et versions ultérieures

Dans Acronis Cyber Protect 15 Update 3 et versions ultérieures, aucune clé de licence n'est ajoutée dans la console locale du serveur de gestion (`https://<adresse IP de votre serveur de gestion>:<port>`).

Au lieu de cela, vous ajoutez les licences à votre compte dans le portail client Acronis (`https://account.acronis.com`) puis vous les gérez dans la console cloud Acronis Cyber Protect (`https://cloud.acronis.com`).

La gestion des licences d'un serveur de gestion hors ligne requiert des opérations à la fois dans les consoles locales et cloud.

Pour en savoir plus sur les consoles locales et cloud, consultez "Compte Acronis, consoles locales et cloud" (p. 24).

Pour commencer à utiliser un serveur de gestion avec Acronis Cyber Protect 15 Update 3 et versions ultérieures

1. Ajoutez une ou plusieurs licences à votre compte dans le portail client Acronis (https://account.acronis.com).
   Les licences achetées en ligne sont automatiquement ajoutées à ce compte.
2. [Pour le mode de déploiement sur site] Activez votre serveur de gestion.
3. Allouez une licence au serveur de gestion.

Types de serveur de gestion

En fonction de vos modes de déploiement, vous pouvez utiliser les types de serveur de gestion suivants :

- Serveur de gestion Cloud
- Serveur de gestion sur site
  - Serveur de gestion sur site
  - Serveur de gestion hors ligne

Vous pouvez avoir plus d'un serveur de gestion dans votre compte Acronis. Vous pouvez également utiliser un mode de déploiement mixte avec un serveur de gestion cloud et un serveur de gestion sur site.

Si vous utilisez plusieurs serveurs de gestion, vous pouvez répartir un quota de licences entre eux. Pour en savoir plus sur la façon de procéder, consultez "Transférer un quota de licence à un autre serveur de gestion" (p. 34).

Serveur de gestion Cloud

Avec le déploiement dans le cloud, vous n'installez et n'entretenez pas de serveur de gestion dans votre réseau. Vous utilisez un serveur de gestion déjà déployé dans un centre de données Acronis et vous n'avez qu'à installer les agents de protection pour vos charges de travail.

Le serveur de gestion cloud ne requiert pas d'activation. Il est toujours en ligne et les informations concernant la licence sont automatiquement synchronisées entre le serveur et votre compte Acronis.

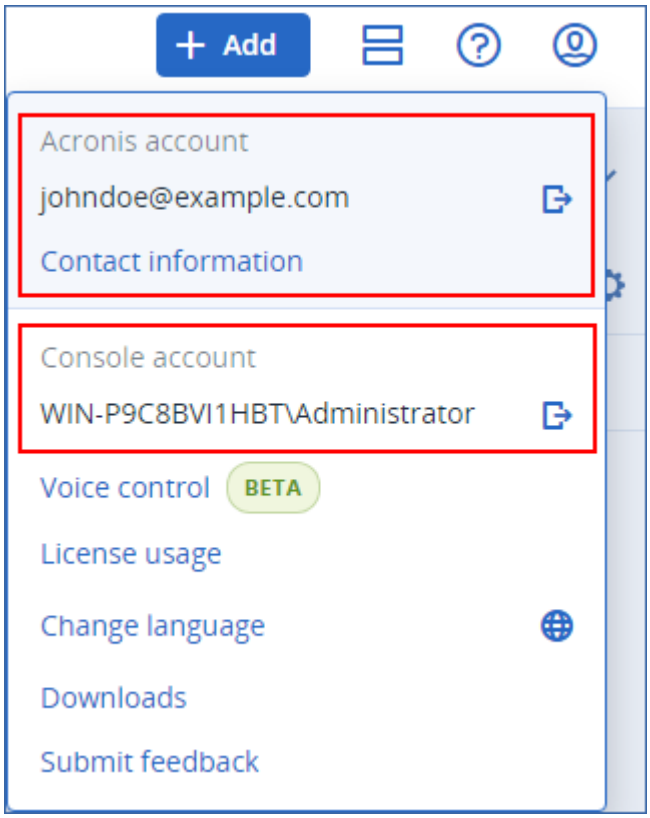
Serveur de gestion sur site

Avec un déploiement sur site, vous installez le serveur de gestion aussi bien que les agents de protection dans votre réseau. Vous pouvez avoir un serveur de gestion hors ligne, non connecté à Internet, ou avoir un serveur de gestion en ligne, qui accès à Internet.

Les serveurs de gestion sur site nécessitent une activation. Pour plus d'informations sur l'activation, consultez "Activer un serveur de gestion" (p. 28).

Remarque

Deux comptes s'affichent dans la console locale d'un serveur de gestion sur site activé : le compte Acronis, utilisé pour synchroniser les informations de licence, et le compte de console, utilisé pour accéder à la console locale en elle-même.



Serveur de gestion sur site en ligne

Vous activez un serveur de gestion en ligne via Internet, en vous connectant à votre compte Acronis quand vous accédez à la console locale pour la première fois.

Serveur de gestion sur site hors ligne

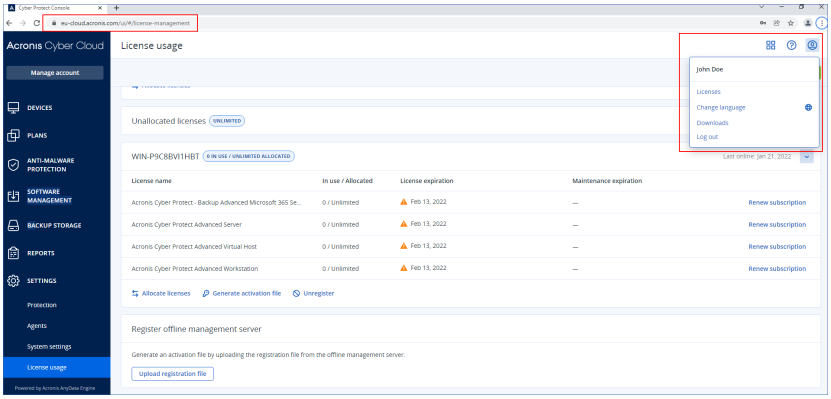
Vous activez un serveur de gestion hors ligne et synchronisez manuellement les informations concernant la licence vers votre compte Acronis via un fichier.

Compte Acronis, consoles locales et cloud

Pour utiliser Acronis Cyber Protect et gérer vos licences ainsi que leur utilisation, vous avez besoin d'un compte Acronis. Toutes vos licences et tous vos serveurs de gestion sont inscrits sur ce compte.

Grâce à ce compte, vous pouvez accéder aux consoles suivantes :

- console cloud (`https://cloud.acronis.com`)

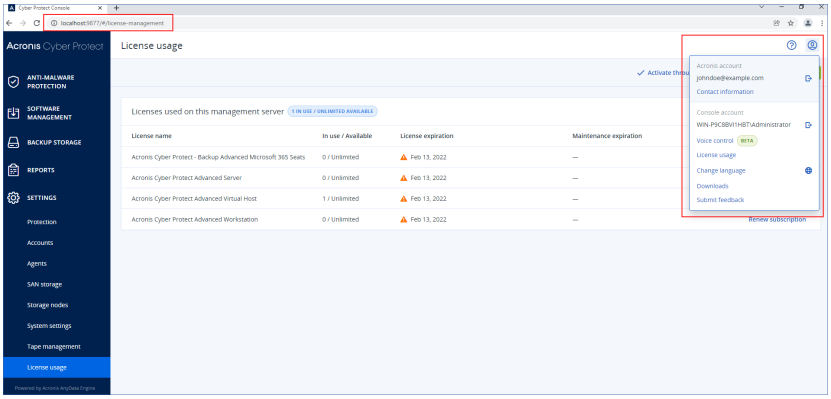


Remarque

Après votre connexion à la console cloud, son URL change et affiche le centre de données exact auquel appartient votre compte. Par exemple, `https://eu-cloud.acronis.com` ou `https://jp-cloud.acronis.com`.

La console cloud est le principal emplacement où vous pourrez gérer vos licences. Ici, dans l'onglet **Paramètres** > **Utilisation de licences**, vous pouvez allouer des licences et un quota de licences disponibles à un serveur de gestion spécifique, réallouer des quotas de licence à un autre serveur de gestion, ou finaliser l'inscription d'un serveur de gestion hors ligne.

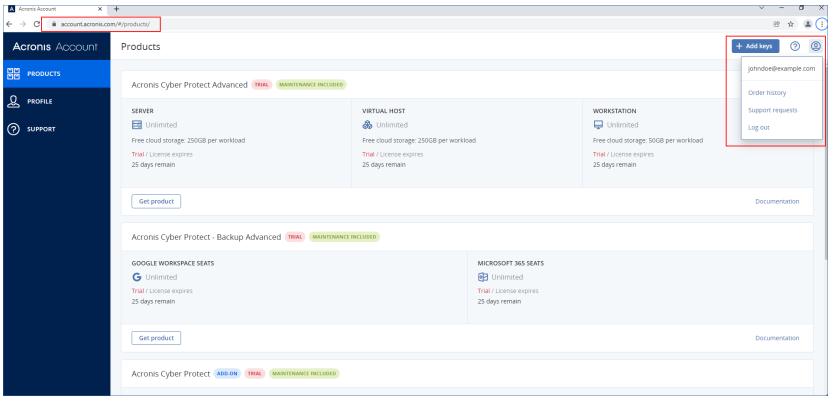
- Console locale d'un serveur de gestion sur site (`https://<adresse IP de votre serveur de gestion>:<port>`)



Ici, vous pouvez consulter les licences allouées, leur quota et leur utilisation, ainsi que leur date d'expiration.

Vous utilisez la console locale, de même que la console cloud, quand vous activez un serveur de gestion hors ligne ou que vous y allouez des licences.

- Portail client Acronis (`https://account.acronis.com`)



Dans le portail client Acronis, vous pouvez gérer les produits que vous avez achetés, par exemple en vérifiant la date d'expiration de vos abonnements, en ajoutant de nouvelles clés de licence, en inscrivant les renouvellements de licence ou en demandant une mise à niveau. Vous pouvez également contacter l'équipe d'assistance, télécharger les fichiers d'installation du produit et accéder à la documentation du produit.

Gestion des licences

Le tableau ci-dessous résume les opérations disponibles et montre où les réaliser.

Opération	Emplacement
Ajouter des licences à votre compte	Vous ajoutez des licences dans le portail client Acronis (`https://account.acronis.com`). Les licences achetées en ligne sont automatiquement ajoutées à cet endroit.
Activer un serveur de gestion	Vous activez un serveur de gestion en l'inscrivant dans votre compte. Vous activez des serveurs de gestion dans leur console locale (`https://<adresse IP de votre serveur de gestion>:<port>`) en vous connectant à votre compte Acronis. L'activation d'un serveur de gestion hors ligne requiert des opérations à la fois dans les consoles locales et cloud.
Allouer des licences à un serveur de gestion Modifier une allocation de licences existante	Sur les serveurs de gestion en ligne, vous allouez des licences à l'aide de la console cloud (`https://cloud.acronis.com`). Les licences allouées sont automatiquement synchronisées avec le serveur de gestion. Sur les serveurs de gestion hors ligne, vous allouez des licences au moyen d'un fichier d'activation. Cette procédure nécessite que vous utilisiez à la fois la console locale du serveur de gestion (`https://<adresse IP de votre serveur de gestion>:<port>`) et la console cloud (`https://cloud.acronis.com`).
Affecter des licences aux charges de travail	Cette opération est automatique.

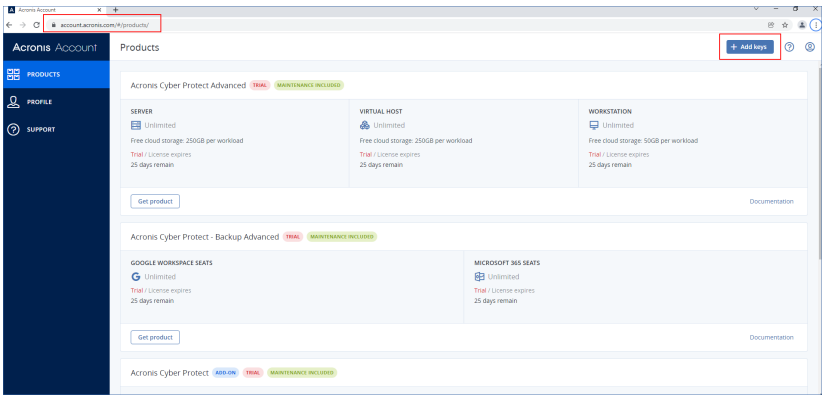
Opération	Emplacement
Désinscrire un serveur de gestion de votre compte	Vous désinscrivez les serveurs de gestion en ligne à l'aide de la console cloud (`https://cloud.acronis.com`). Vous désinscrivez les serveurs de gestion hors ligne au moyen d'un fichier de désactivation. Cette procédure nécessite que vous utilisiez à la fois la console locale du serveur de gestion hors ligne (`https://<IP address of your management server>:<port>`) et la console cloud (`https://cloud.acronis.com`). Pour désinscrire un serveur de gestion hors ligne auquel vous n'avez pas accès, vous utilisez uniquement la console cloud.

Ajouter des licences à votre compte Acronis

Pour utiliser une licence, vous devez l'ajouter à votre compte Acronis. Les licences achetées en ligne sont automatiquement ajoutées à votre compte. Vous devez ajouter manuellement les licences achetées hors ligne.

Pour ajouter une licence à votre compte Acronis

1. Connectez-vous au portail client Acronis (`https://account.acronis.com`) à l'aide de vos identifiants de compte Acronis.
2. Dans le menu de navigation, cliquez sur **Produits**.
3. Cliquez sur **Ajouter des clés**.



4. Saisissez une ou plusieurs clés de licence, une par ligne, puis cliquez sur **Ajouter**.

> **Remarque**
> Vous pouvez saisissez jusqu'à 100 clés de licence à la fois.

Les licences sont alors ajoutées à votre compte et vous pouvez gérer leur utilisation dans la console cloud (`https://cloud.acronis.com`).

Important
Avant la mise à niveau vers Acronis Cyber Protect 15 Update 3, exportez les licences perpétuelles stockées localement vers un fichier, puis ajoutez-les à votre compte Acronis.

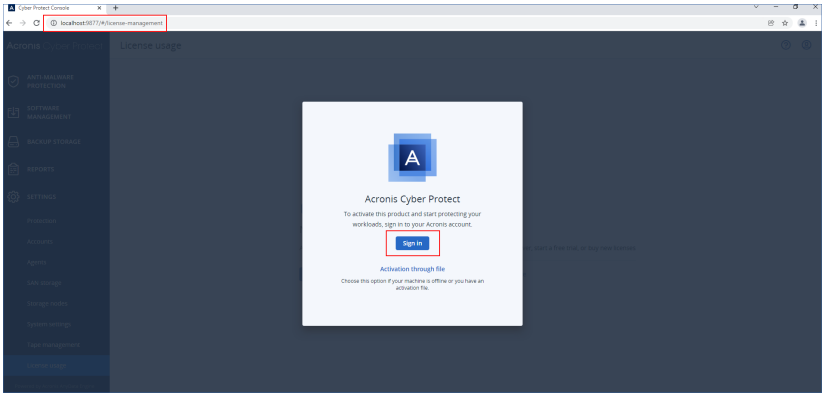
Pour vérifier les clés de licence saisies localement sur un serveur de gestion, accédez à `https://<adresse IP de votre serveur de gestion>:<port>/api/account_server/v2/licensing/legacy/license_keys`.

Activer un serveur de gestion

Vous activez un serveur de gestion en l'inscrivant dans votre compte Acronis.

Pour activer un serveur de gestion en ligne

1. Après avoir installé un serveur de gestion Acronis Cyber Protect, ouvrez sa console locale (`https://<adresse IP de votre serveur de gestion>:<port>`).
2. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Se connecter**.



3. Connectez-vous à votre compte Acronis.

Par conséquent, le serveur de gestion est automatiquement inscrit et activé.

Pour commencer à protéger vos ressources, allouez au moins une licence à ce serveur. Pour en savoir plus sur la façon d'allouer une licence, reportez-vous à "Allouer des licences à un serveur de gestion" (p. 31).

Remarque
Les serveurs de gestion en ligne nécessitent une connexion Internet pour synchroniser les informations de licence avec votre compte Acronis. Si un tel serveur reste hors ligne pendant plus de 30 jours, ses plans de protection cesseront de fonctionner et vos ressources ne seront plus protégées.

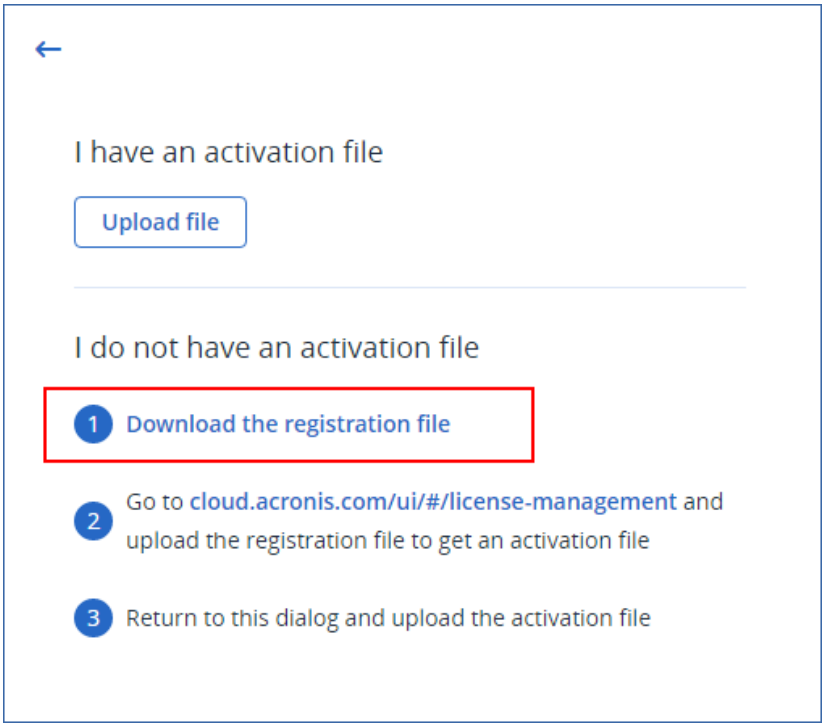
Si vous vous déconnectez de votre compte Acronis dans la console locale, les informations de licence ne pourront pas être synchronisées. Si vous ne vous reconnectez pas dans les 30 jours, les plans de protection cesseront de fonctionner et vos charges de travail ne seront plus protégées.

Pour activer un serveur de gestion hors ligne

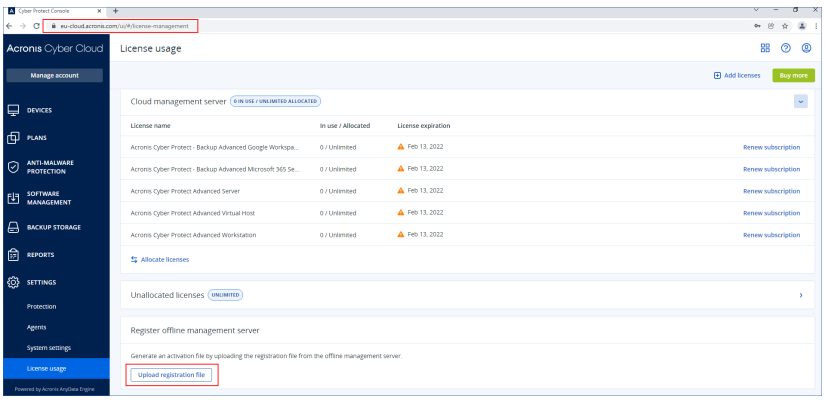
L'activation d'un serveur de gestion hors ligne requiert des opérations à la fois dans les consoles locales et cloud.

Pour accéder à la console cloud, vous avez besoin d'un second ordinateur connecté à Internet.

1. Après avoir installé un serveur de gestion Acronis Cyber Protect, ouvrez sa console locale (`https://<adresse IP de votre serveur de gestion>:<port>`).
2. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Activation au moyen d'un fichier**.
3. Sous **Je ne dispose pas d'un fichier d'activation**, cliquez sur **Téléchargez le fichier d'inscription**.



   Le fichier d'inscription est téléchargé sur votre ordinateur.
4. Sur un ordinateur ayant accès à Internet, connectez-vous à la console cloud (`https://cloud.acronis.com`), puis accédez à **Paramètres** > **Utilisation de licences**.
5. Dans la section **Inscrire le serveur de gestion hors ligne**, cliquez sur **Transférer le fichier d'inscription**.



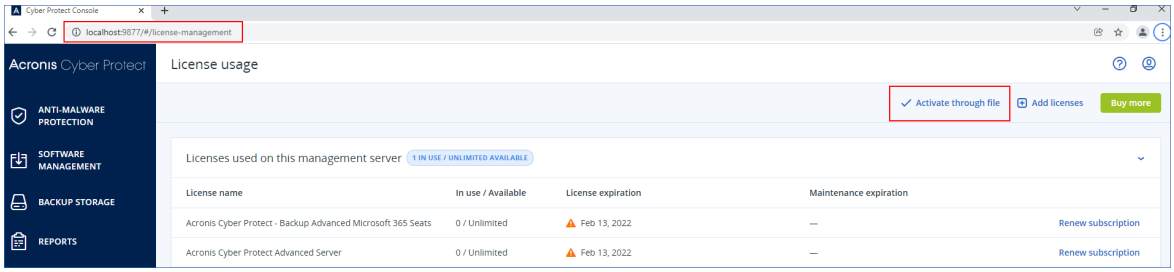
6. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Parcourir** et sélectionnez le fichier d'inscription que vous avez téléchargé dans le serveur de gestion hors ligne.
7. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Télécharger le fichier**.
   Un fichier d'activation est téléchargé sur votre ordinateur.

Important
Si ce serveur de gestion hors ligne est le seul serveur de gestion de votre environnement, les licences de votre compte Acronis lui seront automatiquement allouées. Le fichier d'activation contiendra ces informations, aucune autre allocation n'est donc nécessaire.

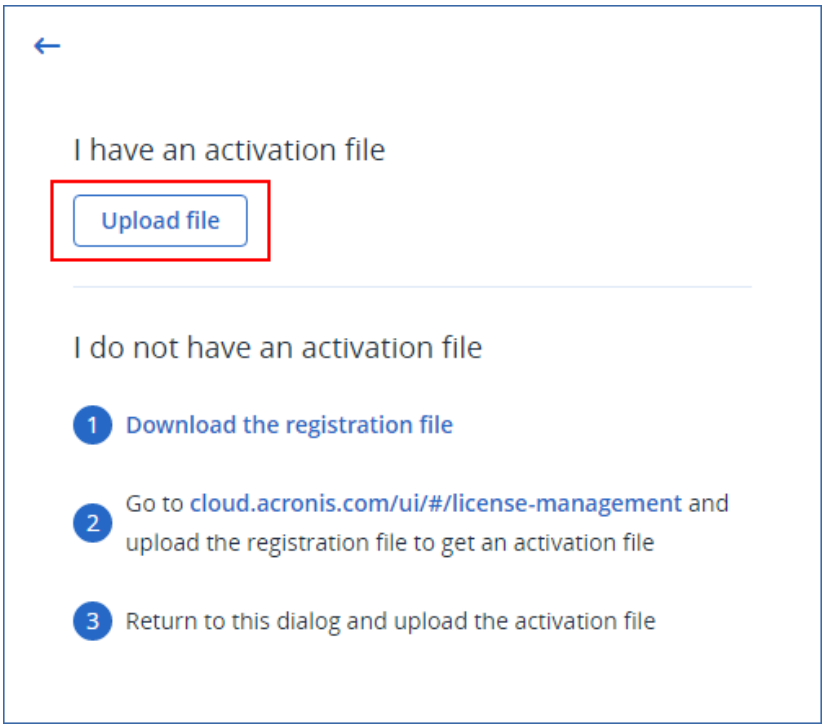
S'il ne s'agit pas du seul serveur de gestion de votre environnement, une fois l'activation effectuée, vous devez allouer des licences en suivant la procédure indiquée dans "Allouer des licences à un serveur de gestion" (p. 31).

8. Dans la console locale du serveur de gestion hors ligne (`https://<adresse IP de votre serveur de gestion>:<port>`), accédez à la boîte de dialogue **Activation au moyen d'un fichier**.

Remarque
Si la boîte de dialogue **Activation au moyen d'un fichier** n'est pas ouverte, accédez à **Paramètres** > **Utilisation de licences**, puis cliquez sur **Activer au moyen d'un fichier**.



9. Sous **Je dispose d'un fichier d'activation**, cliquez sur **Télécharger le fichier**, puis sélectionnez le fichier d'activation que vous avez téléchargé depuis la console cloud.



Par conséquent, le serveur de gestion hors ligne est inscrit dans votre compte Acronis et activé.

Remarque
Vous pourriez ne pas être en mesure d'activer un serveur de gestion exécuté sur une machine virtuelle dont l'UUID n'est pas unique. L'UUID d'une machine virtuelle pourrait être dupliqué lors du clonage ou de la conversion à l'aide de VMware vCenter Converter, par exemple. Si vous rencontrez un problème similaire, contactez notre équipe de support.

Pour plus d'informations sur la manière d'empêcher la duplication de l'UUID sur les machines virtuelles VMware, consultez Editing a virtual machine with a duplicate UUID.bios (1002403).

Allouer des licences à un serveur de gestion

Pour utiliser une licence, vous devez allouer son quota ou une partie de son quota à un serveur de gestion. Vous pouvez allouer plus d'une licence à un serveur de gestion. Vous pouvez également diviser le quota de licences et allouer différentes parties du quota à différents serveurs de gestion.

Remarque
Si votre compte Acronis contient un seul serveur de gestion, toutes vos licences sont automatiquement allouées à ce serveur. Pour savoir comment allouer à nouveau des licences à un autre serveur de gestion, consultez "Transférer un quota de licence à un autre serveur de gestion" (p. 34).

Si vous possédez plus d'un serveur de gestion dans votre compte Acronis, les nouvelles licences s'affichent sous **Licences non allouées** dans la console cloud (`https://cloud.acronis.com`). Vous devez allouer ces licences manuellement.

Toutes les opérations concernant les licences sont automatiquement synchronisées avec les serveurs de gestion en ligne. Pour synchroniser une modification de l'allocation avec un serveur de gestion hors ligne, créez un nouveau fichier d'activation puis répétez la procédure d'allocation. Pour en savoir plus concernant les différents serveurs de gestion, consultez "Types de serveur de gestion" (p. 23).

Pour allouer des licences à un serveur de gestion en ligne

1. Dans la console cloud (`https://cloud.acronis.com`), cliquez sur **Paramètres** > **Utilisation de licences**.
2. Accédez au serveur de gestion auquel vous souhaitez allouer une licence.
3. Cliquez sur **Allouer les licences**.
4. Dans la boîte de dialogue qui s'ouvre, indiquez la licence et le quota de licence que vous souhaitez allouer à ce serveur.
5. Cliquez sur **Enregistrer**.

Par conséquent, les informations de licence sont automatiquement synchronisées avec le serveur de gestion, et vous pouvez utiliser les licences allouées pour protéger vos charges de travail.

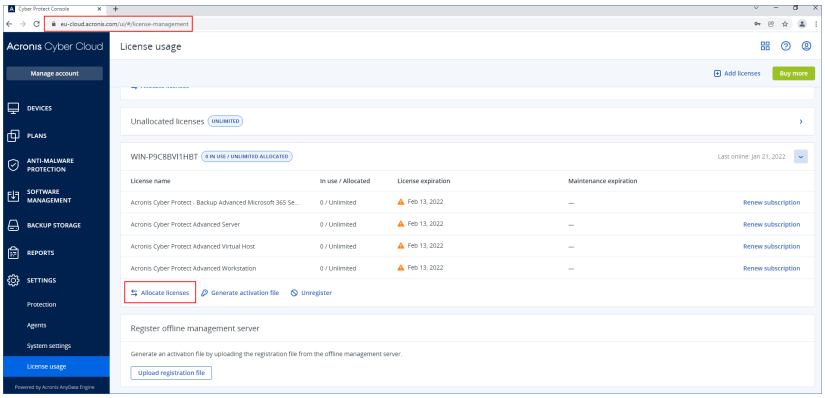
Pour modifier l'allocation, répétez la procédure ci-dessus.

Important
Si le quota de licences modifié est inférieur au nombre d'agents de protection, les agents les moins chargés cesseront de fonctionner. Cette sélection est automatique. Si elle ne correspond pas à vos besoins, réaffectez manuellement les licences disponibles.

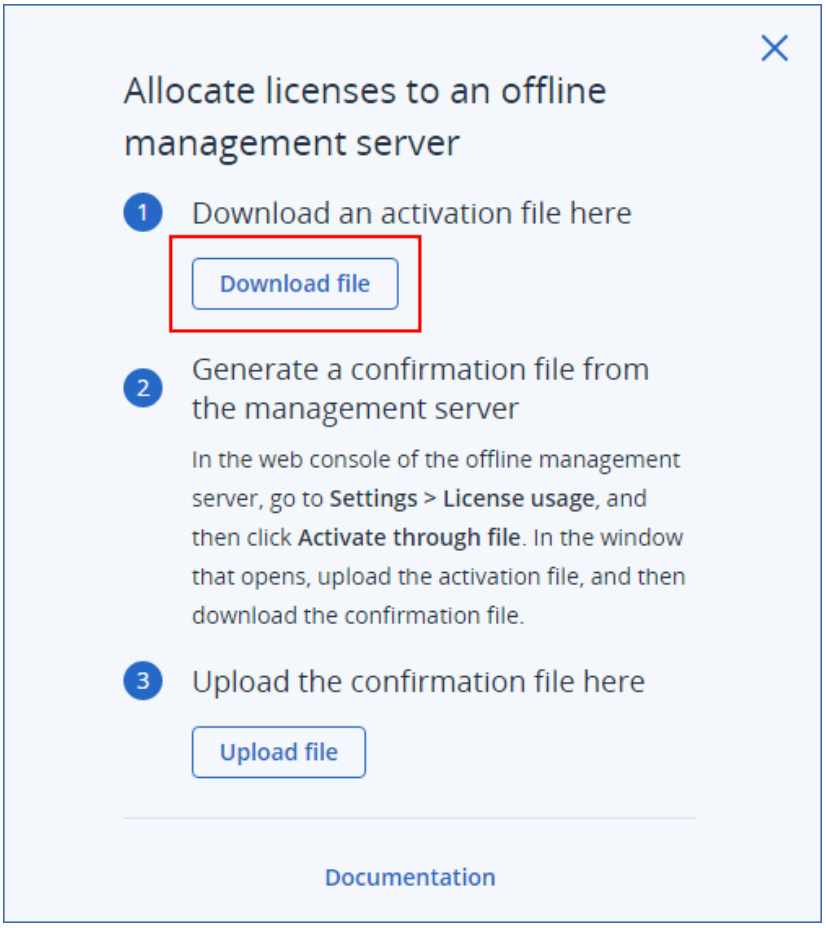
Pour allouer des licences à un serveur de gestion hors ligne

Pour allouer des licences à un serveur de gestion hors ligne, vous devez utiliser aussi bien les consoles cloud que locales. Pour accéder à la console cloud, vous avez besoin d'un second ordinateur connecté à Internet.

1. Sur un ordinateur ayant accès à Internet, connectez-vous à la console cloud (`https://cloud.acronis.com`), puis cliquez sur **Paramètres** > **Utilisation de licences**.
2. Accédez au serveur de gestion auquel vous souhaitez allouer une licence.
3. Cliquez sur **Allouer les licences**.

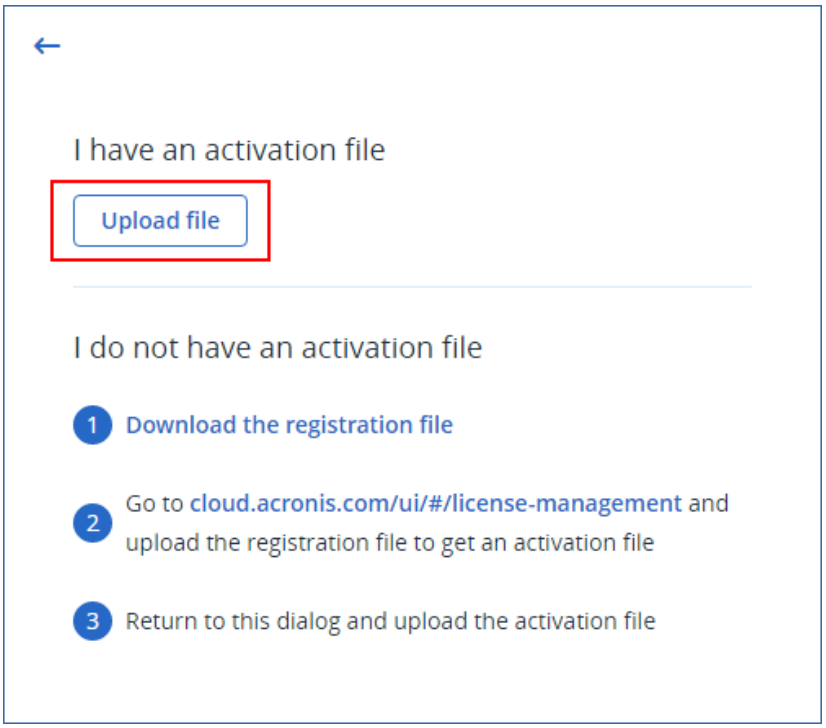


4. Dans la boîte de dialogue qui s'ouvre, indiquez la licence et le quota de licence que vous souhaitez allouer à ce serveur.
5. Cliquez sur **Enregistrer**.
6. Dans la boîte de dialogue **Allouer des licences à un serveur de gestion hors ligne**, cliquez sur **Télécharger le fichier**.



Le fichier d'activation est téléchargé sur votre ordinateur.

7. Dans la console locale du serveur de gestion hors ligne (`https://<adresse IP de votre serveur de gestion>:<port>`), accédez à **Paramètres** > **Utilisation de licences**, puis cliquez sur **Activer au moyen d'un fichier**.
8. Dans la boîte de dialogue qui s'ouvre, sous **Je dispose d'un fichier d'activation**, cliquez sur **Télécharger le fichier**, puis sélectionnez le fichier d'activation que vous avez téléchargé depuis la console cloud.



Par conséquent, les informations de licence sont synchronisées entre votre compte Acronis et le serveur de gestion hors ligne.

Pour augmenter le quota de licences allouées, répétez la procédure ci-dessus.

Pour réduire le quota de licences allouées, reportez-vous à "Diminuer le quota de licence alloué à un serveur de gestion hors ligne" (p. 35).

Transférer un quota de licence à un autre serveur de gestion

Vous pouvez transférer un quota de licences d'un serveur de gestion à un autre. Cette option peut s'avérer utile lorsque les licences allouées à un serveur de gestion ne sont utilisées par aucune charge de travail, et que vous avez besoin de davantage de licences pour un autre serveur de gestion.

Remarque
Si votre compte Acronis contient un seul serveur de gestion, toutes vos licences sont automatiquement allouées à ce serveur.

Si vous possédez plus d'un serveur de gestion dans votre compte Acronis, les nouvelles licences s'affichent sous **Licences non allouées** dans la console cloud (`https://cloud.acronis.com`). Vous devez allouer ces licences manuellement.

Pour transférer un quota de licence à un autre serveur de gestion

1. Réduisez le quota de licences alloué au serveur de gestion d'origine en suivant la procédure dans "Allouer des licences à un serveur de gestion" (p. 31).

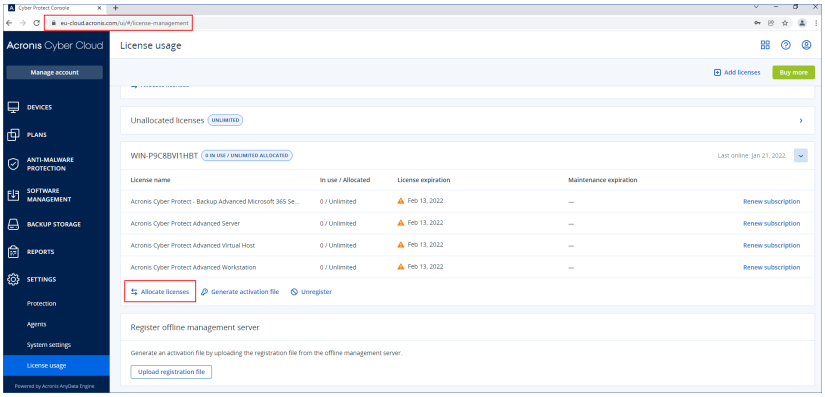
Le quota de licences libéré apparaît dans la section **Licences non allouées** dans la console cloud.

2. Allouez le quota de licences au second serveur de gestion en suivant la procédure dans "Allouer des licences à un serveur de gestion" (p. 31).

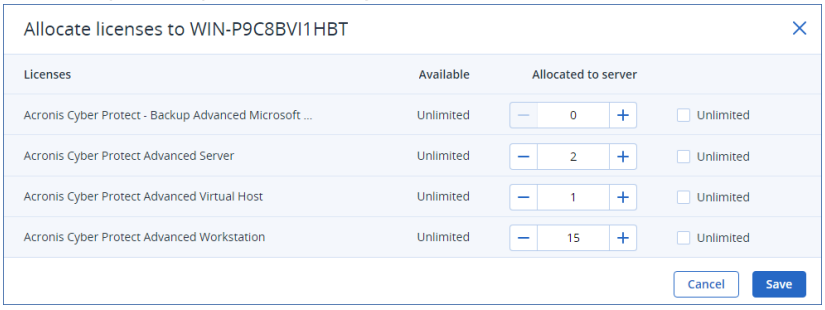
Diminuer le quota de licence alloué à un serveur de gestion hors ligne

Pour réduire le quota de licences allouées à un serveur de gestion hors ligne, vous devez utiliser aussi bien les consoles cloud que locales. Pour accéder à la console cloud, vous avez besoin d'un second ordinateur connecté à Internet.

1. Sur un ordinateur ayant accès à Internet, connectez-vous à la console cloud (`https://cloud.acronis.com`), puis cliquez sur **Paramètres** > **Utilisation de licences**.
2. Accédez au serveur de gestion auquel vous souhaitez allouer une licence, puis cliquez sur **Allouer les licences**.

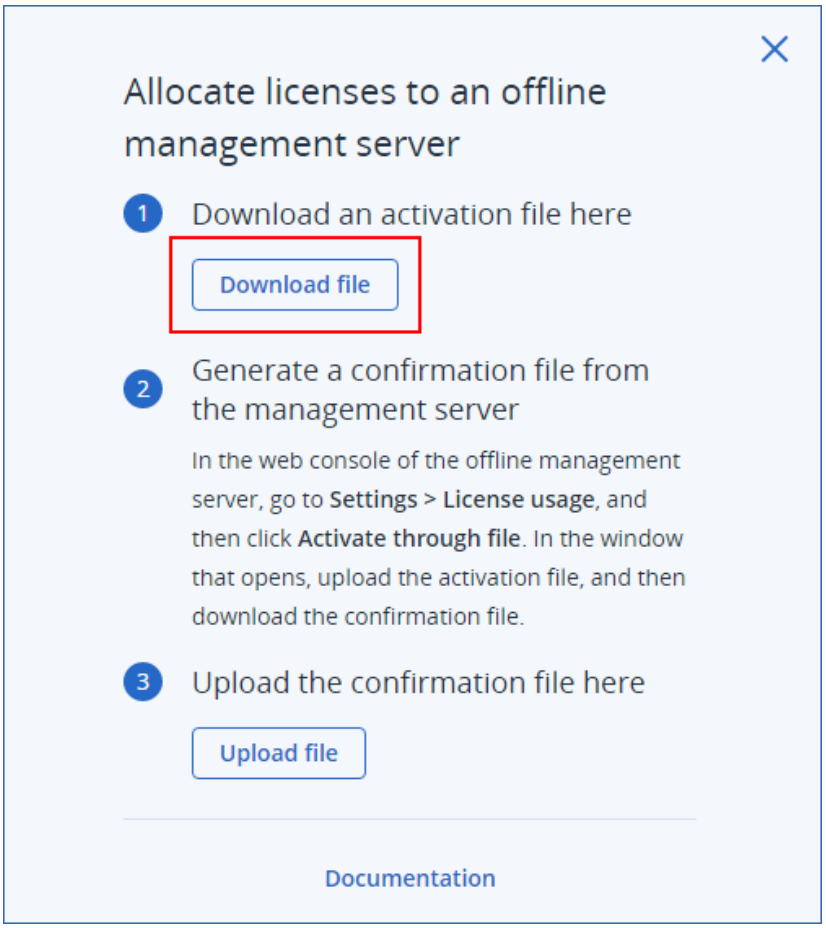


3. Dans la boîte de dialogue qui s'ouvre, modifiez les licences et le quota de licences alloué à ce serveur, puis cliquez sur **Enregistrer**.



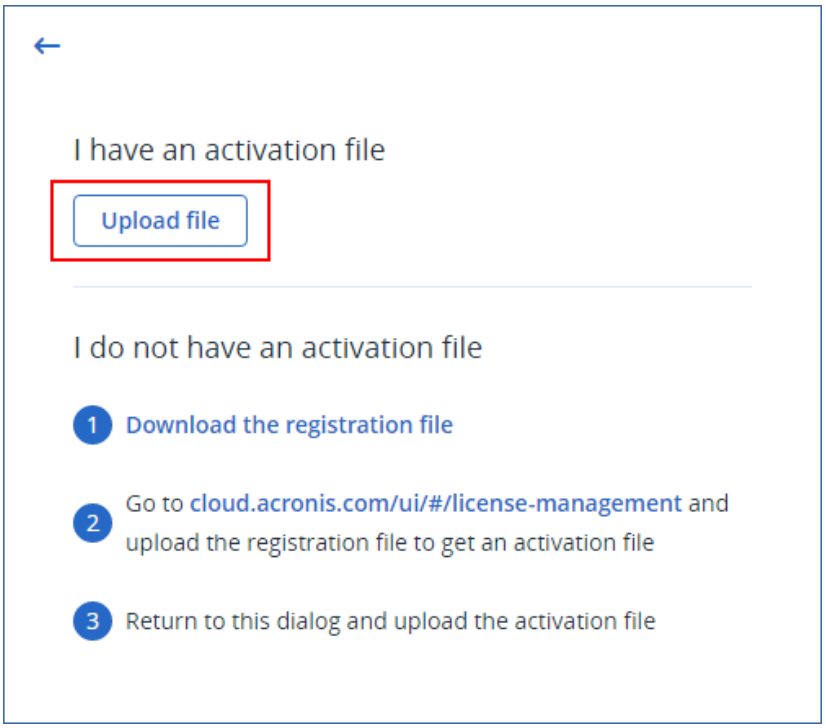
La nouvelle allocation est désormais en attente. Pour l'annuler, cliquez sur **Supprimer cette allocation**.

4. Dans la boîte de dialogue **Allouer des licences à un serveur de gestion hors ligne**, cliquez sur **Télécharger le fichier**.

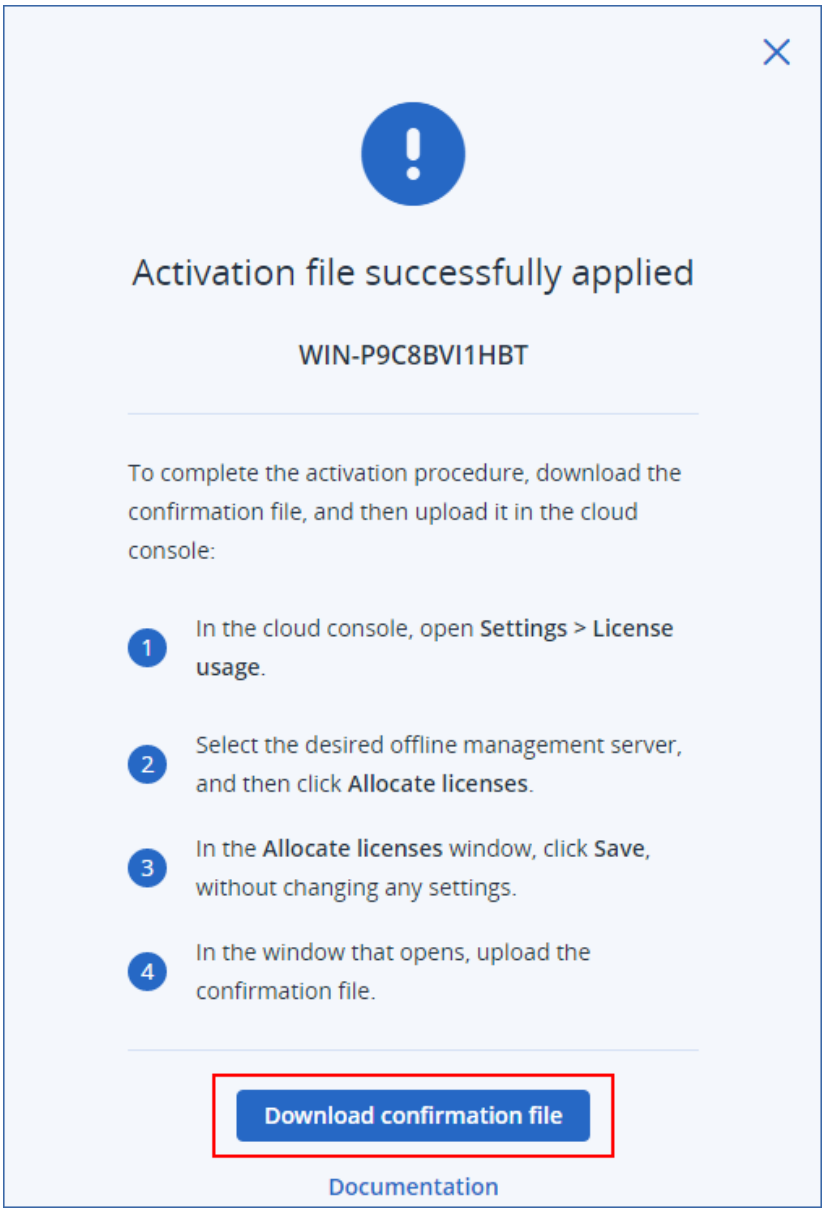


Le fichier d'activation est téléchargé sur votre ordinateur.

5. Dans la console locale du serveur de gestion hors ligne (`https://<adresse IP de votre serveur de gestion>:<port>`), accédez à **Paramètres** > **Utilisation de licences**, puis cliquez sur **Activer au moyen d'un fichier**.
6. Dans la boîte de dialogue qui s'ouvre, sous **Je dispose d'un fichier d'activation**, cliquez sur **Télécharger le fichier**, puis sélectionnez le fichier d'activation que vous avez téléchargé depuis la console cloud.

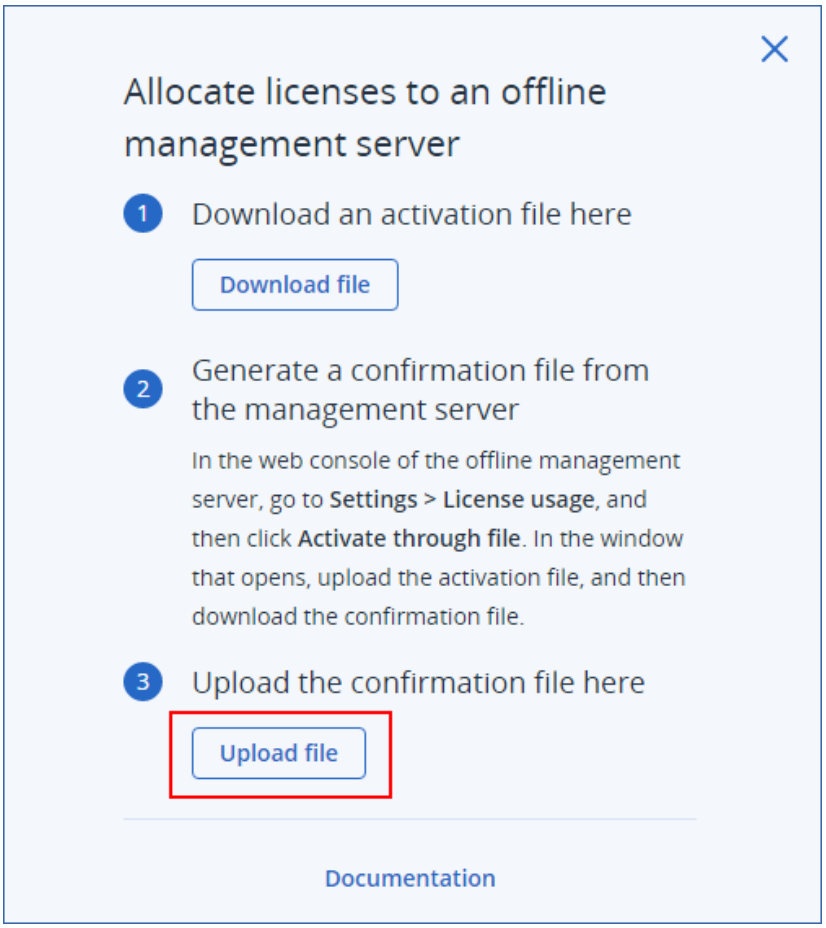


7. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Télécharger le fichier de confirmation**.



Le fichier de confirmation est téléchargé sur votre ordinateur.

8. Dans la console cloud (`https://cloud.acronis.com`), cliquez sur **Paramètres** > **Utilisation de licences**.
9. Accédez au serveur de gestion auquel vous souhaitez allouer une licence, puis cliquez sur **Allouer les licences**.
10. Dans la boîte de dialogue qui s'ouvre, cliquez sur **Enregistrer** sans modifier aucun paramètre.
11. Dans la boîte de dialogue **Allouer des licences à un serveur de gestion hors ligne**, cliquez sur **Télécharger le fichier**, puis sélectionnez le fichier de confirmation téléchargé depuis votre serveur de gestion hors ligne.



Par conséquent, les informations de licence sont synchronisées entre votre compte Acronis et le serveur de gestion hors ligne.

Important
Si le quota de licences modifié est inférieur au nombre d'agents de protection, les agents les moins chargés cesseront de fonctionner. Cette sélection est automatique. Si elle ne correspond pas à vos besoins, réaffectez manuellement les licences disponibles.

Attribution des licences aux charges de travail

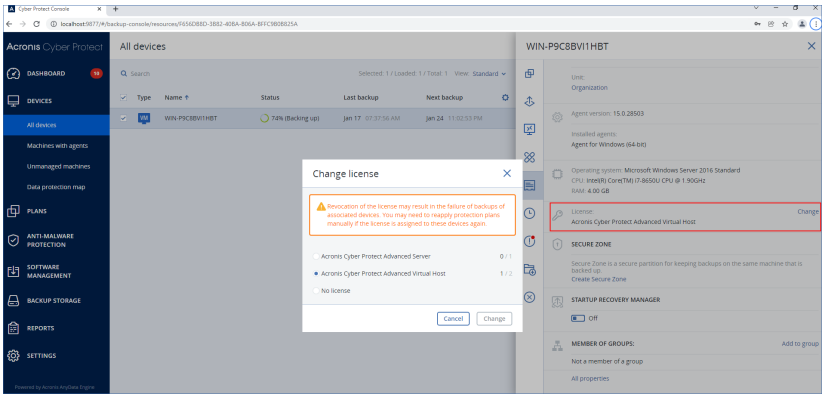
Un serveur de gestion distribue les licences allouées entre les charges de travail inscrites sur ce serveur.

Le serveur de gestion attribue une licence à une charge de travail la première fois que vous appliquez en plan de protection à cette charge de travail. Si plus d'une licence est allouée au serveur de gestion, il affecte la licence la plus appropriée à la charge de travail, en fonction du type de charge de travail, du système d'exploitation et du niveau de protection requis.

Pour vérifier la licence affectée, dans la console Web du serveur de gestion, sélectionnez la charge de travail souhaitée, puis cliquez sur **Détails**.

Pour réattribuer manuellement une licence à une charge de travail

1. Dans la console Web locale du serveur de gestion, cliquez sur **Terminaux**, puis sélectionnez la charge de travail souhaitée.
2. Cliquez sur **Détails**.
3. [Pour les serveurs de gestion sur site] Accédez à la section **Licence**, puis cliquez sur **Modifier**.
4. [Pour les serveurs de gestion cloud] Accédez à la section **Quota de service**, puis cliquez sur **Modifier**.
5. Sélectionnez la licence souhaitée (quota de service), puis cliquez sur **Modifier**.



Limites

Pour les serveurs de gestion hors ligne, l'utilisation actuelle du quota de licence est affichée uniquement dans la console locale. Les serveurs de gestion hors ligne ne synchronisent pas ces données avec votre compte Acronis et celles-ci ne sont pas disponibles dans la console cloud.

Problèmes connus

Dans la console cloud, l'utilisation de la licence ou l'affectation de la licence **Virtual Host** pourraient ne pas être affichées correctement. Pour plus d'informations, veuillez consulter cet article de la base de connaissances.

Désinscrire un serveur de gestion

Pour désinscrire un serveur de gestion en ligne

1. Dans la console cloud (`https://cloud.acronis.com`), cliquez sur **Paramètres** > **Utilisation de licences**.
2. Accédez au serveur de gestion souhaité, puis cliquez sur **Désinscrire**.
3. La fenêtre **Désinscrire le serveur de gestion** s'affiche.
4. Saisissez l'adresse e-mail associée au compte pour confirmer la désinscription.
5. Cliquez sur **Désinscription**.

Par conséquent, toutes les licences allouées au serveur désinscrit sont libérées et peuvent être allouées à un autre serveur de gestion dans votre compte. Dans la console locale du serveur de gestion désinscrit, les licences sont réinitialisées sur zéro.

Pour désinscrire un serveur de gestion hors ligne

Deux points d'entrée sont disponibles pour la désinscription d'un serveur de gestion hors ligne :

Dans la console locale :

1. Dans la console locale, cliquez sur **Désinscrire** dans la ligne où le compte est affiché. La fenêtre **Désinscrire le serveur de gestion** s'affiche.
2. Dans le champ **Connexion**, saisissez l'adresse e-mail associée à l'administrateur local.
3. Cliquez sur **Désinscrire**.
4. La fenêtre **La désinscription est réussie** s'affiche.
5. Cliquez sur **Télécharger le fichier de désinscription**.
6. Dans la console cloud, cliquez sur **Désinscrire**. La fenêtre **Désinscrire le serveur de gestion** s'affiche.
7. Cliquez sur **Inscrire le serveur de gestion hors ligne**. La fenêtre **Désinscrire le serveur de gestion hors ligne** s'affiche.
8. Cliquez sur **Parcourir** et sélectionnez le fichier de désinscription que vous avez téléchargé depuis la console locale.
9. Cliquez sur **Désinscrire**.

Dans la console cloud :

1. Sur un ordinateur ayant accès à Internet, connectez-vous à la console cloud (`https://cloud.acronis.com`), puis cliquez sur **Paramètres** > **Utilisation de licences**.
2. Accédez au serveur de gestion souhaité, puis cliquez sur **Désinscrire**. La fenêtre **Désinscrire le serveur de gestion** s'affiche.
3. Cliquez sur **Inscrire le serveur de gestion hors ligne**. La fenêtre **Désinscrire le serveur de gestion hors ligne** s'affiche.
4. Dans la console locale du serveur de gestion que vous souhaitez désinscrire (`https://<adresse IP de votre serveur de gestion>:<port>`), accédez à **Paramètres** > **Utilisation de licences**, puis cliquez sur **Désinscrire**. Le fichier de désinscription est téléchargé sur votre ordinateur.
5. Dans la console cloud, accédez à la fenêtre **Désinscrire le serveur de gestion hors ligne**.
6. Cliquez sur **Parcourir** et sélectionnez le fichier de désinscription que vous avez téléchargé depuis la console locale.
7. Cliquez sur **Désinscrire**.
8. Également, si vous n'avez plus accès à la machine sur laquelle le serveur de gestion est installé, cliquez sur **Je n'ai pas accès à la machine avec le serveur de gestion**.

Avertissement !
Cette machine sera bloquée et supprimée de votre compte de façon permanente. Vous ne pourrez plus y réenregistrer le serveur de gestion.

Par conséquent, toutes les licences allouées au serveur désinscrit sont libérées et peuvent être allouées à un autre serveur de gestion dans votre compte. Dans la console locale du serveur de gestion désinscrit, les licences sont réinitialisées sur zéro.

Licences dans Acronis Cyber Protect 15 Update 2 et versions précédentes

Pour commencer à utiliser Acronis Cyber Protect version 15 Update 2 et versions précédentes, vous devez ajouter au moins une clé de licence au serveur de gestion. Une licence est affectée automatiquement à une machine lorsqu'un plan de protection est appliqué.

Les licences peuvent également être affectées et révoquées manuellement. Les opérations manuelles avec licences ne sont disponibles que pour des administrateurs de l'organisation. Pour plus d'informations sur les administrateurs, reportez-vous à "Unités et comptes d'administration" (p. 665).

Ajouter des clés de licence à un serveur de gestion

Dans Acronis Cyber Protect 15 Update 2 et versions ultérieures, vous ajoutez les clés de licence au serveur de gestion.

Pour ajouter des clés de licence à un serveur de gestion

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Licences**.
2. Cliquez sur **Ajouter des clés**.
3. Saisissez une ou plusieurs clés, une par ligne.
4. Cliquez sur **Ajouter**.
5. [Lors de l'ajout de clés de licence d'abonnement] Pour activer une licence d'abonnement, connectez-vous à votre compte Acronis.
   a. Dans le formulaire de connexion, saisissez les identifiants que vous utilisez pour le portail client Acronis (`https://account.acronis.com`), puis cliquez sur **Se connecter**.
   b. Confirmez votre compte, puis cliquez sur **Sync**.
   c. Une fois l'opération terminée, cliquez sur **Terminé**.
6. Dans le volet **Ajouter des clés de licence**, cliquez sur **Terminé**.

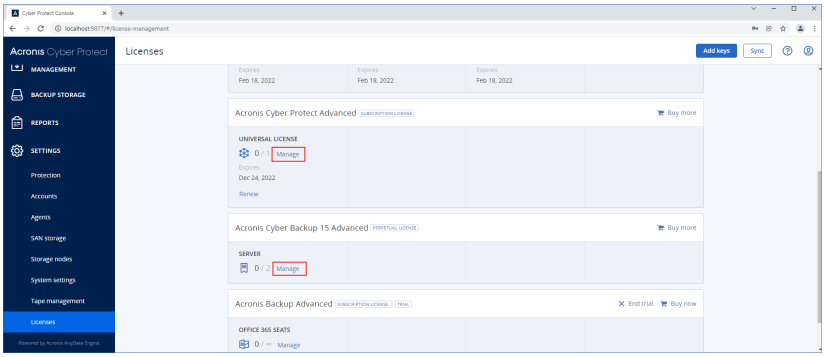
Remarque
Vous pouvez automatiquement importer les clés de licence d'abonnement enregistrées dans votre compte Acronis, au lieu de les ajouter à nouveau au serveur de gestion. Pour importer les clés de licence, dans le volet **Ajouter des clés de licence**, cliquez sur **Synchroniser avec le compte Acronis** puis connectez-vous à votre compte Acronis.

Gestion des licences d'abonnement

Avant d'affecter une licence à une charge de travail, vous devez ajouter la clé de licence au serveur de gestion. Pour en savoir plus sur la façon de procéder, consultez "Ajouter des clés de licence à un serveur de gestion" (p. 42).

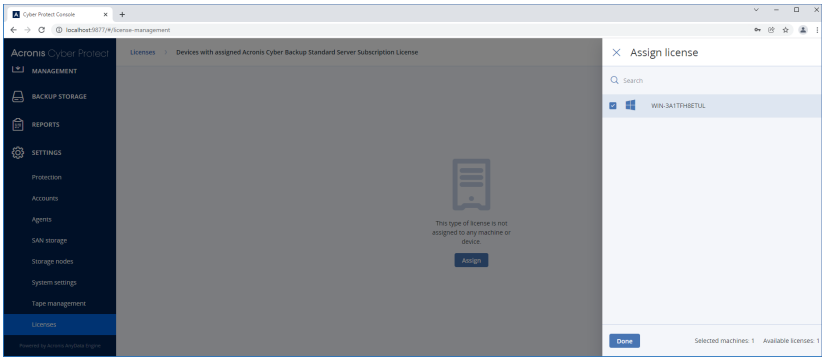
Pour affecter une licence d'abonnement à une charge de travail

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Licences**.
2. Accédez à la licence souhaitée, puis cliquez sur **Gérer**.



3. Cliquez sur **Affecter**.

   Les charges de travail auxquelles vous pouvez affecter cette licence sont affichées.



4. Sélectionnez une charge de travail, puis cliquez sur **Terminé**.

Pour révoquer une licence d'abonnement d'une charge de travail

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Licences**.
2. Accédez à la licence souhaitée, puis cliquez sur **Gérer**.

   Toutes les charges de travail auxquelles cette licence est affectée sont affichées.
3. Sélectionnez la charge de travail à partir de laquelle vous voulez révoquer la licence.
4. Cliquez sur **Révoquer**.
5. Confirmez votre choix.

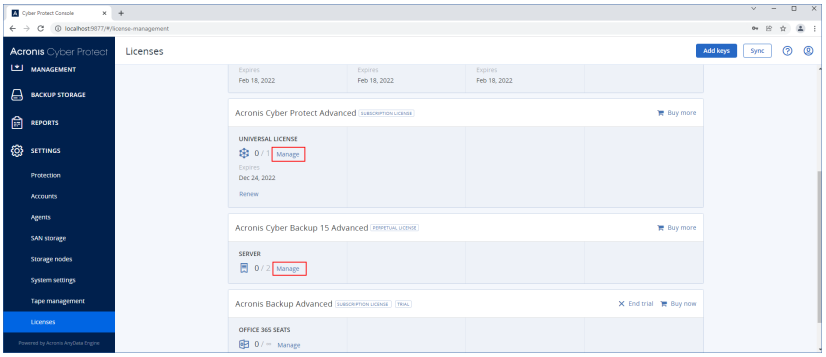
   La licence révoquée est libérée et vous pouvez l'affecter à une autre charge de travail.

Gestion des licences perpétuelles

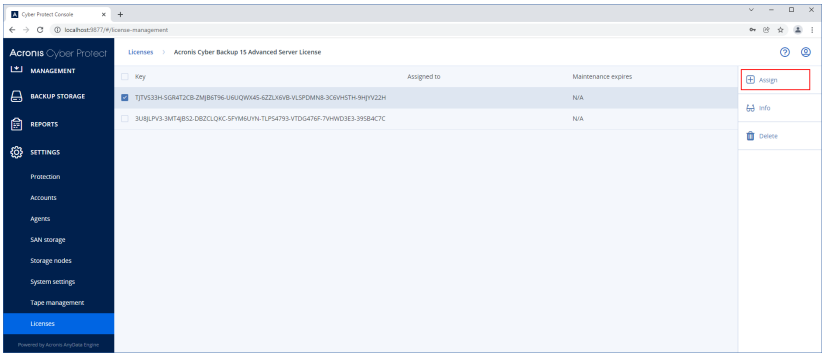
Avant d'affecter une licence à une charge de travail, vous devez ajouter la clé de licence au serveur de gestion. Pour en savoir plus sur la façon de procéder, consultez "Ajouter des clés de licence à un serveur de gestion" (p. 42).

Pour affecter une licence perpétuelle à une charge de travail

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Licences**.
2. Accédez à la licence souhaitée, puis cliquez sur **Gérer**.



   Les clés de licence qui correspondent à la licence sélectionnée sont affichées.
3. Sélectionnez la clé de licence que vous souhaitez affecter à une charge de travail.
4. Cliquez sur **Affecter**.



   Les charges de travail auxquelles vous pouvez affecter cette clé de licence sont affichées.
5. Sélectionnez une charge de travail, puis cliquez sur **Terminé**.

Pour révoquer une licence perpétuelle d'une charge de travail

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Licences**.
2. Sélectionnez la licence souhaitée, puis cliquez sur **Gérer**.

   Les clés de licence qui correspondent à la licence sélectionnée sont affichées. Vérifiez à quelle charge de travail cette clé de licence de licence est affectée dans la colonne **Affecté à**.
3. Sélectionnez la clé de licence que vous souhaitez révoquer.
4. Cliquez sur **Révoquer**.
5. Confirmez votre choix.

   La clé de licence révoquée reste dans la liste des licences et vous pouvez l'affecter à une autre charge de travail.

Installation

Présentation de l'installation

Acronis Cyber Protect prend en charge deux méthodes de déploiement : sur site et dans le Cloud. La différence principale entre les deux réside dans l'emplacement du serveur de gestion Acronis Cyber Protect.

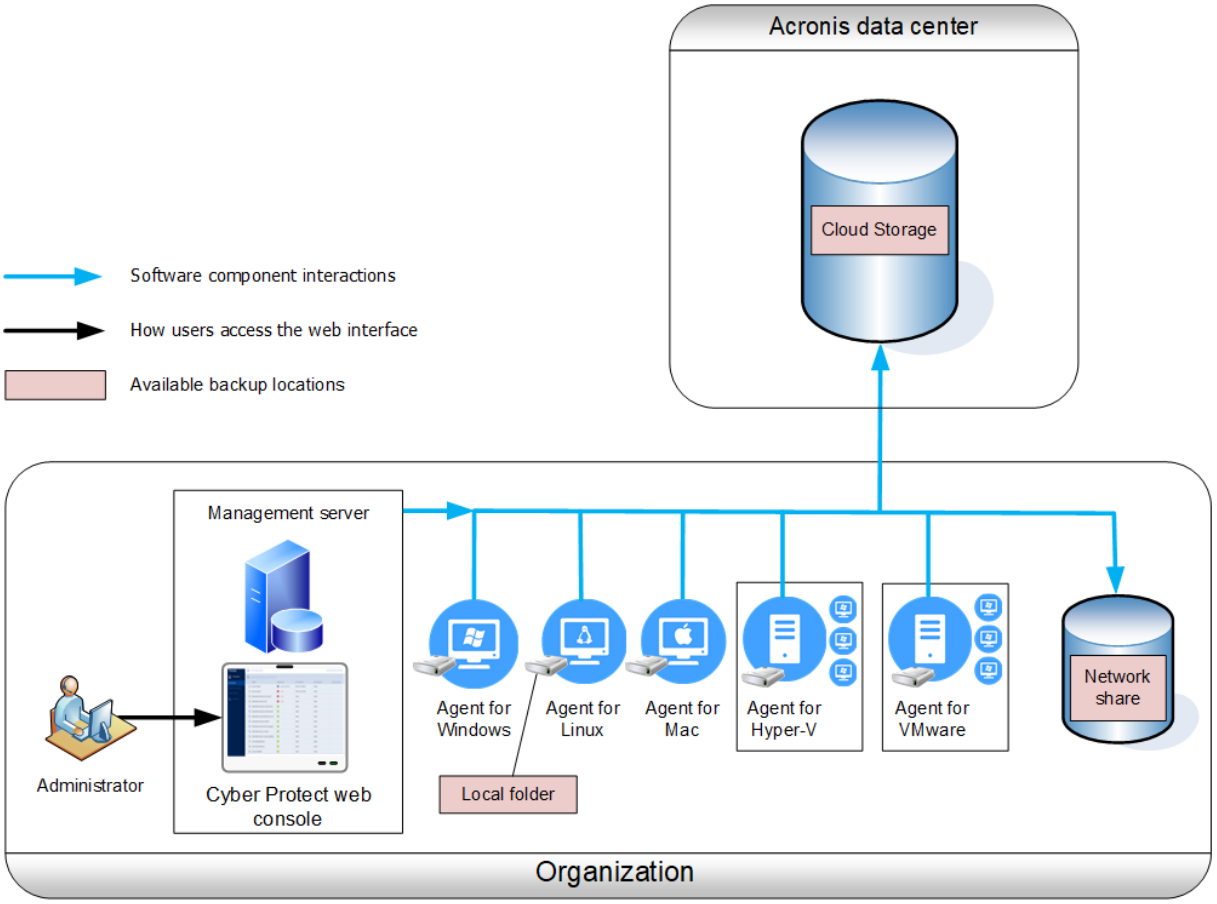
Le serveur de gestion est le point central pour la gestion de toutes vos sauvegardes. Avec le déploiement sur site, il est installé sur votre réseau local, alors qu'il se situera dans un des centres de données Acronis avec le déploiement dans le Cloud. L'interface Web pour ce serveur est appelée console Web Cyber Protect.

Le serveur de gestion est responsable de la communication entre les agents de protection et effectue des fonctions générales de gestion des plans. Avant chaque activité de protection, les agents se réfèrent au serveur de gestion afin de vérifier les prérequis. Parfois, la connexion au serveur de gestion est susceptible d'être perdue, ce qui empêche le déploiement de nouveaux plans de protection. Toutefois, si un plan de protection a déjà été déployé sur une machine, l'agent poursuit les opérations de protection pendant 30 jours après la perte de la communication avec le serveur de gestion.

Les deux types de déploiement nécessitent l'installation d'un agent de protection sur chaque machine que vous souhaitez sauvegarder. Les types de stockage pris en charge sont également les mêmes. L’espace de stockage dans le Cloud est vendu séparément des licences Acronis Cyber Protect.

Déploiement sur site

Avec un déploiement sur site, tous les composants de produits sont installés sur votre réseau local. Il s'agit de la seule méthode de déploiement disponible avec une licence perpétuelle. Vous devez également utiliser cette méthode si vos machines ne sont pas connectées à Internet.



Emplacement du serveur de gestion

Vous pouvez installer le serveur de gestion sur une machine fonctionnant sous Windows ou Linux.

L'installation sous Windows est recommandée, car elle vous permet de déployer des agents sur d'autres machines à partir du serveur de gestion. À l'aide de la licence Advanced, il est possible de créer des unités d'organisation et de leur ajouter des administrateurs. Ainsi, vous pouvez déléguer la gestion de la protection à d'autres personnes dont les droits d'accès seront strictement limités aux unités correspondantes.

L'installation sous Linux est recommandée pour les environnements exclusivement Linux. Il vous faudra installer un agent localement sur les machines que vous souhaitez sauvegarder.

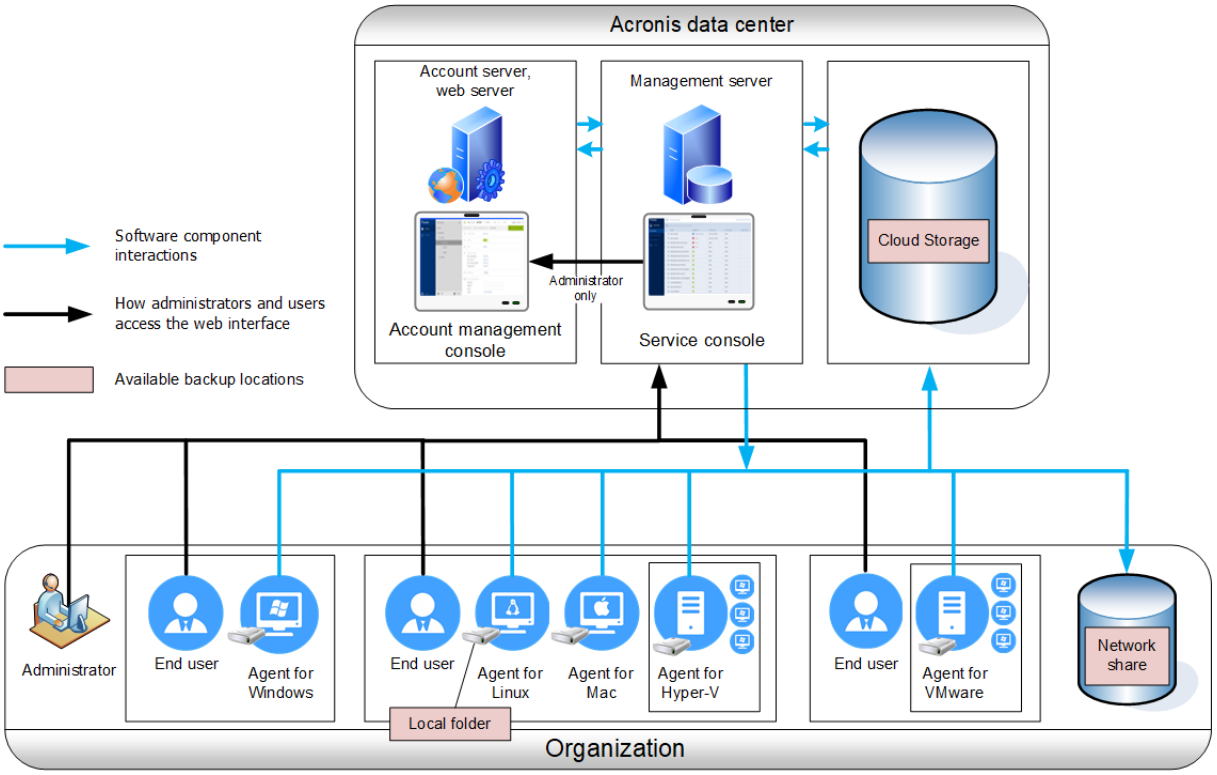
Déploiement Cloud

Le déploiement dans le Cloud signifie que le serveur de gestion est situé dans un des centres de données Acronis. L'avantage de cette approche est que vous n'avez pas besoin d'entretenir le serveur de gestion dans votre réseau local. Vous pouvez considérer Acronis Cyber Protect comme un service de cyberprotection qui vous est fourni par Acronis.

L'accès au serveur de compte vous permet de créer des comptes utilisateur, de leur attribuer des quotas d'utilisation de services et de créer des groupes d'utilisateurs (unités) correspondant à la

structure de votre organisation. Chaque utilisateur peut accéder à la console Web Cyber Protect, télécharger l'agent requis et l'installer sur son ordinateur en quelques minutes.

Les comptes d'administrateur peuvent être créés au niveau des unités ou de l'organisation. Chaque compte dispose d'un affichage centré sur sa zone de commande. Les utilisateurs ont uniquement accès à leurs propres sauvegardes.



Le tableau suivant résume les différences entre le déploiement sur site et dans le Cloud. Chaque colonne répertorie les fonctionnalités disponibles uniquement pour le type de déploiement correspondant.

Déploiement sur site	Déploiement Cloud
• Possibilité d'utiliser les licences perpétuelles • Serveur de gestion sur site pouvant être utilisé dans les environnements isolés par air gap* • Serveur SFTP en tant qu'emplacement de sauvegarde • Acronis Cyber Infrastructure en tant qu'emplacement de sauvegarde • Lecteur de bandes et nœuds de stockage Acronis en tant qu'emplacements de sauvegarde** • Mise à niveau à partir des versions précédentes d'Acronis Cyber Protect, y compris Acronis Backup pour VMware	• Sauvegarde cloud à cloud des données Microsoft 365, y compris la protection des groupes, des dossiers publics, de OneDrive*** et des données SharePoint Online • Sauvegarde Cloud à Cloud de données Google Workspace • L'agent pour Mac prend en charge les processeurs x64 et ARM tels que les puces silicone M1 et M2 d'Apple • Agent pour Virtuozzo (sauvegarde de machines virtuelles Virtuozzo au niveau de l'hyperviseur) • Agent pour oVirt (sauvegarde de machines virtuelles oVirt KVM au niveau de l'hyperviseur)

	• Agent pour Virtuozzo Hybrid Infrastructure (sauvegarde de machines virtuelles Virtuozzo Hybrid Infrastructure au niveau de l'hyperviseur) • Reprise d'activité après sinistre en tant que service cloud****

* Pour plus d'informations sur l'activation du serveur de gestion dans un environnement isolé par air gap, voir "Pour activer un serveur de gestion hors ligne" (p. 28).

** La fonctionnalité n'est pas disponible dans la Standard Edition.

***Par défaut, le dossier racine OneDrive est exclu des opérations de sauvegarde. Si vous choisissez de sauvegarder des fichiers et dossiers OneDrive spécifiques, ils seront sauvegardés. Les fichiers qui ne sont pas disponibles sur l'appareil auront un contenu non valide dans l'archive.

**** La fonctionnalité est disponible uniquement avec le module complémentaire de reprise d'activité après sinistre.

Composants

Agents

Les agents sont des applications qui effectuent la sauvegarde des données, la restauration et d'autres opérations sur les ordinateurs gérés par Acronis Cyber Protect.

L'agent pour Windows est installé avec l'agent pour Exchange, l'agent pour SQL, l'agent pour Active Directory et l'agent pour Oracle. Par exemple, si vous installez agent pour SQL, vous pourrez également sauvegarder la totalité de la machine sur laquelle l'agent est installé.

Certains agents ne peuvent être installés que sur les machines ayant un rôle ou une application spécifique. Par exemple l'agent pour Hyper-V est installé sur des machines qui exécutent le rôle d'Hyper-V, l'agent pour SQL sur des machines qui exécutent des bases de données SQL, l'agent pour Exchange sur des machines qui exécutent le rôle de boîte aux lettres de Microsoft Exchange Server et l'agent pour Active Directory sur des contrôleurs de domaine.

Choisissez un agent en fonction de ce que vous allez sauvegarder. Le tableau suivant regroupe les informations qui vous aideront à faire votre choix.

Qu'allez-vous sauvegarder ?	**Quel agent installer ?**	**Où dois-je l'installer ?**	**Disponibilité de l'agent**	
			Sur site	**Cloud**
Machines physiques				
Disques, volumes et fichiers sur des machines	Agent pour Windows	Sur la machine qui sera sauvegardée.	+	+

physiques sous Windows				
Disques, volumes et fichiers sur des machines physiques sous Linux	Agent pour Linux		+	+
Disques, volumes et fichiers sur des machines physiques sous macOS	Agent pour Mac		+	+
Applications				
Bases de données SQL	Agent pour SQL	Sur une machine fonctionnant sous Microsoft SQL Server.	+	+
Bases de données et boîtes aux lettres Exchange	Agent pour Exchange	Sur une machine exécutant le rôle de boîte aux lettres de Microsoft Exchange Server.* Si seule la sauvegarde de la boîte aux lettres est requise, l'agent peut être installé sur une machine Windows disposant d'un accès réseau à la machine exécutant le rôle Accès Client de Microsoft Exchange Server.	+ Aucune sauvegarde de boîte aux lettres	+
Boîtes aux lettres Microsoft 365	Agent pour Office 365	Sur une machine Windows connectée à Internet.	+	+
Machines fonctionnant sous les services de domaine Active Directory	Agent pour Active Directory	Sur le contrôleur de domaine.	+	+
Machines s'exécutant à partir d'Oracle Database	Agent pour Oracle	Sur la machine sous Oracle Database.	+	-

Machines virtuelles				
Machines virtuelles VMware ESXi	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 (matériel virtuel)	Sur l'hôte ESXi.	+	+
Les machines virtuelles Hyper-V	Agent pour Hyper-V	Sur un hôte Hyper-V.	+	+
Machines virtuelles HC3 de Scale Computing	Agent pour HC3 de Scale Computing	Sur l'hôte HC3 de Scale Computing	+	+
Les machines virtuelles hébergées sur Windows Azure	Comme pour les machines physiques***	Sur la machine qui sera sauvegardée.	+	+
Les machines virtuelles hébergées sur Amazon EC2			+	+
Machines virtuelles Citrix XenServer			+****	+
Machines virtuelles Red Hat Virtualization (RHV/RHEV)				
Machines virtuelles basées sur un noyau (KVM)				
Machines virtuelles Oracle				
Machines				

virtuelles Nutanix AHV				
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 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 obtenir des instructions détaillées, reportez-vous à l'article « Sauvegarde sans réseau local ».

***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. La machine est toutefois considérée comme une machine virtuelle lorsque vous définissez les quotas pour le nombre de machines dans un déploiement Cloud.

****Grâce à une licence Acronis Cyber Protect Advanced Virtual Host, ces machines sont considérées comme étant virtuelles (en raison de la licence d'hébergement utilisée). ****Grâce à une licence Acronis Cyber Protect Virtual Host, ces machines sont considérées comme étant physiques (par licence de machine utilisée).

Autres composants

Composant	Fonctionnalité	Où dois-je l'installer ?	Disponibilité	
			Sur site	Cloud
Serveur de gestion	Le serveur de gestion est le point de gestion central de toutes vos sauvegardes. Avec le déploiement sur site, il est installé sur votre réseau local. Il gère les agents et fournit l'interface Web aux utilisateurs.	Sur une machine sous Windows ou Linux	+	-

Composants pour l'installation à distance	Sauvegarde les packages d'installation d'agent dans un dossier local.	Sur la machine Windows exécutant le serveur de gestion.	+	-
Service d'analyse	Composant facultatif qui permet l'analyse antimalware des sauvegardes au sein d'un stockage dans le cloud, ou dans un dossier réseau ou local. Le service d'analyse nécessite une base de données Microsoft SQL Server ou PostgreSQL. Il n'est pas compatible avec la base de données SQLite par défaut utilisée par le serveur de gestion.	Sur la machine Windows ou Linux exécutant le serveur de gestion.	+	-
Bootable Media Builder	Crée un support de démarrage.	Sur une machine sous Windows ou Linux	+	-
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.	Sur un ordinateur exécutant Windows, Linux ou macOS.	+	+
Acronis Cyber Protect 15 Moniteur	Fournit l'interface graphique à l'agent pour Windows et à l'agent pour Mac. Il affiche des informations à propos de l'état de protection de la	Sur une machine sous Windows ou macOS.	+	+

	machine sur laquelle l'agent est installé, et permet à ses utilisateurs de définir les paramètres de chiffrement de sauvegarde et de serveur proxy. Dans Windows, le moniteur Acronis Cyber Protect 15 nécessite que l'agent pour Windows soit installé sur la même machine.			
Nœud de stockage	Stocke les sauvegardes. Elle est requise pour le catalogage et la déduplication. Le nœud de stockage nécessite que l'agent pour Windows soit installé sur la même machine.	Sur une machine sous Windows.	+	-
Service de catalogue	Effectue le catalogage des sauvegardes sur les nœuds de stockage.	Sur une machine sous Windows.	+	-
Serveur PXE	Permet de démarrer des machines en tant que support de démarrage au sein du réseau.	Sur une machine sous Windows.	+	-

Utilisation d'Acronis Cyber Protect avec d'autres solutions de sécurité dans votre environnement

Vous pouvez utiliser Acronis Cyber Protect avec ou sans autres solutions de sécurité telles qu'un logiciel antivirus autonome dans votre environnement.

Sans autre solution de sécurité, vous pouvez utiliser Acronis Cyber Protect pour réaliser la cyberprotection ou la sauvegarde et restauration traditionnelles, selon votre licence et vos besoins. Pour plus d'informations sur les fonctionnalités disponibles avec chaque licence, consultez la section Comparaison des éditions Acronis Cyber Protect 15 incluant le déploiement dans le Cloud. Vous pouvez ajuster la portée de vos plans de protection en n'activant que les modules dont vous avez besoin.

Vous pouvez choisir Acronis Cyber Protect pour bénéficier d'une cyberprotection complète, y compris la protection contre les virus et d'autres malwares, même si vous avez déjà une autre solution de sécurité dans votre environnement. Dans ce cas, vous devez désactiver ou supprimer l'autre solution de sécurité afin d'éviter les conflits.

Vous souhaiterez peut-être améliorer votre cyberprotection sans désactiver ni supprimer votre solution de sécurité actuelle. C'est tout à fait possible. Vous devez simplement veiller à ne pas utiliser le module Antivirus et antimalware dans vos plans de protection. Tous les autres modules peuvent être utilisés librement.

Limites

- L'analyse antimalware des sauvegardes exige que vous installiez le service d'analyse lors de l'installation du serveur de gestion Cyber Protect.
- L'accès à distance via un client HTML 5 n'est disponible que si le serveur de gestion Cyber Protect est installé sur un ordinateur Linux.

Exigences logicielles

Navigateurs Web pris en charge

L'interface Web prend en charge les navigateurs suivants :

- Google Chrome 29 ou version ultérieure
- Mozilla Firefox 23 ou version ultérieure
- Opera 16 ou version ultérieure
- Windows Internet Explorer 10 ou version ultérieure

Remarque
Dans les déploiements cloud, Internet Explorer n'est pas pris en charge.

- Microsoft Edge 25 ou version ultérieure
- Safari 8 ou version ultérieure s'exécutant sur 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.

Systèmes d'exploitation et environnements pris en charge

Agents

Agent pour Windows

- Windows XP Professionnel SP1 (x64), SP2 (x64), SP3 (x86)
- Windows XP Professionnel SP2 (x86) – pris en charge avec une version spéciale de l'agent pour Windows. Pour les détails et limites de cette prise en charge, reportez-vous à « Agent pour Windows XP SP2 ».
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 et versions ultérieures – éditions Standard et Enterprise (x86, x64)

  Remarque
  Acronis Cyber Protect nécessite la mise à jour KB940349 de Microsoft, qui ne peut plus être téléchargée séparément. Pour garantir que la fonctionnalité fournie à l'origine par KB940349 est disponible sur votre machine, installez toutes les mises à jour actuellement disponibles pour Windows Server 2003.
  Pour en savoir plus sur KB940349, veuillez consulter cet article de la base de connaissances.

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008 – éditions Standard, Enterprise, Datacenter, Foundation et Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – toutes les éditions (x86, x64)

  Remarque
  Pour utiliser Acronis Cyber Protect avec Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft :
  - Mises à jour de sécurité étendues (ESU) pour Windows 7
  - KB4474419
  - KB4490628

  Pour plus d'informations sur les mises à jour requises, reportez-vous à 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 – éditions Famille, Professionnel, Éducation, Entreprise, IoT Entreprise et LTSC (anciennement LTSB)
- Windows Server 2016 – toutes les options d'installation, sauf Nano Server
- Windows Server 2019 – toutes les options d'installation, sauf Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server

Agent pour SQL, agent pour Exchange (pour la sauvegarde de bases de données et la sauvegarde reconnaissant les applications), agent pour Active Directory

Chacun de ces agents peut être installé sur une machine fonctionnant sous tout système d'exploitation figurant dans la liste ci-dessus, avec une version prise en charge de l'application respective, avec l'exception suivante :

- Agent pour SQL n'est pas pris en charge pour le déploiement sur site dans Windows 7 Édition Starter et Édition Familiale (x86, x64)

Agent pour Exchange (pour la sauvegarde de boîte aux lettres)

Cet agent peut être installé sur une machine avec ou sans Microsoft Exchange Server.

- 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 R2/2012/2012R2
- Windows 10 – éditions Famille, Professionnel, Éducation et Entreprise
- Windows Server 2016 – toutes les options d'installation, sauf Nano Server
- Windows Server 2019 – toutes les options d'installation, sauf Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server

Agent pour Office 365

- 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, sauf Nano Server

Agent pour Oracle

- 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 Linux

Remarque
Les distributions Linux et les versions de noyau suivantes ont été spécifiquement testées. Toutefois, même si votre distribution Linux ou votre version de noyau n'est pas répertoriée, il est possible qu'elle fonctionne quand même correctement dans tous les scénarios nécessaires, en raison des spécificités des systèmes d'exploitation Linux.

Si vous rencontrez des problèmes lors de l'utilisation de Acronis Cyber Protect avec votre association de distribution Linux et de version de noyau, contactez l'équipe d'assistance pour une enquête approfondie.

Linux avec noyau de la version 2.6.9 à la version 5.19 et glibc 2.3.4 ou version ultérieure, y compris les distributions x86 et x86_64 suivantes :

- 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*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

Important
Les configurations avec Btrfs ne sont pas prises en charge pour SUSE Linux Enterprise Server 12 et SUSE Linux Enterprise Server 15.

- 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
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel et Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Avant d'installer le produit sur un système qui n'utilise pas de gestionnaire de paquets RPM, comme un système Ubuntu, vous devez installer ce gestionnaire manuellement ; par exemple, en exécutant la commande suivante (en tant qu'utilisateur racine) : `apt-get install rpm`

Si votre distribution Linux n'est pas compatible avec le mécanisme D-bus (par exemple Red Hat Enterprise Linux 6.x ou CentOS 6.x) Acronis Cyber Protect utilisera l'emplacement par défaut pour stocker les clés sécurisées, car le système d'exploitation ne fournit pas d'emplacement D-Bus compatible.

* Pris en charge uniquement avec les noyaux des versions 4.18 à 5.19

Agent pour Mac

Remarque
Les processeurs ARM tels que les puces silicone M1 et M2 d'Apple ne sont pas pris en charge.

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13

Agent pour VMware (matériel virtuel)

Cet agent est fourni en tant que matériel virtuel pour s'exécuter sur un hôte ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent pour VMware (Windows)

Cet agent est livré comme une application Windows pour s'exécuter dans tout système d'exploitation inscrit dans la liste ci-dessus pour l'agent pour Windows, avec les exceptions 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.

Agent pour Hyper-V

- 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
- 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 avec Hyper-V – toutes les options d'installation, excepté Nano Server

Agent pour HC3 de Scale Computing (matériel virtuel)

Cet agent est fourni en tant qu'appliance virtuelle déployée dans le cluster HC3 de Scale Computing via la console Web Cyber Protect. Il n'existe aucun programme d'installation autonome pour cet agent.

Scale Computing Hypercore 8.8, 8.9, 9.0

Serveur de gestion (uniquement pour les déploiements sur site)

Sous Windows

- Windows 7 – toutes les éditions (x86, x64)

  Remarque
  Pour utiliser Acronis Cyber Protect avec Windows 7, vous devez installer les mises à jour suivantes fournies par Microsoft :
  - Mises à jour de sécurité étendues (ESU) pour Windows 7
  - KB4474419
  - KB4490628

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

- Windows Server 2008 R2 - éditions Standard, Enterprise, Datacenter et Foundation
- 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 2008 R2/2012/2012 R2/2016
- Windows 10 – éditions Famille, Professionnel, Éducation, Entreprise, IoT Entreprise et LTSC (anciennement LTSB)
- Windows Server 2016 – toutes les options d'installation, sauf Nano Server
- Windows Server 2019 – toutes les options d'installation, sauf Nano Server
- Windows 11 – toutes les éditions
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server

Sous Linux

Remarque
Les distributions Linux et les versions de noyau suivantes ont été spécifiquement testées. Toutefois, même si votre distribution Linux ou votre version de noyau n'est pas répertoriée, il est possible qu'elle fonctionne quand même correctement dans tous les scénarios nécessaires, en raison des spécificités des systèmes d'exploitation Linux.

Si vous rencontrez des problèmes lors de l'utilisation de Acronis Cyber Protect avec votre association de distribution Linux et de version de noyau, contactez l'équipe d'assistance pour une enquête approfondie.

Linux avec noyau de la version 2.6.9 à la version 5.19 et glibc 2.3.4 ou version ultérieure, y compris les distributions x86_64 suivantes.

Les distributions x86 suivantes ne sont pas prises en charge.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  Important
  Les configurations avec Btrfs ne sont pas prises en charge pour SUSE Linux Enterprise Server 12 et SUSE Linux Enterprise Server 15.

- 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
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel et Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Avant d'installer le produit sur un système qui n'utilise pas de gestionnaire de paquets RPM, comme un système Ubuntu, vous devez installer ce gestionnaire manuellement ; par exemple, en exécutant la commande suivante (en tant qu'utilisateur racine) : `apt-get install rpm`

Si votre distribution Linux n'est pas compatible avec le mécanisme D-bus (par exemple Red Hat Enterprise Linux 6.x ou CentOS 6.x) Acronis Cyber Protect utilisera l'emplacement par défaut pour stocker les clés sécurisées, car le système d'exploitation ne fournit pas d'emplacement D-Bus compatible.

* Pris en charge uniquement avec les noyaux des versions 4.18 à 5.19

Nœud de stockage (uniquement pour les déploiements sur site)

- Windows Server 2008 – éditions Standard, Enterprise, Datacenter et Foundation (x64 uniquement)
- Windows Small Business Server 2008
- Windows 7 - toutes les éditions (x64 uniquement)
- Windows Server 2008 R2 - éditions Standard, Enterprise, Datacenter et Foundation
- 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 (x64 uniquement), sauf les éditions Windows RT
- Windows Server 2012/2012 R2 – toutes les éditions
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016
- Windows 10 – éditions Famille, Professionnel, Éducation, Entreprise et IoT Entreprise
- Windows Server 2016 – toutes les options d'installation, sauf Nano Server
- Windows Server 2019 – toutes les options d'installation, sauf Nano Server
- Windows Server 2022 – toutes les options d'installation, sauf Nano Server

Agent pour Windows XP SP2

L'agent pour Windows XP SP2 prend en charge uniquement la version 32 bits de Windows XP SP2.

Pour protéger des machines sous Windows XP SP1 (x64), Windows XP SP2 (x64), or Windows XP SP3 (x86), utilisez l'agent pour Windows standard.

L'agent pour Windows XP SP2 nécessite une licence Acronis Cyber Backup 12.5. Les clés de licence Acronis Cyber Protect 15 ne sont pas prises en charge.

Installation

L'agent pour Windows XP SP2 doit disposer au minimum de 550 Mo d'espace disque et de 150 Mo de RAM. Lors de la sauvegarde, l'agent utilise en général environ 350 Mo de mémoire. Le pic de consommation peut atteindre jusqu'à 2 Go en fonction du volume de données traitées.

L'agent pour Windows XP SP2 peut être installé uniquement en local sur la machine que vous souhaitez sauvegarder. Pour télécharger le programme d'installation de l'agent, cliquez sur l'icône

de compte dans le coin supérieur droit, puis cliquez sur > **Téléchargements** > **Agent pour Windows XP SP2**.

Cyber Protect Monitor et Bootable Media Builder ne peuvent pas être installés. Pour télécharger le fichier ISO du support de démarrage, cliquez sur l'icône de compte dans le coin supérieur droit > **Téléchargements** > **Support de démarrage**.

Mise à jour

L'agent pour Windows XP SP2 ne prend pas en charge la fonctionnalité de mise à jour distante. Pour mettre l'agent à jour, téléchargez la nouvelle version du programme d'installation, puis répétez la procédure.

Si vous avez mis à jour Windows XP de SP2 vers SP3, désinstallez l'agent pour Windows XP SP2, puis installez l'agent pour Windows standard.

Limites

- Seule la sauvegarde de lecteur est disponible. Des fichiers distincts peuvent être récupérés à partir d'une sauvegarde de disque ou volume.
- La fonction Planifier par événement n'est pas prise en charge.
- Les conditions d'exécution du plan de protection ne sont pas prises en charge.
- Seules les destinations de sauvegarde suivantes sont prises en charge :
  - Stockage dans le Cloud
  - Dossier local
  - Dossier réseau
  - Secure Zone
- Le format de sauvegarde **Version 12** et les caractéristiques exigeant le format de sauvegarde **Version 12** ne sont pas pris en charge. L'envoi des données physiques, en particulier, n'est pas disponible. L'option **Performance et créneau de sauvegarde**, si elle est activée, s'applique uniquement aux paramètres de niveau vert.
- La sélection de disques/volumes distincts pour la restauration et le mappage de disque manuel lors d'une reprise ne sont pas pris en charge dans l'interface Web. Cette fonctionnalité est disponible au niveau du support de démarrage.
- Le traitement des données hors hôte n'est pas pris en charge.
- L'agent pour Windows XP SP2 ne peut pas exécuter les opérations suivantes sur des sauvegardes :
  - Conversion de sauvegardes vers une machine virtuelle
  - Montage de volumes à partir d'une sauvegarde
  - Extraction de fichiers à partir d'une sauvegarde
  - L'exportation et la validation manuelle d'une sauvegarde.

  Vous pouvez exécuter ces opérations à l'aide d'un autre agent.

- Les sauvegardes créées par l'agent pour Windows XP SP2 ne peuvent pas être exécutées en tant que machines virtuelles.

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

Les éditions SQL Server Express des versions de serveur SQL susmentionnées sont également prises en charge.

Versions Microsoft Exchange Server compatibles

- 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.
- 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

Acronis Cyber Protect 15 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

- Version Oracle Database 11g, toutes éditions
- Version Oracle Database 12c, 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.

SAP HANA ne prend pas en charge la récupération de conteneurs de bases de données multi-locataires à l'aide d'instantanés de stockage. Par conséquent, cette solution prend en charge les conteneurs SAP HANA avec une base de données locataire uniquement.

Plates-formes de virtualisation prises en charge

Le tableau suivant récapitule la prise en charge de diverses plates-formes de virtualisation.

Remarque
Les fournisseurs d'hyperviseur et versions suivants pris en charge via la méthode **Sauvegarde depuis un SE invité** ont été testés de façon spécifique. Toutefois, même si vous exécutez un hyperviseur provenant d'un fournisseur ou un hyperviseur dont la version n'est pas répertoriée ci-dessous, il est possible que la méthode **Sauvegarde depuis un SE invité** fonctionne toujours correctement dans tous les scénarios requis.

Si vous rencontrez des problèmes lors de l'utilisation d'Acronis Cyber Protect avec votre combinaison version/fournisseur d'hyperviseur, contactez l'équipe d'assistance pour un examen approfondi.

Plate-forme	Sauvegarde au niveau de l'hyperviseur (sauvegarde sans agent)	Sauvegarde depuis un SE invité
VMware		
Versions VMware vSphere : 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **Éditions VMware vSphere :** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard*	+	+

VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus		
VMware vSphere Hypervisor (ESXi gratuit)**		+
Serveur VMware (serveur virtuel VMware) VMware Workstation VMware ACE Lecteur VMware		+
Microsoft* **		
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 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	+	+
Microsoft Virtual PC 2004 et 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		

Citrix 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		Uniquement les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge.
Red Hat et Linux		
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		+
Red Hat Virtualization (géré par oVirt) 4.2, 4.3, 4.4 (disponible uniquement avec le déploiement dans le cloud)	+	+
Machines virtuelles basées sur un noyau (KVM)		+
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.3 et s'exécutant sur Red Hat Enterprise Linux 7.6, 7.7 ou CentOS 7.6, 7.7 (disponible uniquement avec le déploiement dans le cloud et une licence Advanced)	+	+
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.4 et s'exécutant sur Red Hat Enterprise Linux 8.x ou CentOS 8.x (disponible uniquement avec le déploiement dans le cloud et une licence Advanced)	+	+
Machines virtuelles basées sur un noyau (KVM) gérées par oVirt 4.5 et s'exécutant sur Red Hat Enterprise Linux 8.x ou CentOS 8.x (disponible uniquement avec le déploiement dans le cloud et une licence Advanced)	+	+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+

Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Uniquement les invités entièrement virtualisés (également appelés HVM). Les invités paravirtualisés (également appelés PV) ne sont pas pris en charge.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x à 20180425.x		+
Virtuozzo (disponible uniquement avec le déploiement dans le cloud)		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge.
Virtuozzo 7.0.13, 7.0.14	Conteneurs ploop uniquement. Les machines virtuelles ne sont pas prises en charge.	Machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge.
Virtuozzo Hybrid Server 7.5	+	Machines virtuelles uniquement. Les conteneurs ne sont pas pris en charge.
Virtuozzo Hybrid Infrastructure (disponible uniquement avec le déploiement dans le cloud)		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+

Amazon		
Instances Amazon EC2		+
Microsoft Azure		
Machines virtuelles Azure		+

* 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.

*** 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

- **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 périphérique 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.
- **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 VMware et l'agent pour Hyper-V ne sauvegardent pas les volumes LUN connectés par un initiateur iSCSI qui fonctionne sous le système d'exploitation invité. Étant donné que les hyperviseurs ESXi et Hyper-V n'ont 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 Linux contenant des volumes logiques (LVM)**

  L'agent pour VMware et l'agent pour Hyper-V ne sont pas compatibles avec les opérations suivantes pour les machines Linux avec LVM :
  - Migration P2V et V2P. Utilisez l'agent pour Linux ou un support de démarrage pour créer la sauvegarde et le support de démarrage à restaurer.
  - Exécution d'une machine virtuelle à partir d'une sauvegarde créée par l'agent pour Linux ou le support de démarrage.
  - Conversion d'une sauvegarde créée par l'agent pour Linux ou le support de démarrage vers une machine virtuelle.
- **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.
- **Démarrage sécurisé**(introduit dans VMware vSphere 6.5)

  Le démarrage sécurisé 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.
- **La sauvegarde de la configuration ESXi** n'est pas prise en charge pour VMware vSphere 7.0.

Paquets Linux

Pour ajouter les modules nécessaires au noyau Linux, le programme d'installation 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.

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 retournée par la commande est la même que dans `gcc version` dans l'étape1. 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
   ```

   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	**kernel-source**	sudo zypper install kernel-source

openSUSE	**gcc** **make** **perl**	sudo zypper install gcc sudo zypper install make sudo zypper install perl

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

Pour d'autres distributions Linux, veuillez vous référer à la documentation de la distribution concernant les noms exacts des paquets requis et les façons de les installer.

Installation manuelle des paquets

Vous pourriez devoir installer les paquets **manuellement** si :

- 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
```

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.

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
- CheckPoint Harmony Endpoint
- Chiffrement McAfee Endpoint
- Chiffrement PGP de disque complet

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 :

1. Installez le logiciel de chiffrement.
2. Installez l'agent de protection.
3. Créez Secure Zone.
4. 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. N'essayez pas de sauvegarder à l'aide d'un support de démarrage.

Procédures de restauration spécifiques au logiciel

Chiffrement de lecteur BitLocker Microsoft et CheckPoint Harmony Endpoint

Vous pouvez restaurer un système à l'aide d'une reprise avec redémarrage ou d'un support de démarrage.

Restauration avec redémarrage

Pour restaurer un système chiffré, suivez les étapes figurant dans "Restauration d'une machine physique" (p. 321).

Assurez-vous que les exigences de "Restauration avec redémarrage" (p. 328) sont remplies.

Remarque
Pour les volumes chiffrés à l'aide de Bitlocker, la reprise avec redémarrage n'est disponible que sur les ordinateurs UEFI exécutant Windows 7 et les versions ultérieures, ou Windows Server 2008 R2 et les versions ultérieures. Pour les volumes chiffrés à l'aide de CheckPoint, la reprise avec redémarrage n'est disponible que sur les ordinateurs UEFI exécutant Windows 10 et Windows 11.

La reprise avec redémarrage n'est pas disponible sur les ordinateurs BIOS ou ceux exécutant Linux ou macOS.

Reprise avec support de démarrage

1. Démarrer à partir du support de démarrage.
2. Restaurer le système.

Important
Les données sauvegardées sont restaurées sous forme non chiffrée.

3. Redémarrer le système restauré.
4. Lancez le logiciel de chiffrement.

Si vous n'avez besoin de restaurer qu'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.

Chiffrement McAfee Endpoint et PGP Whole Disk

Vous pouvez restaurer une partition système chiffrée uniquement en utilisant 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 stockages Data Domain Dell EMC

Grâce à Acronis Cyber Protect, vous pouvez utiliser les terminaux Data Domain Dell EMC comme stockage des sauvegardes. Le verrouillage de rétention (mode de gouvernance) est pris en charge.

Si le verrou de rétention est activé, 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 la sauvegarde.

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.

Pour ajouter la variable dans 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.

Pour ajouter la variable dans 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.

Pour ajouter la variable dans une appliance virtuelle

1. Connectez-vous en tant qu'administrateur à l'ordinateur avec 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'ordinateur de l'appliance virtuelle.

Configuration requise

Le tableau suivant résume les exigences en matière d'espace disque et de mémoire pour des installations standard. L'installation est effectuée avec les paramètres par défaut.

Composants à installer	Espace disque requis pour l'installation	Consommation de mémoire minimale
Agent pour Windows	850 Mo	150 Mo
L'agent pour Windows et un des agents suivants : • Agent pour SQL • Agent pour Exchange	950 Mo	170 Mo
L'agent pour Windows et un des agents suivants : • Agent pour VMware (Windows) • Agent pour Hyper-V	1 170 Mo	180 Mo
Agent pour Office 365	500 Mo	170 Mo
Agent pour Linux	2 Go	130 Mo
Agent pour Mac	500 Mo	150 Mo

Pour les déploiements sur site uniquement		
Serveur de gestion sous Windows	1,7 Go	200 Mo
Serveur de gestion sous Linux	1,5 Go	200 Mo
Serveur de gestion et agent pour Windows	2,4 Go	360 Mo
Serveur de gestion et agents sur une machine exécutant Windows, Microsoft SQL Server, Microsoft Exchange et les services de domaine Active Directory	3,35 Go	400 Mo
Serveur de gestion et agent pour Linux	4 Go	340 Mo
Nœud de stockage et agent pour Windows • Plate-forme 64 bits uniquement • Pour utiliser la déduplication, 8 Go de RAM minimum sont requis. Pour plus d'informations, voir "Meilleures pratiques pour la déduplication" (p. 646).	1,1 Go	330 Mo

Lors de la sauvegarde, un agent utilise en général environ 350 Mo de mémoire (mesure effectuée lors de la sauvegarde d'un volume de 500 Go). Le pic de consommation peut atteindre jusqu'à 2 Go en fonction du volume et du type de données traitées.

Les sauvegardes dans des jeux de sauvegarde volumineux (600 Go ou plus) nécessitent environ 1 Go de mémoire RAM pour 1 To de jeu de sauvegardes.

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

Dans les systèmes x64, les opérations avec support de démarrage et restauration de disque avec redémarrage nécessitent au moins 2 Go de mémoire.

Un serveur de gestion avec une charge de travail enregistrée consomme 200 Mo de mémoire. Une charge de travail est tout type de ressource protégée, par exemple une machine physique, une machine virtuelle, une boîte aux lettres ou une instance de base de données. Chaque charge de travail supplémentaire ajoute environ 2 Mo. L'espace mémoire consommé par un serveur avec 100 charges de travail enregistrées est donc d'environ 400 Mo en plus du système d'exploitation et des applications exécutées.

Le nombre maximal de charges de travail enregistrées est de 900 à 1 000. Cette limite provient de la base de données SQLite intégrée au serveur de gestion.

Pour ignorer cette limite, indiquez une instance Microsoft SQL Server externe pendant l'installation du serveur de gestion. À l'aide d'une base de données SQL externe, vous pouvez enregistrer jusqu'à 8 000 charges de travail dans le serveur de gestion sans que les performances soient réduites de

façon importante. Avec 8 000 charges de travail enregistrées, l'instance SQL Server consommera environ 8 Go de RAM.

Pour de meilleures performances de sauvegarde, gérez les charges de travail par groupes de 500 maximum.

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.

Le tableau ci-dessous répertorie les systèmes de fichiers qui peuvent être sauvegardés et restaurés. Les limites s'appliquent aux agents comme au support de démarrage.

<table>
<tr><th rowspan="2">Système de fichiers</th><th colspan="4">Pris en charge par</th><th rowspan="2">Limites</th></tr>
<tr><th>Agents</th><th>Support de démarrage WinPE</th><th>Support de démarrage basé sur un environnement Linux</th><th>Support de démarrage Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Tous les agents</td><td>+</td><td>+</td><td>+</td><td rowspan="4">Aucune limite</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td rowspan="2">Agent pour Mac</td><td>-</td><td>-</td><td>+</td></tr>
<tr><td>APFS</td><td>-</td><td>-</td><td>+</td><td>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.</td></tr>
</table>

JFS	Agent pour Linux	-	+	-	• Il n'est pas possible d'exclure des fichiers d'une sauvegarde de disque • Impossible d'activer une sauvegarde incrémentielle/différentielle
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	• Il n'est pas possible d'exclure des fichiers d'une sauvegarde de disque • Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration
ReFS	Tous les agents	+	+	+	
XFS		+	+	+	• Il n'est pas possible d'exclure des fichiers d'une sauvegarde de disque • Impossible d'activer une sauvegarde incrémentielle/différentielle • Il n'est pas possible de redimensionner des volumes pendant une restauration • La récupération des fichiers à partir d'une sauvegarde stockée sur une bande n'est pas prise en charge
Linux swap	Agent	-	+	-	Aucune limite

	pour Linux				
exFAT	Tous les agents	+	+ Un support de démarrage ne peut pas être utilisé pour la reprise si la sauvegarde *est stockée sur* exFAT	+	• Seule la sauvegarde de disque/volume est prise en charge • Il n'est pas possible d'exclure des fichiers d'une sauvegarde • Des fichiers individuels ne peuvent pas être restaurés à partir d'une sauvegarde

Le logiciel passe automatiquement en mode secteur par secteur lorsque la sauvegarde présente des systèmes de fichiers non reconnus ou non pris en charge. 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.

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 d'Acronis VSS Provider. 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 est non liée à la fonctionnalité de déduplication d'Acronis Backup.

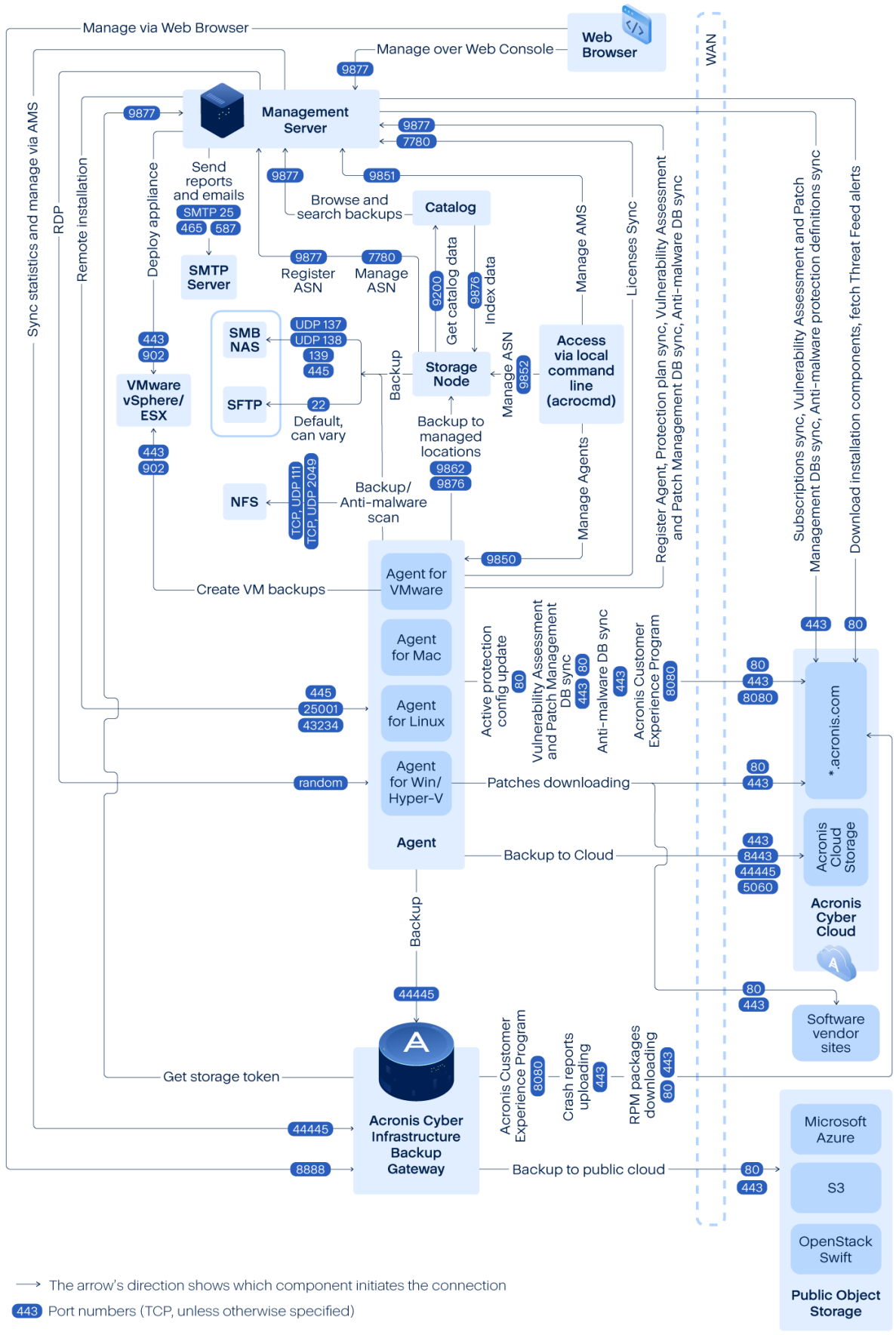
Diagramme de connexion au réseau pour Acronis Cyber Protect

Cette rubrique contient les diagrammes de connexion pour Acronis Cyber Protect.

Consultez notre base de connaissances pour obtenir une liste des ports, services et processus que Acronis Cyber Protect utilise :

- Pour Windows, consultez Windows services and processes (65663).
- Pour Linux, consultez Linux components, services, and processes (67276).

Diagramme de connexion au réseau - Cyber Protect



Important
Les ports sortants de votre diagramme réseau sont dynamiques. Certains services peuvent également utiliser les ports dynamiques pour les connexions entrantes. Lorsque vous résolvez les problèmes de réseau, vérifiez que le trafic par les ports dynamiques est autorisé.

Les ports dynamiques sont gérés par le système d'exploitation et sont affectés de manière aléatoire. Sous Windows, la plage de ports dynamiques par défaut est comprise entre 49152 et 65535. Cette plage peut varier en fonction du système d'exploitation et peut être modifiée manuellement.

Le **serveur de gestion** est le composant central de Acronis Cyber Protect. Il présente deux ports TCP : 7780 et 9877. Le port 9877, protégé par TLS, est utilisé pour fournir à la fois l'API REST et une interface utilisateur basée sur le Web. Les terminaux de l'API REST authentifient les demandes à l'aide de jetons JWT qui sont soit représentés comme un en-tête HTTP distinct, soit chiffrés en tant que cookie HTTP. Le port 7780 met en place le protocole ZeroMQ à l'aide de l'authentification et du chiffrement ZMTP CURVE. Le port 7780 est utilisé par les agents et le nœud de stockage pour échanger des messages de gestion avec le serveur de gestion de façon asynchrone. Le serveur de gestion communique aussi avec les services cloud pour télécharger des mises à jour via les ports HTTP standard et HTTPS.

Le **nœud de stockage** est le principal composant de Acronis Cyber Protect. Il présente le port TCP 9876. Ce port est utilisé pour envoyer et recevoir des données de sauvegarde. Le transport est protégé par TLS et l'authentification se fait par un TLS mutuel. Le protocole de niveau application est exclusif à Acronis. Le nœud de stockage communique avec les systèmes de stockage de l'infrastructure principale à l'aide des protocoles et des mécanismes d'authentification adéquats.

Le **catalogue** est un composant d'appui de Acronis Cyber Protect. Il indexe les données sur le nœud de stockage en y accédant via le port 9876, et présente l'index sur le port 9200.

La **passerelle de sauvegarde** met en place la génération suivante du protocole d'accès aux données exclusives à Acronis. Le même composant est utilisé dans Acronis Cyber Cloud si le client choisit la sauvegarde cloud. Le port TCP 44445, enregistré auprès de l'IANA, est utilisé par la passerelle. La protection de données s'effectue via le TLS et l'authentification se fait via un TLS mutuel. La passerelle de sauvegarde peut aussi utiliser le port 8888 pour le service de gestion basé sur HTTP.

L'**agent** communique avec le serveur de gestion, le nœud de stockage et la passerelle de sauvegarde via les ports, comme décrit ci-dessus. L'agent peut aussi communiquer avec des services de fichiers basés sur des normes (SMB, NFS) quand ils sont utilisés en tant que destination de sauvegarde. Les ports standard et les protocoles d'authentification adéquats sont alors employés. L'agent pour VMware a recours à l'API VMware vSphere via les ports définis par VMware vSphere lorsqu'une telle fonctionnalité est configurée.

L'évaluation des vulnérabilités pour Linux est mise en œuvre via un service CVSS déployé dans Acronis Cyber Cloud. Les agents de protection choisissent de façon dynamique le centre de données le plus proche via un ping depuis la liste https://cloud.acronis.com/services.json.

Déploiement sur site

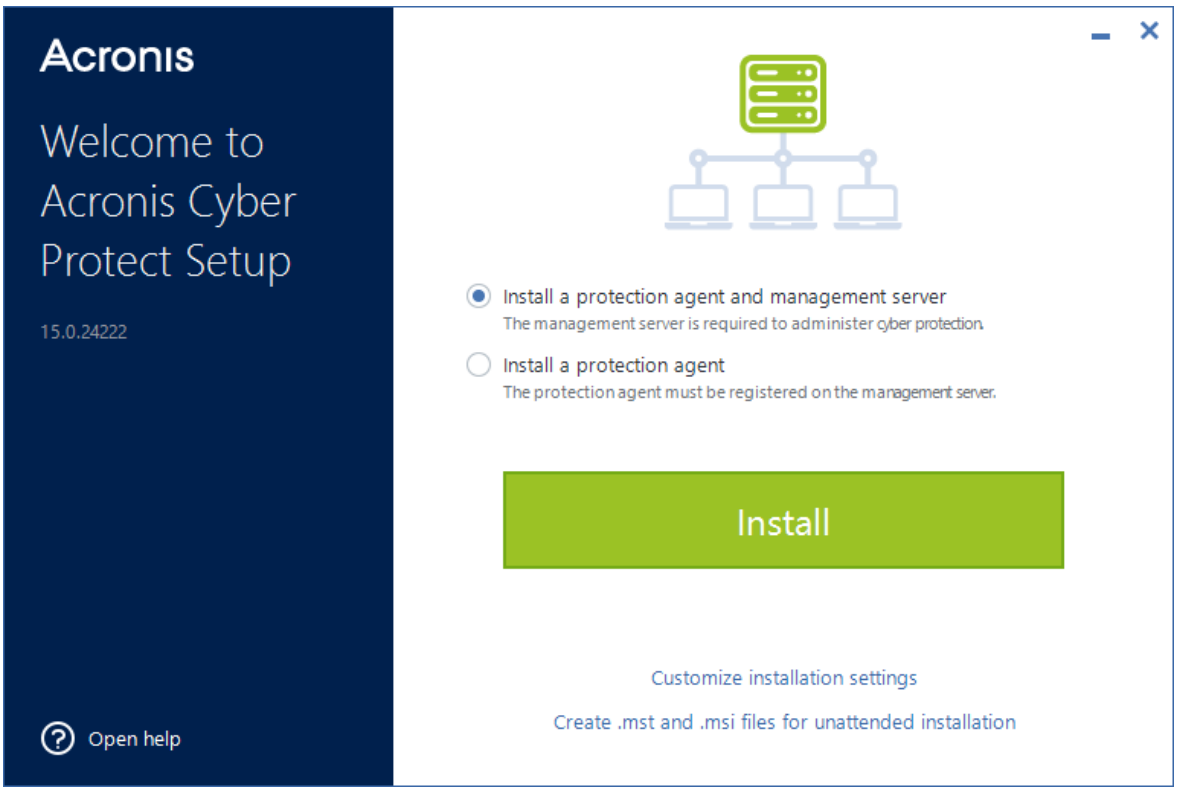
Un déploiement sur site inclut un certain nombre de composants logiciels décrits dans la section "Composants" (p. 48). Pour en savoir plus sur l'interaction entre ces composants et les ports requis, consultez "Diagramme de connexion au réseau pour Acronis Cyber Protect" (p. 82).

Installation du serveur d'administration

Installation sous Windows

Pour installer le serveur de gestion

1. Connectez-vous comme administrateur et lancez le programme d'installation d'Acronis Cyber Protect.
2. [Facultatif] Pour changer la langue du programme d'installation, cliquez sur **Configurer la langue**.
3. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
4. Conservez les paramètres par défaut **Installer un agent de protection et un serveur de gestion**.



5. Effectuez l'une des actions suivantes :

- Cliquez sur **Installer**.

  C'est le moyen le plus simple d'installer le produit. La plupart des paramètres d'installation seront définis sur leurs valeurs par défaut.

  Les composants suivants seront installés :

  - Serveur de gestion
  - Composants pour l'installation à distance
  - Agent pour Windows
  - Autres agents (l'agent pour Hyper-V, l'agent pour Exchange, l'agent pour SQL et l'agent pour Active Directory), si l'application ou l'hyperviseur respectif est détecté sur la machine
  - Bootable Media Builder
  - Outil de ligne de commande
  - Moniteur Cyber Protect
- Cliquez sur **Personnaliser les paramètres d'installation** pour la configuration.

  Vous pourrez sélectionner les composants à installer et spécifier des paramètres supplémentaires. Pour plus d'informations, veuillez consulter l'article "Personnalisation des paramètres d'installation" (p. 87).
- Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance** pour extraire les packages d'installation. Vérifiez ou modifiez les paramètres d'installation qui seront ajoutés au fichier .mst, puis cliquez sur **Générer**. Les étapes suivantes de cette procédure ne sont pas nécessaires.

  Si vous souhaitez déployer des agents via la règle de groupe, reportez-vous à "Déploiement des agents via la stratégie de groupe" (p. 182).

6. Effectuez l'installation.
7. Une fois l'installation terminée, cliquez sur **Fermer**.

Pour commencer à utiliser votre serveur de gestion, activez-le en vous connectant à votre compte Acronis ou grâce un fichier d'activation.

Personnalisation des paramètres d'installation

Cette section présente les paramètres qui peuvent être modifiés pendant l'installation.

Composants à installer

Selon que vous installez un serveur de gestion et un agent de protection, ou seulement un agent de protection, les composants suivants seront sélectionnés par défaut :

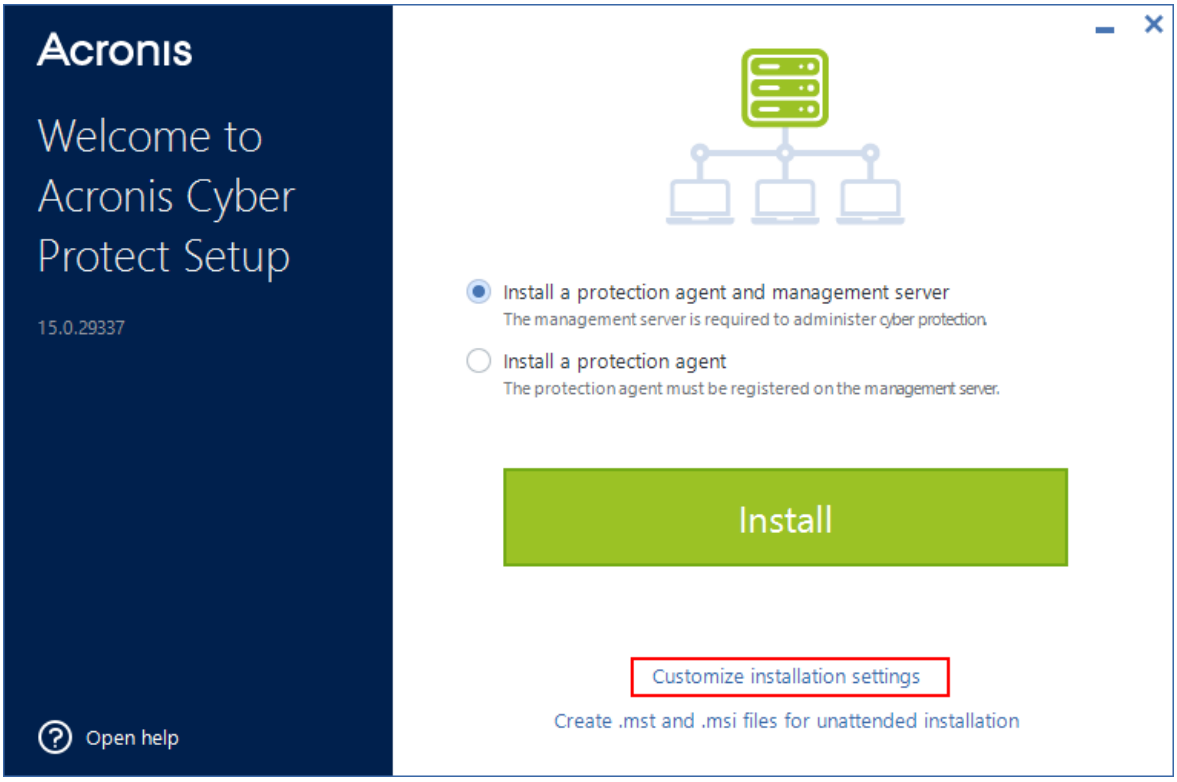
Serveur de gestion et agent de protection	Agent de protection uniquement
Serveur de gestion	Agent pour Windows
Composants pour l'installation à distance	Bootable Media Builder

Serveur de gestion et agent de protection	Agent de protection uniquement
Agent pour Windows	Outil de ligne de commande
Bootable Media Builder	Cyber Protect Moniteur
Outil de ligne de commande	
Cyber Protect Moniteur	

Pour la liste complète des composants disponibles, reportez-vous à "Composants" (p. 48).

Pour installer les composants facultatifs

1. Dans l'assistant d'installation, cliquez sur **Personnaliser les paramètres d'installation**.



2. Dans **Éléments à installer**, cliquez sur **Modifier**.
3. Sélectionnez les composants souhaités, puis cliquez sur **Terminé**.
4. Si vous y êtes invité, configurez les paramètres pour les composants sélectionnés.
5. Cliquez sur **Installer**.

Compte d'ouverture de session du service

Vous pouvez changer le compte via lequel l'agent ou le service de gestion s'exécutera, en utilisant respectivement les options **Compte d'ouverture de session pour le service de l'agent** et **Compte d'ouverture de session pour le service de serveur de gestion**.

Vous pouvez choisir 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. Cette option 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** (par défaut pour le service du serveur de gestion et le service du nœud de stockage)

  Les noms de compte sont respectivement **Acronis Agent User**, **AMS User** et **ASN User** pour l'agent, le serveur de gestion et les services du nœud de stockage.
- **Utiliser le compte suivant**

  Si vous installez le produit sur un contrôleur de domaine, le programme d'installation vous invite à spécifier des comptes existants (ou le même compte) pour chaque service. Pour des raisons de sécurité, le programme d'installation 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.

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

  En outre, sélectionner **Utiliser le compte suivant** vous permet d'utiliser l'authentification Windows pour Microsoft SQL Server si vous configurez le serveur de gestion avec une base de données SQL.

Si vous choisissez l'option **Créer un nouveau compte** ou **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 affectés lors de l'installation, le composant correspondant pourrait ne pas fonctionner correctement ou ne pas fonctionner.

Droits d'utilisateur requis pour le compte de connexion au service

Un agent de protection s'exécute en tant que **service de machine gérée (MMS)** sur une machine Windows. Le compte sur lequel l'agent s'exécute doit avoir les droits suivants pour que l'agent fonctionne correctement :

1. L'utilisateur MMS doit être inclus dans les groupes **Opérateurs de sauvegarde** et **Administrateurs**. Sur un contrôleur de domaine, l'utilisateur doit être inclus dans le groupe **Admins de domaine**.
2. L'utilisateur MMS doit disposer de l'autorisation **Contrôle complet** sur le dossier `%PROGRAMDATA%\Acronis` (sous Windows XP et Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) et ses sous-dossiers.

3. L'utilisateur MMS doit disposer de l'autorisation **Contrôle complet** sur certaines clés de la base de registre pour la clé suivante : `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. L'utilisateur MMS doit être affecté aux droits d'utilisateur suivants dans Windows :
   - **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**

L'**utilisateur ASN** doit disposer de droits d'administrateur local sur la machine sur laquelle le nœud de stockage Acronis est installé.

Pour affecter les droits d'utilisateur sous Windows

Remarque
Cette procédure utilise le droit d'utilisateur **Ouvrir une session en tant que service** en tant qu'exemple. Les étapes pour les autres droits d'utilisateur sont identiques.

1. Connectez-vous à l'ordinateur en tant qu'administrateur.
2. Dans **Panneau de configuration**, ouvrez **Outils d'administration**. Autrement, appuyez sur Win+R sur le clavier, saisissez **control admintools**, puis appuyez sur Entrée.
3. Ouvrez **Stratégie de sécurité locale**.
4. Développez **Stratégies locales** puis cliquez sur **Attribution des droits utilisateur**.
5. Dans le panneau de droite, cliquez avec le bouton droit sur **Ouvrir une session en tant que service**, puis sélectionnez **Propriétés**.
6. Cliquez sur le bouton **Ajouter un utilisateur ou un groupe...** pour ajouter un nouvel utilisateur.
7. Dans la fenêtre **Sélectionnez des utilisateurs ou des groupes**, trouvez l'utilisateur que vous souhaitez ajouter, puis cliquez sur **OK**.
8. Cliquez sur **OK** dans la fenêtre **Propriétés d'ouverture de session en tant que service** afin d'enregistrer les modifications.

Remarque
L'utilisateur que vous ajoutez au droit d'utilisateur **Ouverture de session en tant que service** ne doit pas être répertorié dans la stratégie **Interdire l'ouverture de session en tant que service** sous **Stratégie de sécurité locale**.

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

Base de données pour le serveur de gestion

Vous pouvez configurer le serveur de gestion à l'aide des bases de données suivantes :

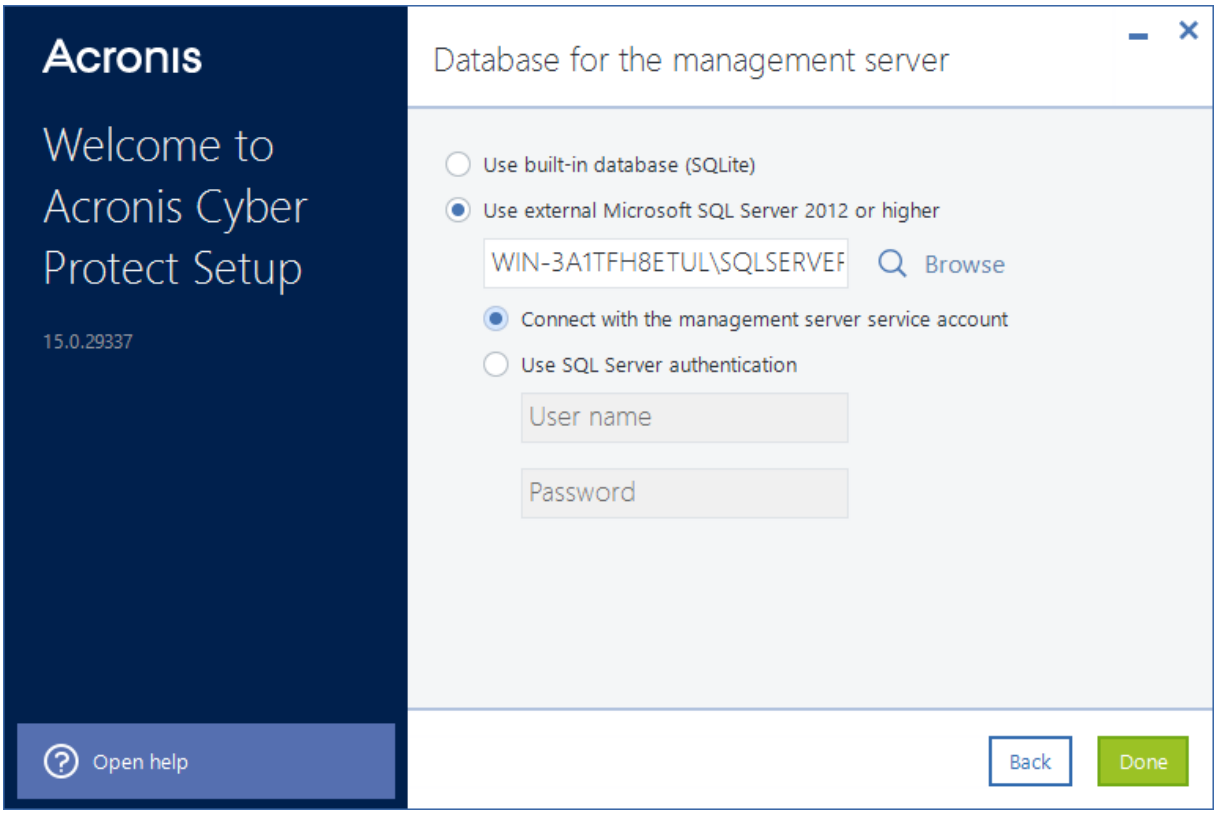
- SQLite

  Par défaut, le serveur de gestion utilise la base de données SQLite intégrée. Cela permet d'enregistrer environ 900 à 1000 charges de travail sur le serveur de gestion. SQLite n'est pas compatible avec le service d'analyse.
- Microsoft SQL

  Microsoft SQL permet d'enregistrer jusqu'à 8000 charges de travail sur le serveur de gestion sans que les performances soient réduites de façon importante. La même instance Microsoft SQL peut être utilisée par le serveur de gestion, le service d'analyse et d'autres programmes.

  Les versions suivantes de MS SQL Server sont prises en charge :
  - Microsoft SQL Server 2019 (sous Windows)
  - Microsoft SQL Server 2017 (sous Windows)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

Si l'instance Microsoft SQL est celle par défaut, **MSSQLSERVER**, vous pouvez spécifier uniquement le nom de la machine sur laquelle elle s'exécute. Si l'instance a un nom personnalisé, vous devez le spécifier en utilisant le format suivant : `nom de la machine\nom de l'instance`.



Remarque
Assurez-vous que le service SQL Server Browser et le protocole TCP/IP sont activés sur la machine qui exécute l'instance Microsoft SQL. Pour plus d'informations sur la façon de démarrer le service SQL Server Browser, reportez-vous à http://msdn.microsoft.com/en-us/library/ms189093.aspx. Vous pouvez activer le protocole TCP/IP en utilisant une procédure similaire.

Pour vous connecter à l'instance Microsoft SQL spécifiée, vous pouvez utiliser les méthodes d'authentification suivantes :

- Authentification Windows (**connectez-vous avec le compte du service de serveur de gestion**)
  Vous pouvez utiliser cette méthode si vous avez configuré le compte de connexion pour le service de serveur de gestion à l'aide de l'option **Utiliser le compte suivant**, par exemple en précisant `<NOM DE LA MACHINE>\Administrateur`. Le compte spécifié doit avoir le rôle **dbcreator** ou **sysadmin** dans Microsoft SQL Server.
  Pour plus d'informations sur le compte de connexion, reportez-vous à "Droits d'utilisateur requis pour le compte de connexion au service" (p. 89).
- Authentification SQL Server
  Vous pouvez toujours utiliser cette méthode. Le compte spécifié doit avoir le rôle **dbcreator** ou **sysadmin** dans Microsoft SQL Server.

Service d'analyse

Le service d'analyse est un composant facultatif, qui permet de rechercher les malware dans les sauvegardes situées soit dans un stockage dans le cloud, soit dans un dossier réseau ou local. Le service d'analyse nécessite que le serveur de gestion soit installé sur la même machine.

L'installation du service d'analyse donne accès aux fonctionnalités suivantes :

- Plan d'analyse des sauvegardes
- Widget des détails de l'analyse de la sauvegarde
- Liste blanche d'entreprise
- Restauration sûre
- La colonne **Statut** dans la liste des sauvegardes.

Vous pouvez installer le service d'analyse lors de l'installation du serveur de gestion ou ultérieurement en modifiant l'installation existante. Pour plus d'informations sur la façon d'installer les composants facultatifs tels que le service d'analyse, reportez-vous à "Pour installer les composants facultatifs" (p. 88).

Important
Le service d'analyse n'est pas compatible avec la base de données SQLite utilisée par le serveur de gestion.

Vous pouvez configurer le service d'analyse avec une base de données Microsoft SQL ou PostgreSQL. Pour plus d'informations sur le choix de l'une ou de l'autre, reportez-vous à "Base de données pour le service d'analyse" (p. 94).

Base de données pour le service d'analyse

Le service d'analyse n'est pas compatible avec SQLite, la base de données utilisée par défaut par le serveur de gestion.

Si votre serveur de gestion utilise SQLite, vous ne pouvez configurer le service d'analyse qu'avec une base de données PostgreSQL. PostgreSQL 9.6 et les versions ultérieures sont prises en charge.

Si votre serveur de gestion utilise Microsoft SQL Server, vous pouvez configurer le service d'analyse avec la même base de données, sans paramètres supplémentaires. Vous pouvez également configurer le service d'analyse avec une base de données PostgreSQL.

Pour configurer le service d'analyse avec une base de données PostgreSQL

1. Dans l'assistant d'installation, sous **Base de données pour le service d'analyse**, cliquez sur **Modifier**.
2. Sélectionnez **Base de données de serveur PostgreSQL**.
3. Spécifiez le nom de l'hôte de l'instance PostgreSQL, ou l'adresse IP et le port.
4. Spécifiez les identifiants d'un utilisateur qui a créé le privilège **CREATEDB** ou qui est un superutilisateur.

   Remarque
   La méthode d'authentification SCRAM-SHA-256 dans PostgreSQL 10 et dans les versions ultérieures n'est pas prise en charge.

5. Cliquez sur **Valider**.

Ports

Vous pouvez personnaliser le port qui sera utilisé par un navigateur Web pour accéder au serveur de gestion (par défaut : 9877) et le port qui sera utilisé pour la communication entre les composants des produits (par défaut : 7780). La modification de ce dernier port après l'installation nécessitera le réenregistrement de tous les composants.

Le pare-feu Windows est configuré automatiquement lors de l'installation. Si vous utilisez un autre pare-feu, assurez-vous que les ports sont ouverts pour les requêtes entrantes et sortantes sur ce pare-feu.

Serveur proxy

Vous pouvez choisir si les agents de protection doivent utiliser ou non un serveur proxy HTTP lors d'une sauvegarde et d'une restauration à partir du stockage dans le cloud.

De plus, vous utilisez le même serveur proxy pour la communication entre les composants Acronis Cyber Protect.

Pour utiliser un serveur proxy, spécifiez son nom d'hôte ou son adresse IP, et le numéro de port. Si le serveur proxy nécessite une authentification, spécifiez les identifiants.

Remarque
La mise à jour des définitions de protection (définitions antivirus et antimalware, définitions de détection avancées, définitions de l'évaluation des vulnérabilités et de la gestion des correctifs) n'est pas possible en cas d'utilisation d'un serveur proxy.

Installation sous Linux

Préparation

1. Si vous souhaitez installer l'agent pour Linux avec le serveur de gestion, assurez-vous que les packages Linux nécessaires sont installés sur la machine.
2. Choisissez la base de données qui doit être utilisée par le serveur de gestion.

Limites

Les serveurs de gestion exécutés sur des ordinateurs Linux ne prennent pas en charge l'installation à distance des agents de protection, utilisée par exemple dans la procédure de découverte automatique. Pour en savoir plus sur les éventuelles solutions de contournement, consultez notre base de connaissances : https://kb.acronis.com/content/69553.

Installation

Pour installer le serveur de gestion, vous avez besoin d'au moins 4 Go d'espace disque libre.

Pour installer le serveur de gestion

1. 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>
   ```

2. Acceptez les termes du contrat de licence.
3. [Facultatif] Sélectionnez les composants que vous souhaitez installer.
   Par défaut, les composants suivants seront installés :
   - Serveur de gestion
   - Agent pour Linux
   - Bootable Media Builder
4. Spécifiez le port qui sera utilisé par un navigateur Web pour accéder au serveur de gestion. La valeur par défaut est 9877.
5. Spécifiez le port pour la communication entre les composants des produits La valeur par défaut est 7780.
6. Cliquez sur **Suivant** pour procéder à l'installation.

7. Une fois l'installation terminée, sélectionnez **Ouvrir la console Web**, puis cliquez sur **Quitter**. La console Web Cyber Protect s'ouvrira dans votre navigateur Web par défaut.

Pour commencer à utiliser votre serveur de gestion, activez-le en vous connectant à votre compte Acronis ou grâce un fichier d'activation.

Appliance Acronis Cyber Protect

Grâce à l'appliance Acronis Cyber Protect, vous pouvez facilement obtenir une machine virtuelle via le logiciel suivant :

- CentOS
- Composants Acronis Cyber Protect :
  - Serveur de gestion
  - Agent pour Linux
  - Agent pour VMware (Linux)

Le matériel est fourni en tant qu'archive .zip. L'archive contient les fichiers .ovf et .iso. Vous pouvez déployer le fichier .ovf vers un hôte ESXi ou utilisez un fichier .iso pour démarrer une machine virtuelle existante. L'archive contient également un fichier .vmdk qui doit être placé dans le même répertoire que le fichier .ovf.

Remarque
Le client VMware Host (un client web utilisé pour gérer des hôtes ESXi 6.0+ autonomes) ne permet pas le déploiement de modèles OVF avec une image ISO à l'intérieur. Si c'est votre cas, créez une machine virtuelle avec la configuration requise ci-dessous et utilisez le fichier .iso pour installer le logiciel.

La configuration requise pour le matériel virtuel est la suivante :

- Configuration système minimale requise :
  - 2 processeurs
  - 6 Go de RAM
  - Un disque virtuel de 10 Go (40 Go recommandé)
- Dans les paramètres de la machine virtuelle VMware, cliquez sur l'onglet **Options** > **Général** > **Paramètres de configuration**, puis assurez-vous que la valeur du paramètre `disk.EnableUUID` est `true`.

Limites

Les serveurs de gestion exécutés sur des ordinateurs Linux, y compris l'appliance Acronis Cyber Protect, ne prennent pas en charge l'installation à distance des agents de protection utilisée par exemple dans la procédure de découverte automatique. Pour en savoir plus sur les éventuelles solutions de contournement, consultez notre base de connaissances : https://kb.acronis.com/content/69553.

Installation du logiciel

1. Effectuez l'une des actions suivantes :
   - Déployez l'appliance à partir du fichier .ovf. À la fin du déploiement, allumez la machine résultante.
   - Démarrez une machine virtuelle existante à partir d'un fichier .iso.
2. Sélectionnez **Installer ou mettre à jour Acronis Cyber Protect**, puis appuyez sur **Entrée**. Patientez jusqu'à l'apparition de la fenêtre de configuration initiale.
3. [Facultatif] Pour modifier les paramètres d'installation, sélectionnez **Modifier les paramètres**, puis appuyez sur **Entrée**. En complément, vous pouvez spécifier les paramètres suivants :
   - Le nom d'hôte de l'appliance (par défaut, `AcronisAppliance-<partie aléatoire>`).
   - Le mot de passe pour le compte root (superutilisateur) qui sera utilisé pour se connecter à la console Web Cyber Protect (par défaut, **non spécifié**).

     Si vous laissez la valeur par défaut, après l'installation d'Acronis Cyber Protect, vous serez invité à entrer le mot de passe. Sans ce mot de passe, vous ne pourrez pas vous connecter à la console Web Cyber Protect et à la console Web Cockpit.
   - Paramètres du réseau d'une carte d'interface réseau :
     - **Utilisez DHCP** (par défaut)
     - **Paramétrez une adresse IP statique**

     Si la machine possède plusieurs cartes d'interface réseau, le logiciel sélectionne l'une d'elle de façon aléatoire et lui applique ces paramètres.
4. Sélectionnez **Installer avec les paramètres actuels**.

En conséquence, CentOS et Acronis Cyber Protect seront installés sur l'ordinateur.

Autres actions

Une fois l'installation terminée, le logiciel affiche les liens dans la console Web Cyber Protect et dans la console web Cockpit. Connectez-vous à la console Web Cyber Protect pour commencer à utiliser Acronis Cyber Protect : ajoutez d'autres terminaux, créez des plans de sauvegarde, etc.

Pour ajouter des machines virtuelles ESXi, cliquez sur **Ajouter** > **VMware ESXi**, puis spécifiez l'adresse et les informations d'identification pour le vCenter Server ou l'hôte autonome ESXi.

Aucun paramètre d'Acronis Cyber Protect n'est configuré dans la console Web Cockpit. La console est fournie pour aider et dépanner.

Mise à jour du logiciel

1. Téléchargez et extrayez l'archive .zip avec la nouvelle version du matériel.
2. Démarrez la machine avec le fichier .iso extrait dans l'étape précédente.
   a. Sauvegardez le fichier .iso dans votre magasin de données vSphere.
   b. Connectez le fichier .iso au lecteur CD/DVD de la machine.

c. Redémarrez la machine.

d. [Uniquement lors de la première mise à jour] Appuyez sur **F2**, puis modifiez l'ordre de démarrage pour que le lecteur CD/DVD soit en premier.

3. Sélectionnez **Installer ou mettre à jour Acronis Cyber Protect**, puis appuyez sur **Entrée**.
4. Sélectionnez **Mettre à jour**, puis appuyez sur **Entrée**.
5. Une fois la mise à jour terminée, déconnectez le fichier .iso du lecteur CD/DVD de la machine.

En conséquence, Acronis Cyber Protect sera mis à jour. Si la version CentOS dans le fichier .iso est plus récente que la version sur le disque, le système d'exploitation sera mis à jour avant Acronis Cyber Protect.

Ajout d'ordinateurs depuis la console Web Cyber Protect

Vous pouvez ajouter un ordinateur de l'une des manières suivantes :

- En téléchargeant le programme d'installation et en l'exécutant localement sur la machine cible.
- En installant à distance un agent de protection sur la machine cible.

Limites

- L'installation à distance n'est disponible qu'avec un serveur de gestion s'exécutant sur un ordinateur Windows. Les machines cibles doivent également exécuter Windows.
- L'installation à distance n'est pas prise en charge sur les ordinateurs exécutant Windows XP.
- L'installation à distance n'est pas prise en charge sur les contrôleurs de domaine. Pour savoir comment installer un agent de protection sur un contrôleur de domaine, reportez-vous à "Installation sous Windows" (p. 107). Assurez-vous de personnaliser les paramètres d'installation en sélectionnant **Utiliser le compte suivant** sous **Compte de connexion pour le service de l'agent**. Pour en savoir plus sur cette option, reportez-vous à "Droits d'utilisateur requis pour le compte de connexion au service" (p. 89).

Ajout d'une machine fonctionnant sous Windows

Vous pouvez ajouter un ordinateur Windows en installant un agent de protection à distance, dans la console Web Cyber Protect ou en téléchargeant et en exécutant le programme d'installation localement.

Pour installer un agent à distance

Important
Avant de démarrer l'installation, assurez-vous que les conditions préalables à l'installation à distance sont satisfaites et qu'un agent au moins de votre environnement peut être utilisé comme agent de déploiement. Pour plus d'informations, voir "Conditions préalables à l'installation à distance" (p. 100) et "Agent de déploiement" (p. 101).

1. Dans la console Web Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur **Ajouter**.
3. [Pour installer l'agent pour Windows] Cliquez sur **Windows**.
4. [Pour installer un autre agent pris en charge] Cliquez sur le bouton correspondant à l'application que vous souhaitez protéger.
   Les agents suivants sont disponibles :
   - Agent pour Hyper-V
   - Agent pour SQL + Agent pour Windows
   - Agent pour Exchange + Agent pour Windows
     Si vous cliquez sur **Microsoft Exchange Server** > **Boîtes aux lettres Exchange** et si au moins un agent pour Exchange est déjà enregistré, passez à l'étape 9.
   - Agent pour Active Directory + Agent pour Windows
   - Agent pour Office 365
5. Dans le panneau qui s'ouvre, sélectionnez l'agent de déploiement.
6. Indiquez le nom d'hôte ou l'adresse IP de la machine cible, ainsi que les identifiants d'un compte disposant de droits d'administration sur cet ordinateur.
   Nous vous recommandons d'utiliser le compte administrateur intégré. Pour utiliser un autre compte, ajoutez-le au groupe Administrateurs et modifiez le registre de la machine cible en suivant les indications de l'article suivant : https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
7. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.
   Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.
8. Cliquez sur **Installer**.
9. [Si vous avez sélectionné **Microsoft Exchange Server** > **Boîtes aux lettres Exchange** à l'étape 4] Spécifiez l'ordinateur sur lequel le rôle de serveur **Accès client** (CAS) de Microsoft Exchange Server est activé. Pour obtenir plus d'informations, consultez l'article "Sauvegarde de boîte de réception" (p. 464).

Pour télécharger et installer un agent localement

1. Dans la console Web Cyber Protect, cliquez sur l'icône de compte en haut à droite, puis sur **Téléchargements**.
2. Cliquez sur le nom du programme d'installation Windows dont vous avez besoin.
   Le programme d'installation est téléchargé sur votre ordinateur.
3. Exécutez le programme d'installation sur l'ordinateur que vous souhaitez protéger. Pour obtenir plus d'informations, consultez l'article "Installation sous Windows" (p. 107).

Conditions préalables à l'installation à distance

- 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 cette machine.
- Pour réussir l'installation sur une machine distante qui n'est *pas* membre d'un domaine Active Directory, le contrôle de compte utilisateur (CCU) doit être *désactivé* sur cette machine. Pour en savoir plus sur la façon de le désactiver, consultez "Pour désactiver l'UAC" (p. 101).
- Par défaut, les identifiants du compte administrateur intégré sont requis pour l'installation à distance sur tout ordinateur 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 (CCU) doivent être *désactivées*. Pour en savoir plus sur la façon de les désactiver, consultez "Pour désactiver les restrictions à distance UAC" (p. 101).
- 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 réseau et partage** > **Modifier les paramètres de partage avancés**.
- Acronis Cyber Protect 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.

Remarque
L'installation à distance n'est pas prise en charge sur les ordinateurs exécutant Windows XP.

Remarque
L'installation à distance n'est pas prise en charge sur les contrôleurs de domaine. Pour savoir comment installer un agent de protection sur un contrôleur de domaine, reportez-vous à "Installation sous Windows" (p. 107). Assurez-vous de personnaliser les paramètres d'installation en sélectionnant **Utiliser le compte suivant** sous **Compte de connexion pour le service de l'agent**. Pour en savoir plus sur cette option, reportez-vous à "Droits d'utilisateur requis pour le compte de connexion au service" (p. 89).

Exigences pour le contrôle de compte d'utilisateur (UAC)

Sur un ordinateur exécutant Windows 7 ou une version ultérieure, 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

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**.

Agent de déploiement

Pour que vous puissiez installer les agents de protection sur les machines distantes depuis la console Web Cyber Protect, un agent au moins doit être déjà installé dans votre environnement. Cet agent servira d'agent de déploiement pour l'installation à distance et se connectera au serveur de gestion et à la machine distante cible.

En général, le premier agent de protection de l'environnement est celui que vous installez avec le serveur de gestion. Toutefois, vous pouvez sélectionner comme agent de déploiement chaque agent pour Windows de l'environnement.

Remarque
Lorsque vous utilisez la découverte automatique pour installer des agents de protection sur plusieurs ordinateurs, l'agent de déploiement est appelé « agent de découverte ».

Fonctionnement de l'agent de déploiement

1. L'agent de déploiement se connecte au serveur de gestion et télécharge le fichier `web_installer.exe`.
2. L'agent de déploiement se connecte à la machine distante à l'aide du nom d'hôte ou de l'adresse IP de l'ordinateur, ainsi que des identifiants administrateur que vous indiquez, puis transfère le fichier `web_installer.exe` vers cet ordinateur.
3. Le fichier `web_installer.exe` s'exécute sur la machine distante en mode sans assistance.
4. Selon le champ d'application de l'installation, le programme d'installation Web récupère des packages d'installation supplémentaires depuis le dossier `installation_files` sur le serveur de gestion, puis les installe sur la machine cible à l'aide de la commande `msiexec`.
   Le dossier `installation_files` se situe dans :
   - Windows : `\Program Files\Acronis\RemoteInstallationFiles\`
   - Linux : `/usr/lib/Acronis/RemoteInstallationFiles/`
5. Une fois l'installation terminée, l'agent est inscrit dans le serveur de gestion.

Composants pour l'installation à distance

Les composants de l'installation à distance sont installés par défaut lorsque vous installez le serveur de gestion.

Selon le système d'exploitation de l'ordinateur sur lequel s'exécute le serveur de gestion, vous trouverez ces composants dans les emplacements suivants :

- Windows : `%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux : `/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

Ces emplacements risquent de ne pas être disponibles si vous avez effectué la mise à niveau depuis une version antérieure de Acronis Cyber Protect ou si vous avez explicitement exclu **Composants pour l'installation à distance** lorsque vous avez installé le serveur de gestion. Dans ce cas, vous devez ajouter les composants de l'installation à distance manuellement en mettant à jour et en modifiant votre installation existante de Acronis Cyber Protect.

Pour ajouter les composants de l'installation à distance à une installation existante

1. Téléchargez le dernier fichier d'installation de Acronis Cyber Protect depuis le site Web Acronis.
   Sélectionnez le fichier d'installation correspondant au nombre de bits de votre système d'exploitation. Dans la plupart des cas, vous aurez besoin du fichier d'installation **Windows 64 bits**. Si vous devez installer des agents de protection à distance sur des machines 32 bits, téléchargez le fichier d'installation **Windows 32/64 bits**.
2. Sur l'ordinateur sur lequel s'exécute le serveur de gestion, démarrez le fichier d'installation, puis sélectionnez **Mettre à jour**.
3. Une fois la mise à jour terminée, redémarrez le fichier d'installation, puis sélectionnez **Modifier l'installation actuelle**.
4. Sélectionnez **Composants pour l'installation à distance**, puis cliquez sur **Terminé**.

Une fois l'installation terminée, vous pourrez installer les agents de protection sur les machines distantes depuis la console Web Cyber Protect.

Ajout d'une machine fonctionnant sous Linux

Vous ne pouvez ajouter un ordinateur Linux qu'en installant l'agent de protection localement. L'installation à distance n'est pas prise en charge.

Pour ajouter un ordinateur exécutant Linux

1. Dans la console Web Cyber Protect, cliquez sur **Tous les terminaux** > **Ajouter**.
2. Cliquez sur **Linux**.
   Le programme d'installation est téléchargé sur votre ordinateur.
3. Exécutez le programme d'installation sur l'ordinateur que vous souhaitez protéger. Pour obtenir plus d'informations, consultez l'article "Installation sous Linux" (p. 110).

Ajout d'un ordinateur fonctionnant sous macOS

Vous ne pouvez ajouter un ordinateur macOS qu'en installant l'agent de protection localement. L'installation à distance n'est pas prise en charge.

Pour ajouter un ordinateur exécutant macOS

1. Dans la console Web Cyber Protect, cliquez sur **Tous les terminaux** > **Ajouter**.
2. Cliquez sur **Mac**.
   Le programme d'installation est téléchargé sur votre ordinateur.
3. Exécutez le programme d'installation sur l'ordinateur que vous souhaitez protéger. Pour obtenir plus d'informations, consultez l'article "Installation sous macOS" (p. 111).

Ajout d'un vCenter ou d'un hôte ESXi

Quatre méthodes sont disponibles afin d'ajouter un vCenter ou un hôte ESXi autonome au serveur de gestion :

- Déploiement de l'agent pour VMware (matériel virtuel)

  Cette méthode est recommandée dans la plupart des cas. Le matériel virtuel sera déployé automatiquement sur chaque hôte géré par le vCenter spécifié. Vous pouvez sélectionner les hôtes et personnaliser les paramètres du matériel virtuel.
- Installation de l'agent pour VMware (Windows)

  Vous souhaitez peut-être installer l'agent pour VMware sur une machine physique fonctionnant sous Windows afin d'obtenir une sauvegarde sans réseau ou déchargée.
  - **Sauvegarde déchargée**

    Utilisez cette méthode si vos hôtes de production ESXi sont trop chargés pour exécuter le matériel virtuel.
  - **Sauvegarde sans LAN**

    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 ESXi et le réseau local. Pour obtenir des instructions détaillées, reportez-vous à l'article « Sauvegarde sans réseau local ».

  Si le serveur de gestion s'exécute sous Windows, l'agent sera déployé automatiquement sur la machine spécifiée. Autrement, vous devez installer l'agent.
- Inscription d'un agent pour VMware déjà installé

  Cette étape est nécessaire après une réinstallation du serveur de gestion. Vous pouvez également enregistrer et configurer l'agent pour VMware (matériel virtuel) à partir d'un modèle OVF.
- Configurer un agent pour VMware déjà enregistré

  Cette étape est nécessaire après une installation manuelle de l'agent pour VMware (Windows) ou un déploiement de l'appliance Acronis Cyber Protect. Vous pouvez également associer un agent déjà configuré à un autre vCenter Server ou hôte ESXi autonome.

Déploiement de l'agent pour VMware (matériel virtuel) via l'interface Web

1. Cliquez sur **Tous les périphériques** > **Ajouter**.
2. Cliquez sur **VMware ESXi**.
3. Sélectionnez **Déployer en tant que matériel virtuel sur chaque hôte d'un vCenter**.
4. Spécifiez l'adresse et les identifiants de vCenter Server ou de l'hôte autonome ESXi. Nous vous conseillons d'utiliser un compte auquel le rôle **Administrateur** a été attribué. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server ou ESXi.
5. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.

   Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.

6. [Facultatif] Cliquez sur **Paramètres** pour modifier les paramètres du déploiement :
   - Les hôtes ESXi sur lesquels vous souhaitez déployer l'agent (seulement si vous avez spécifié un vCenter Server lors de l'étape précédente).
   - Le nom du matériel virtuel.
   - Le magasin de données où l'appareil sera situé.
   - Le pool de ressources ou vApp dans lequel se trouvera l'appareil.
   - Le réseau auquel la carte d'interface réseau du matériel virtuel sera connectée.
   - Paramètres réseau du matériel virtuel. Vous pouvez choisir la configuration automatique DHCP ou spécifier les valeurs manuellement, y compris une adresse IP statique.
7. Cliquez sur **Déployer**.

Installation de l'agent pour VMware (Windows)

Préparation

Suivez les étapes préparatoires décrites dans la section « Ajout d'une machine fonctionnant sous Windows ».

Installation

1. Cliquez sur **Tous les périphériques** > **Ajouter**.
2. Cliquez sur **VMware ESXi**.
3. Sélectionnez **Installer à distance sur une machine exécutant Windows**.
4. Sélectionnez l'agent de déploiement.
5. Renseignez le nom d'hôte ou l'adresse IP de la machine cible, ainsi que les identifiants d'un compte disposant de privilèges d'administration sur cet ordinateur.
6. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.
   Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.
7. Cliquez sur **Connecter**.
8. Spécifiez l'adresse et les identifiants de vCenter Server ou de l'hôte autonome ESXi, puis cliquez sur **Connecter**. Nous vous conseillons d'utiliser un compte auquel le rôle **Administrateur** a été attribué. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server ou ESXi.
9. Cliquez sur **Installer** pour installer l'agent.

Inscription d'un agent pour VMware déjà installé

Cette section décrit l'enregistrement de l'agent pour VMware via l'interface Web.

Autres méthodes d'inscription :

- Vous pouvez enregistrer l'agent pour VMware (matériel virtuel) en spécifiant le serveur de gestion dans l'interface utilisateur du matériel virtuel. Consultez l'étape 3 de « Configuration du matériel virtuel » dans la section Déploiement de l'agent pour VMware (appliance virtuelle) à partir d'un modèle OVF.
- L'agent pour VMware (Windows) est enregistré au cours de son installation locale.

Pour enregistrer l'agent pour VMware

1. Cliquez sur **Tous les périphériques** > **Ajouter**.
2. Cliquez sur **VMware ESXi**.
3. Sélectionnez **Inscrire un agent déjà installé**.
4. Sélectionnez l'agent de déploiement.
5. Si vous enregistrez l'*agent pour VMware (Windows)*, spécifiez le nom d'hôte ou l'adresse IP de l'ordinateur sur lequel il est installé, ainsi que les identifiants d'un compte avec des privilèges d'administration sur celui-ci.

   Si vous enregistrez l'*Agent pour VMware (matériel virtuel)*, spécifiez le nom d'hôte ou l'adresse IP de la machine virtuelle, ainsi que les informations d'identification du vCenter Server ou de l'hôte ESXi autonome sur lequel le matériel est exécuté.
6. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.

   Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.
7. Cliquez sur **Connecter**.
8. Spécifiez le nom d'hôte ou l'adresse IP de vCenter Server ou de l'hôte ESXi, ainsi que les identifiants permettant d'y accéder, puis cliquez sur **Connecter**. Nous vous conseillons d'utiliser un compte auquel le rôle **Administrateur** a été attribué. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server ou ESXi.
9. Cliquez sur **Enregistrer** pour enregistrer l'agent.

Configurer un agent pour VMware déjà enregistré

Cette section décrit comment associer l'agent pour VMware avec un serveur vCenter ou ESXi via l'interface Web. Comme alternative, vous pouvez faire ceci dans la console de l'agent pour VMware (matériel virtuel).

En utilisant cette procédure, vous pouvez également modifier l'association existante de l'agent avec un serveur vCenter ou ESXi. Comme alternative, vous pouvez effectuer cette tâche dans la console de l'agent pour VMware (matériel virtuel) ou en cliquant sur **Paramètres** > **Agents** > l'agent > **Détails** > **vCenter/ESXi**.

Pour configurer l'agent pour VMware

1. Cliquez sur **Tous les périphériques** > **Ajouter**.
2. Cliquez sur **VMware ESXi**.
3. Le logiciel affiche l'agent pour VMware non configuré qui apparaît en premier par ordre alphabétique.
   Si tous les agents enregistrés sur le serveur de gestion sont configurés, cliquez sur **Configurer un agent déjà enregistré**, et le logiciel affichera l'agent qui apparaît en premier par ordre alphabétique.
4. Si besoin, cliquez sur **Machine avec un agent** et sélectionnez un agent à configurer.
5. Spécifiez ou changez le nom d'hôte ou l'adresse IP du vCenter Server ou de l'hôte ESXi ainsi que les identifiants permettant d'y accéder. Nous vous conseillons d'utiliser un compte auquel le rôle **Administrateur** a été attribué. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server ou ESXi.
6. Cliquez sur **Configurer** pour enregistrer les modifications.

Ajout d'un cluster Scale Computing HC3

Pour ajouter un cluster HC3 de Scale Computing au serveur de gestion Cyber Protect

1. Déployez un agent pour Scale Computing HC3 (appliance virtuelle) dans le cluster.
2. Configurez sa connexion pour ce cluster et pour le serveur de gestion Cyber Protect.

Installation locale d'agents

Installation sous Windows

Pour installer l'agent pour Windows, l'agent pour Hyper-V, l'agent pour Exchange, l'agent pour SQL ou l'agent pour Active Directory

1. Connectez-vous comme administrateur et lancez le programme d'installation d'Acronis Cyber Protect.
2. [Facultatif] Pour changer la langue du programme d'installation, cliquez sur **Configurer la langue**.
3. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
4. Sélectionnez **Installer un agent de protection**.
5. Effectuez l'une des actions suivantes :
   - Cliquez sur **Installer**.
     C'est le moyen le plus simple d'installer le produit. La plupart des paramètres d'installation seront définis sur leurs valeurs par défaut.
     Les composants suivants seront installés :

- Agent pour Windows
- Autres agents (l'agent pour Hyper-V, l'agent pour Exchange, l'agent pour SQL et l'agent pour Active Directory), si l'application ou l'hyperviseur respectif est détecté sur la machine
- Bootable Media Builder
- Outil de ligne de commande
- Cyber Protect Moniteur

- Cliquez sur **Personnaliser les paramètres d'installation** pour la configuration.

  Vous pourrez sélectionner les composants à installer et spécifier des paramètres supplémentaires. Pour plus d'informations, veuillez consulter l'article "Personnalisation des paramètres d'installation" (p. 87).
- Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance** pour extraire les packages d'installation. Vérifiez ou modifiez les paramètres d'installation qui seront ajoutés au fichier .mst, puis cliquez sur **Générer**. Les étapes suivantes de cette procédure ne sont pas nécessaires.

  Si vous souhaitez déployer des agents via la règle de groupe, continuez comme décrit dans "Déploiement des agents via la stratégie de groupe" (p. 182).

6. Indiquez le serveur de gestion sur lequel la machine avec l'agent sera enregistrée :
   a. Spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé.
   b. Spécifiez les informations d'identification d'un administrateur du serveur de gestion ou un jeton d'enregistrement.

      Pour en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Etape 1 : Génération d'un jeton d'enregistrement" (p. 183).
   c. Cliquez sur **Valider**.
7. Si vous y êtes invité, sélectionnez si la machine avec l'agent sera ajouté à l'organisation ou à l'une des unités.

   Cette invite apparaît sur vous administrez plus d'une unité, ou une organisation possédant au moins une unité. Sinon, la machine sera silencieusement ajoutée à l'unité que vous administrez ou à l'organisation. Pour obtenir plus d'informations, consultez l'article "Unités et comptes d'administration" (p. 665).
8. Effectuez l'installation.
9. Une fois l'installation terminée, cliquez sur **Fermer**.
10. Si vous avez installé aagent pour Exchange, vous pourrez sauvegarder des bases de données Exchange. Si vous souhaitez sauvegarder des boîtes aux lettres Exchange, ouvrez la console Web Cyber Protect, cliquez sur **Ajouter** > **Microsoft Exchange Server** > **Boîtes aux lettres Exchange**, puis spécifiez l'ordinateur sur lequel le rôle de serveur d'**Accès Client** (CAS) de Microsoft Exchange Server est activé. Pour obtenir plus d'informations, consultez l'article "Sauvegarde de boîte de réception" (p. 464).

Pour installer l'agent pour VMware (Windows), l'agent pour Office 365, l'agent pour Oracle ou l'agent pour Exchange sur une machine sans Microsoft Exchange Server

1. Connectez-vous comme administrateur et lancez le programme d'installation d'Acronis Cyber Protect.
2. [Facultatif] Pour changer la langue du programme d'installation, cliquez sur **Configurer la langue**.
3. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
4. Sélectionnez **Installer un agent de protection** puis cliquez sur **Personnaliser les paramètres d'installation**.
5. En regard de **Éléments à installer**, cliquez sur **Modifier**.
6. Sélectionnez la case à cocher correspondante à l'agent que vous voulez installer. Décochez les cases pour les composants que vous ne souhaitez pas installer. Cliquez sur **Terminé** pour continuer.
7. Indiquez le serveur de gestion sur lequel la machine avec l'agent sera enregistrée :
   a. En regard de **Serveur de gestion AcronisCyber Protect**, cliquez sur **Spécifier**.
   b. Spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé.
   c. Spécifiez les informations d'identification d'un administrateur du serveur de gestion ou un jeton d'enregistrement.
      Pour en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Etape 1 : Génération d'un jeton d'enregistrement" (p. 183).
   d. Cliquez sur **Valider**.
8. Si vous y êtes invité, sélectionnez si la machine avec l'agent sera ajouté à l'organisation ou à l'une des unités.
   Cette invite apparaît sur vous administrez plus d'une unité, ou une organisation possédant au moins une unité. Sinon, la machine sera silencieusement ajoutée à l'unité que vous administrez ou à l'organisation. Pour obtenir plus d'informations, consultez l'article "Unités et comptes d'administration" (p. 665).
9. [Facultatif] Modifiez d'autres paramètres d'installation comme décrit dans "Personnalisation des paramètres d'installation" (p. 87).
10. Cliquez sur **Installer** pour procéder à l'installation.
11. Une fois l'installation terminée, cliquez sur **Fermer**.
12. [Uniquement lors de l'installation de l'agent pour VMware (Windows)] Effectuez la procédure décrite dans "Configurer un agent pour VMware déjà enregistré" (p. 106).
13. [Uniquement lors de l'installation d'Agent pour Exchange] Ouvrez la console Web Cyber Protect, cliquez sur **Ajouter** > **Microsoft Exchange Server** > **Boîtes aux lettres Exchange**, puis spécifiez l'ordinateur sur lequel le rôle de serveur **d'Accès Client** (CAS) de Microsoft Exchange

Server est activé. Pour obtenir plus d'informations, consultez l'article "Sauvegarde de boîte de réception" (p. 464).

Installation sous Linux

Préparation

1. Assurez-vous que les packages Linux nécessaires sont installés sur la machine.
2. Lors de l'installation de l'agent dans SUSE Linux, vérifiez que vous utilisez `su` au lieu de `sudo`. Dans le cas contraire, l'erreur suivante se produit lorsque vous essayez d'inscrire l'agent par l'intermédiaire de la console Web Cyber Protect : `Échec de 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 le programme d'installation ne peut pas ouvrir le navigateur dans l'interface graphique.

Installation

Pour installer l'agent pour Linux, vous avez besoin d'au moins 2 Go d'espace disque libre.

Pour installer l'agent pour Linux

1. En tant qu'utilisateur root (superutilisateur), accédez au répertoire dans lequel est stocké le fichier d'installation (.i686 ou .x86_64), définissez-le comme fichier exécutable, puis exécutez-le.

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

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

2. Acceptez les termes du contrat de licence.
3. Précisez les composants à installer :
   a. Cochez la case **Serveur de gestion Acronis Cyber Protect**.
   b. Sélectionnez les cases à cocher correspondant aux agents que vous voulez installer. Les agents suivants sont disponibles :
      - **Agent pour Linux**
      - **Agent pour Oracle**

      L'agent pour Oracle nécessite que l'agent pour Linux soit également installé.
   c. Cliquez sur **Suivant**.
4. Indiquez le serveur de gestion sur lequel la machine avec l'agent sera enregistrée :
   a. Spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé.
   b. Indiquez le nom d'utilisateur et le mot de passe d'un administrateur du serveur de gestion.
   c. Cliquez sur **Suivant**.

5. Si vous y êtes invité, sélectionnez si la machine avec l'agent sera ajoutée à l'organisation ou à l'une des unités, puis appuyez sur **Entrée**.

   Cette invite apparaît si le compte spécifié dans l'étape précédente administre plus d'une unité ou une organisation possédant au moins une unité.
6. Si UEFI Secure Boot est activé sur la machine, vous êtes informé que vous devez redémarrer le système après l'installation. Veillez à vous rappeler le mot de passe (celui de l'utilisateur racine ou « acronis ») qui doit être utilisé.

   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.

7. 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 sous macOS

Pour installer l'agent pour Mac

1. Double-cliquez sur le fichier d'installation (.dmg).
2. Patientez pendant que le système d'exploitation monte l'image du disque d'installation.
3. Double-cliquez sur **Installer**, puis cliquez sur **Continuer**.
4. [Facultatif] Cliquez sur **Modifier l'emplacement de l'installation** pour modifier le disque sur lequel le logiciel sera installé. Par défaut, le disque au démarrage du système est sélectionné.
5. Cliquez sur **Installer**. Si vous y êtes invité, entrez le nom d'utilisateur et le mot de passe de l'administrateur.
6. Indiquez le serveur de gestion sur lequel la machine avec l'agent sera enregistrée :
   a. Spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé.
   b. Indiquez le nom d'utilisateur et le mot de passe d'un administrateur du serveur de gestion.
   c. Cliquez sur **Enregistrer**.
7. Si vous y êtes invité, sélectionnez si la machine avec l'agent sera ajoutée à l'organisation ou à l'une des unités, puis appuyez sur **Terminé**.

Cette invite apparaît si le compte spécifié dans l'étape précédente administre plus d'une unité ou une organisation possédant au moins une unité.

8. Une fois l'installation terminée, cliquez sur **Fermer**.

Installation ou désinstallation sans assistance

Installation ou désinstallation sans assistance sous Windows

Cette section décrit l'installation ou la désinstallation de Acronis Cyber Protect en mode sans assistance sur un ordinateur Windows via Windows Installer (le programme `msiexec`). Dans un domaine Active Directory, il est également possible d'exécuter une installation sans assistance en passant par la règle de groupe - voir "Déploiement des agents via la stratégie de groupe" (p. 182).

Pendant l'installation, vous pouvez utiliser un fichier appelé **Transformation** (un fichier .mst). Un fichier transformation est un fichier avec des paramètres d'installation. Comme alternative, vous pouvez spécifier les paramètres d'installation directement dans la ligne de commande.

Création du fichier de transformation .mst et extraction des packages d'installation

1. Connectez-vous comme administrateur, puis exécutez le programme d'installation.
2. Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
3. [Non disponible dans tous les programmes d'installation] Dans **Nombre de bits du composant**, sélectionnez **32 bits** ou **64 bits**.
4. Dans **Que faut-il installer**, sélectionnez les composants que vous souhaitez installer, puis cliquez sur **Terminé**.

   Les packages d'installation pour ces composants seront extraits du programme d'installation.
5. Dans **Serveur de gestionAcronis Cyber Protect**, 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 en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Etape 1 : Génération d'un jeton d'enregistrement" (p. 183).
6. [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 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, veuillez consulter cet article de la base de connaissances.

7. Vérifiez ou modifiez les autres paramètres d'installation qui seront ajoutés au fichier .mst, puis cliquez sur **Poursuivre**.
8. Sélectionnez le dossier dans lequel la transformation .mst sera générée, ainsi que les packages d'installation .msi et .cab qui seront extraits, puis cliquez sur **Générer**.

En conséquence, le fichier de transformation .mst est généré et les packages d'installation .msi et .cab sont extraits vers le dossier que vous avez spécifié.

Installation du produit en utilisant le fichier de transformation .mst

Dans la ligne de commande, exécutez la commande suivante :

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Où :

- Le `<nom package>` est le nom du fichier .msi. Ce nom est **AB.msi** ou **AB64.msi**, en fonction du nombre de bits du système d'exploitation.
- Le `<nom de transformation>` est le nom du fichier de la transformation. Ce nom est **AB.msi.mst** ou **AB64.msi.mst**, en fonction du nombre de bits du système d'exploitation.

Par exemple, `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

Installation ou désinstallation du produit en spécifiant les paramètres manuellement

Dans la ligne de commande, exécutez la commande suivante :

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Ici, le `<nom package>` est le nom du fichier .msi. Ce nom est **AB.msi** ou **AB64.msi**, en fonction du nombre de bits du système d'exploitation.

Les paramètres disponibles et leurs valeurs sont décrits dans "Paramètres communs" (p. 114).

Exemples

- Installation du serveur de gestion et des composants pour une installation à distance.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
  ```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et de Cyber Protect Monitor. Enregistrement de la machine avec l'agent sur un serveur de gestion précédemment installé.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

- Mise à jour du serveur de gestion, du nœud de stockage, du service de catalogue et de l'agent de protection.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
```

Paramètres d'installation ou de désinstallation sans assistance

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

En plus de ces paramètres, vous pouvez utiliser d'autres paramètres de `msiexec`, comme décrit dans https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Paramètres d'installation

Paramètres communs

`ADDLOCAL=<list of components>`

Les composants à installer, séparés par des virgules sans caractères d'espace. Toues les composants spécifiés doivent être extraits du programme d'installation avant l'installation.

La liste complète des composants est la suivante :

Composant	Doit être installé avec	Nombre de bits	Nom / description du composant
AcronisCentralizedManagementServer	WebConsole	32 bits/64 bits	Serveur de gestion
WebConsole	AcronisCentralizedManagementServer	32 bits/64 bits	Console Web
ComponentRegisterFeature	AcronisCentralizedManagementServer	32 bits/64 bits	Composants pour l'installation à distance

AtpScanService	AcronisCentralizedManagementServer	32 bits/64 bits	Service d'analyse
AgentsCoreComponents		32 bits/64 bits	Composants clés pour les agents
BackupAndRecoveryAgent	AgentsCoreComponents	32 bits/64 bits	Agent pour Windows
ArxAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour SQL
ARADAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32 bits/64 bits	Agent pour Office 365
AcronisESXSupport	AgentsCoreComponents	32 bits/64 bits	Agent pour VMware (Windows)
HyperVAgent	AgentsCoreComponents	32 bits/64 bits	Agent pour Hyper-V
ESXVirtualAppliance		32 bits/64 bits	Agent pour VMware (matériel virtuel)
ScaleVirtualAppliance		32 bits/64 bits	Agent pour HC3 de Scale Computi

			ng (matériel virtuel)
CommandLineTool		32 bits/64 bits	Outil de ligne de commande
TrayMonitor	BackupAndRecoveryAgent	32 bits/64 bits	Cyber Protect Moniteur
BackupAndRecoveryBootableComponents		32 bits/64 bits	Bootable Media Builder
ServeurPXE		32 bits/64 bits	Serveur PXE
StorageServer	BackupAndRecoveryAgent	64 bits	Nœud de stockage
CatalogBrowser	JRE 8 (mise à jour 111 ou ultérieure)	64 bits	Service de catalogue

`TARGETDIR=<path>`

Le dossier où le produit sera installé.

`REBOOT=ReallySuppress`

Si le paramètre est spécifié, il est interdit de redémarrer la machine.

`CURRENT_LANGUAGE=<language ID>`

La langue du produit. Les valeurs disponibles sont les suivantes : `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`ACEP_AGREEMENT={0,1}`

Si la valeur est `1`, l'ordinateur participera au programme d'amélioration du produit Acronis.

`REGISTRATION_ADDRESS=<host name or IP address>:<port>`

Le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé. Les agents, le nœud de stockage et le service de catalogue spécifiés dans le paramètre `ADDLOCAL` seront enregistrés sur le serveur de gestion. Le numéro de port est obligatoire s'il diffère de la valeur par défaut (9877).

Avec ce paramètre, vous devez spécifier soit le paramètre `REGISTRATION_TOKEN`, soit les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`.

`REGISTRATION_TOKEN=<token>`

Le jeton d'inscription généré dans la console Web Cyber Protect comme décrit dans Déploiement des agents via la règle de groupe.

`REGISTRATION_LOGIN=<user name>, REGISTRATION_PASSWORD=<password>`

Le nom d'utilisateur et le mot de passe d'un administrateur du serveur de gestion.

`REGISTRATION_TENANT=<unit ID>`

L'unité au sein de l'organisation. Les agents, le nœud de stockage et le service de catalogue spécifiés dans le paramètre `ADDLOCAL` seront ajoutés à cette unité.

Pour connaître l'identifiant d'une unité, dans la console Web Cyber Protect, cliquez sur **Paramètres** > **Comptes**, sélectionnez l'unité puis cliquez sur **Détails**.

Ce paramètre ne fonctionne pas sans `REGISTRATION_TOKEN`, ou sans `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`. Dans ce cas, les composants seront ajoutés à l'organisation.

Sans ce paramètre, les composants seront ajoutés à l'organisation.

`REGISTRATION_REQUIRED={0,1}`

Le résultat de l'installation dans le cas où l'enregistrement échoue. Si la valeur est `1`, l'installation échoue. Si la valeur est `0`, l'installation réussit même si le composant n'était pas enregistré.

`REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>`

Ces paramètres mutuellement exclusifs définissent la méthode de vérification du certificat du serveur de gestion pendant l'enregistrement. Vérifiez le certificat si vous souhaitez vérifier l'authenticité du serveur de gestion pour empêcher des attaques de l'intercepteur (MITM, man-in-the-middle).

Si la valeur est `1`, la vérification emploie respectivement l'autorité de certification système ou le lot d'autorité de certification fourni avec le produit. Si une clé publique avec code PIN est précisée, elle est également utilisée pour la vérification. Si la valeur est `0` ou si les paramètres ne sont pas spécifiés, le certificat n'est pas vérifié, mais le trafic d'inscription reste chiffré.

`/l*v <log file>`

Si le paramètre est spécifié, le journal d'installation en mode détaillé sera sauvegardé dans le fichier spécifié. Le fichier journal peut être utilisé pour analyser les problèmes d'installation.

Paramètres d'installation du serveur de gestion

`WEB_SERVER_PORT=<port number>`

Le port qui sera utilisé par un navigateur Web pour accéder au serveur de gestion. Par défaut, 9877.

`AMS_ZMQ_PORT=<port number>`

Le port pour la communication entre les composants des produits Par défaut, 7780.

`SQL_INSTANCE=<instance>`

La base de données peut être utilisée par le serveur de gestion. Vous pouvez sélectionner n'importe quelle édition de Microsoft SQL Server 2012, Microsoft SQL Server 2014 ou Microsoft SQL Server 2016. L'instance choisie peut également être utilisée par d'autres programmes.

Sans ce paramètre, la base de données SQLite intégrée sera utilisée.

`SQL_USER_NAME=<user name>` et `SQL_PASSWORD=<password>`

Informations d'identification d'un compte Microsoft SQL Server. Le serveur de gestion utilisera ces informations de connexion pour se connecter à l'instance SQL Server sélectionnée. Sans ces paramètres, le serveur de gestion utilisera les informations de connexion du compte du service de serveur de gestion (**Utilisateur AMS**).

Le compte sous lequel le service de serveur de gestion sera exécuté.

Spécifiez l'un des paramètres suivants :

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  Si la valeur est `1`, le compte système sera utilisé.
- `AMS_CREATE_NEW_ACCOUNT={0,1}`
  Si la valeur est `1`, un nouveau compte sera créé.
- `AMS_SERVICE_USERNAME=<user name>` et `AMS_SERVICE_PASSWORD=<password>`
  Le compte spécifié sera utilisé.

Paramètres d'installation de l'agent

`HTTP_PROXY_ADDRESS=<IP address>` et `HTTP_PROXY_PORT=<port>`

Le serveur proxy HTTP utilisé par l'agent. Sans ces paramètres, aucun serveur proxy ne sera utilisé.

`HTTP_PROXY_LOGIN=<login>` et `HTTP_PROXY_PASSWORD=<password>`

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Si la valeur est `0` ou si le paramètre n'est pas spécifié, l'agent utilisera le serveur proxy uniquement pour la sauvegarde et la reprise depuis le Cloud. Si la valeur est `1`, l'agent se connectera aussi au serveur de gestion via le serveur proxy.

`SET_ESX_SERVER={0,1}`

Si la valeur est `0`, l'agent pour VMware installé ne sera pas connecté à un vCenter Server ou un hôte ESXi. Après l'installation, Procédez tel que décrit dans « Configurer un agent pour VMware déjà enregistré ».

Si la valeur est `1`, spécifiez les paramètres suivants :

`ESX_HOST=<host name or IP address>`

Le nom d'hôte ou l'adresse IP du vCenter Server ou de l'hôte ESXi.

`ESX_USER=<user name>` et `ESX_PASSWORD=<password>`

Informations d'identification pour accéder au vCenter Server ou à l'hôte ESXi.

Le compte sous lequel le service de l'agent sera exécuté

Spécifiez l'un des paramètres suivants :

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  Si la valeur est `1`, le compte système sera utilisé.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  Si la valeur est `1`, un nouveau compte sera créé.
- `MMS_SERVICE_USERNAME=<user name>` et `MMS_SERVICE_PASSWORD=<password>`
  Le compte spécifié sera utilisé.

Paramètres d'installation d'un nœud de stockage

Le compte sous lequel le service de nœud de stockage sera exécuté

Spécifiez l'un des paramètres suivants :

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  Si la valeur est `1`, le compte système sera utilisé.
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  Si la valeur est `1`, un nouveau compte sera créé.
- `ASN_SERVICE_USERNAME=<user name>` et `ASN_SERVICE_PASSWORD=<password>`
  Le compte spécifié sera utilisé.

Paramètres d'installation d'un service de catalogue

`CATALOG_DATA_MIGRATION_PATH=<path>`

Utilisez ce paramètre pour migrer les données de catalogue vers la nouvelle version du service de catalogue dans Acronis Cyber Protect 15 Update 4. Spécifiez le chemin vers le dossier temporaire vers lequel les données de catalogue seront exportées.

`SKIP_CATALOG_DATA_MIGRATION=1`

Utilisez ce paramètre pour ignorer la migration de données de catalogue.

Les paramètres `SKIP_CATALOG_DATA_MIGRATION` et `CATALOG_DATA_MIGRATION_PATH` s'excluent mutuellement.

Paramètres de désinstallation

`REMOVE={<list of components>|ALL}`

Les composants sont supprimés, séparés par des virgules sans caractères d'espace.

Les composants disponibles sont décrits plus haut dans cette section.

Si la valeur est `ALL`, tous les composants du produit seront désinstallés. En complément, vous pouvez spécifier le paramètre suivant :

`DELETE_ALL_SETTINGS={0, 1}`

Si la valeur est `1`, les paramètres de configuration, de tâches et de journaux des produits seront supprimés.

Installation et désinstallation sans assistance sous Linux

Cette section décrit l'installation ou la désinstallation de Acronis Cyber Protect en mode sans assistance sur un ordinateur sous Linux via la ligne de commande.

Pour installer ou désinstaller le produit

1. Ouvrir l'application Terminal.
2. Exécuter la commande suivante :

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

   Ici, le `<nom package>` est le nom du package d'installation (un fichier .i686 ou .x86_64).
3. [Uniquement lors de l'installation de l'agent pour Linux] Si UEFI Secure Boot est activé sur la machine, vous êtes informé que vous devez redémarrer le système après l'installation. Veillez à vous rappeler le mot de passe (celui de l'utilisateur racine ou « acronis ») qui doit être utilisé. 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.

Si vous activez UEFI Secure Boot après l'installation de l'agent, répétez l'installation en incluant l'étape 3. Dans le cas contraire, les sauvegardes échoueront.

Paramètres d'installation

Paramètres communs

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

Les composants à installer, séparés par des virgules sans caractères d'espace.

Les composants suivants sont disponibles pour l'installation :

Composant	Description du composant
AcronisCentralizedManagementServer	Serveur de gestion
BackupAndRecoveryAgent	Agent pour Linux
BackupAndRecoveryBootableComponents	Bootable Media Builder

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

`--language=<language ID>`

La langue du produit. Les valeurs disponibles sont les suivantes : `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`{-d|--debug}`

Si le paramètre est spécifié, le journal d'installation est écrit en mode détaillé. Ce journal est situé dans le fichier **/var/log/trueimage-setup.log**.

`{-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}`

Si le paramètre est spécifié, l'absence des packages Linux requis sera ignorée pendant l'installation.

Paramètres d'installation du serveur de gestion

`{-W |--web-server-port=}<port number>`

Le port qui sera utilisé par un navigateur Web pour accéder au serveur de gestion. Par défaut, 9877.

`--ams-tcp-port=<port number>`

Le port pour la communication entre les composants des produits Par défaut, 7780.

Paramètres d'installation de l'agent

Spécifiez l'un des paramètres suivants :

- `--skip-registration`
  - N'enregistre pas l'agent sur le serveur de gestion.
- `{-C |--ams=}<host name or IP address>`
  - Le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé. L'agent sera enregistré sur ce serveur de gestion.

Si vous installez l'agent et le serveur de gestion au sein d'une seule commande, l'agent sera enregistré sur ce serveur de gestion, quel que soit le paramètre `-C`.

Avec ce paramètre, vous devez spécifier soit le paramètre `token`, soit les paramètres `login` et `password`.

`--token=<token>`

Le jeton d'inscription généré dans la console Web Cyber Protect comme décrit dans Déploiement des agents via la règle de groupe.

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

Informations d'identification d'un administrateur du serveur de gestion.

`--unit=<unit ID>`

L'unité au sein de l'organisation. L'agent sera ajouté à cette unité.

Pour connaître l'identifiant d'une unité, dans la console Web Cyber Protect, cliquez sur **Paramètres** > **Comptes**, sélectionnez l'unité puis cliquez sur **Détails**.

Sans ce paramètre, l'agent sera ajouté à l'organisation.

`--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

La méthode de vérification du certificat du serveur de gestion pendant l'enregistrement. Vérifiez le certificat si vous souhaitez vérifier l'authenticité du serveur de gestion pour empêcher des attaques de l'intercepteur (MITM, man-in-the-middle).

Si la valeur est `https` ou si le paramètre n'est pas spécifié, le certificat n'est pas vérifié, mais le trafic d'inscription reste chiffré. Si la valeur *n'est pas* `https`, la vérification emploie respectivement l'autorité de certification système, le lot d'autorité de certification fourni avec le produit ou la clé publique avec code PIN.

`--reg-transport-pinned-public-key=<public key value>`

La valeur de la clé publique avec code PIN. Ce paramètre doit être spécifié en complément ou à la place du paramètre `--reg-transport=https-pinned-public-key`.

- `--http-proxy-host=<IP address>` et `--http-proxy-port=<port>`
  - Le serveur proxy HTTP que l'agent utilisera pour la sauvegarde et la reprise 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. Utilisez ces paramètres si le serveur exige une authentification.
- `--no-proxy-to-ams`
  - L'agent de protection se connecte au serveur de gestion sans utiliser le serveur proxy spécifié par les paramètres `--http-proxy-host` et `--http-proxy-port`.

Paramètres de désinstallation

`{-u|--uninstall}`

Désinstalle le produit.

`--purge`

Supprime les paramètres de configuration, de tâches et de journaux des produits.

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.

Exemples

- Installation du serveur de gestion.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Installation du serveur de gestion, spécification de ports personnalisés

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- Installation et enregistrement de l'agent pour Linux sur le serveur de gestion spécifié.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- Installation et enregistrement de l'agent pour Linux sur le serveur de gestion spécifié, dans l'unité spécifiée.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

Installation ou désinstallation sans assistance sous macOS

Cette section décrit l'installation, l'enregistrement et la désinstallation de l'agent de protection en mode sans assistance sur un ordinateur sous macOS via la ligne de commande. Pour en savoir plus sur le téléchargement du fichier d'installation (.dmg), reportez-vous à « Ajout d'une machine exécutant macOS ».

Pour installer l'agent pour Mac

1. Créez un répertoire temporaire dans lequel vous monterez le fichier d'installation (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Remplacez `<racine_dmg>` par le nom de votre choix.
2. Montez le fichier .dmg.

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

Remplacez <fichier_dmg> par le nom du fichier d'installation. Par exemple, **AcronisCyberProtect_15_MAC.dmg**.

3. Exécutez le programme d'installation.

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

4. Détachez le fichier d'installation (.dmg).

```
hdiutil detach <dmg_root>
```

Exemples

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
  ```

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

  ```
  hdiutil detach mydirectory
  ```

Pour enregistrer l'agent pour Mac

Effectuez l'une des actions suivantes :

- Enregistrez l'agent sous un compte administrateur spécifique.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  <management server address:port> -u <user name> -p <password>
  ```

  La valeur <adresse du serveur de gestion:port> correspond au nom d'hôte ou à l'adresse IP de l'ordinateur sur lequel le serveur de gestion Acronis Cyber Protect est installé. Le numéro de port est obligatoire s'il diffère de celui par défaut (9877).

  <nom d'utilisateur> et <mot de passe> correspondent aux identifiants du compte administrateur sous lequel l'agent sera enregistré.
- Enregistrez l'agent dans une unité spécifique.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
  <management server address:port> -u <user name> -p <password> --tenant <unit ID>
  ```

  Pour connaître l'identifiant d'une unité, dans la console Web Cyber Protect, cliquez sur **Paramètres** > **Comptes**, sélectionnez l'unité de votre choix, puis cliquez sur **Détails**.
  ```

Important
Les administrateurs peuvent enregistrer des agents en spécifiant l'identifiant de l'unité uniquement à leur niveau dans la hiérarchie de l'organisation. Les administrateurs d'unité peuvent enregistrer des machines avec leurs propres unités et leurs sous-unités. Les administrateurs de l'organisation peuvent enregistrer des machines dans toutes les unités. Pour plus d'informations sur les différents comptes administrateur, reportez-vous à l'article « Administration des comptes d'utilisateur et des unités de l'organisation ».

- Vous pouvez également enregistrer l'agent à l'aide d'un jeton d'enregistrement.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Vous pouvez en générer un dans la console Web Cyber Protect, comme décrit dans Déploiement des agents via la règle de groupe.

Important
Sous macOS 10.14 ou une version ultérieure, vous devez accorder l'accès complet au disque à l'agent de protection. Pour cela, accédez à **Applications** >**Utilitaires**, puis exécutez **Cyber Protect Agent Assistant**. Suivez ensuite les instructions contenues dans la fenêtre de l'application.

Exemples

Enregistrement à l'aide d'un nom d'utilisateur et d'un mot de passe.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

Enregistrement avec un identifiant d'unité et des informations d'identification d'un administrateur.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
86d8-005056bdd3a0
```

Enregistrement avec un jeton.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 --token D91D-DC46-4F0B
```

Pour désinstaller l'agent pour Mac

Exécuter la commande suivante :

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

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

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

Enregistrement manuel de machines

En plus d'enregistrer un ordinateur dans le serveur de gestion Cyber Protect lors de l'installation de l'agent, vous pouvez également l'enregistrer à l'aide de l'interface de ligne de commande. Il se peut que vous deviez procéder ainsi si vous avez installé l'agent, mais que l'enregistrement automatique a échoué par exemple, ou si vous souhaitez enregistrer une machine existante sous un nouveau compte.

Pour enregistrer une machine

À l'invite de commande de l'ordinateur sur lequel l'agent est installé, exécutez l'une des commandes suivantes :

- Pour enregistrer la machine sous un compte administrateur spécifique :

  ```
  <path to the registration tool> -o register –a <management server address:port> -u
  <user name> -p <password>
  ```

  Le `<chemin d'accès à l'outil d'enregistrement>` est :

  - Sous Windows : `%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
  - Sous Linux : `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
  - sous macOS : `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

  La valeur `<adresse du serveur de gestion:port>` correspond au nom d'hôte ou à l'adresse IP de l'ordinateur sur lequel le serveur de gestion Acronis Cyber Protect est installé. Si vous utilisez le port par défaut (9877), il n'est pas nécessaire de l'indiquer.

  `<nom d'utilisateur>` et `<mot de passe>` correspondent aux identifiants du compte administrateur sous lequel l'agent sera enregistré.
- Pour enregistrer l'agent dans une unité spécifique, spécifiez l'identifiant de l'unité :

  ```
  <path to the registration tool> -o register –a <management server address:port> u
  <user name> -p <password> --tenant <unit ID>
  ```

  Pour connaître l'identifiant d'une unité, dans la console Web Cyber Protect, cliquez sur **Paramètres** > **Comptes**, sélectionnez l'unité de votre choix, puis cliquez sur **Détails**.

Important
Les administrateurs peuvent uniquement enregistrer des agents à leur niveau de la hiérarchie dans l'organisation. Les administrateurs d'unité peuvent enregistrer des agents avec leurs propres unités et leurs sous-unités. Les administrateurs de l'organisation peuvent enregistrer des agents dans toutes les unités. Pour plus d'informations sur les différents comptes administrateur, reportez-vous à l'article « Administration des comptes d'utilisateur et des unités de l'organisation ».

- Pour enregistrer une machine à l'aide d'un jeton d'enregistrement :

```
<path to the registration tool> -o register -a <management server address:port> --
token <token>
```

  - Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Pour en savoir plus sur comment en générer un, reportez-vous à « Déploiement des agents via la stratégie de groupe ».

Pour désenregistrer une machine

À l'invite de commandes de l'ordinateur sur lequel l'agent est installé, exécutez cette commande :

```
<path to the registration tool> -o unregister
```

Exemples

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

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

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

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

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

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

Mots de passe contenant 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 :

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

Exemple (pour Windows) :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

Si vous recevez toujours une erreur :

1. Encodez votre mot de passe au format base64 sur https://www.base64encode.org/.
2. Dans la ligne de commande, indiquez le mot de passe encodé à l'aide du paramètre -b ou --base64.

Exemple (pour Windows) :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Vérification des mises à jour de logiciel

Cette fonctionnalité n'est disponible que pour un administrateur de l'organisation.

Chaque fois que vous vous connectez à la console Web Cyber Protect, Acronis Cyber Protect vérifie si une nouvelle version du logiciel est disponible sur le site Web de Acronis. Si c'est le cas, la console Web Cyber Protect affiche un lien de téléchargement de la nouvelle version en bas de chaque page sous les onglets **Terminaux**, **Plans** et **Stockage de sauvegarde**. Le lien est également disponible sur la page **Paramètres** > **Agents**.

Pour activer ou désactiver les vérifications automatiques des mises à jour, modifiez le paramètre système **Mises à jour**.

Pour vérifier les mises à jour manuellement, cliquez sur l'icône en forme de point d'interrogation en haut à droite > **À propos de** > **Vérifier les mises à jour** ou l'icône en forme de point d'interrogation > **Vérifier les mises à jour**.

Migration du serveur de gestion

Vous pouvez migrer un serveur de gestion s'exécutant sur un ordinateur Windows vers un autre ordinateur Windows du même environnement.

Le processus de migration se compose des phases suivantes :

1. "Opérations sur la machine source" (p. 130)
   Dans cette phase, vous préparez les données du serveur de gestion d'origine pour la migration.
2. "Opérations sur la machine cible" (p. 131)
   Dans cette phase, vous installez et configurez un nouveau serveur de gestion, puis copiez les données du serveur de gestion d'origine vers le nouveau.

Prérequis

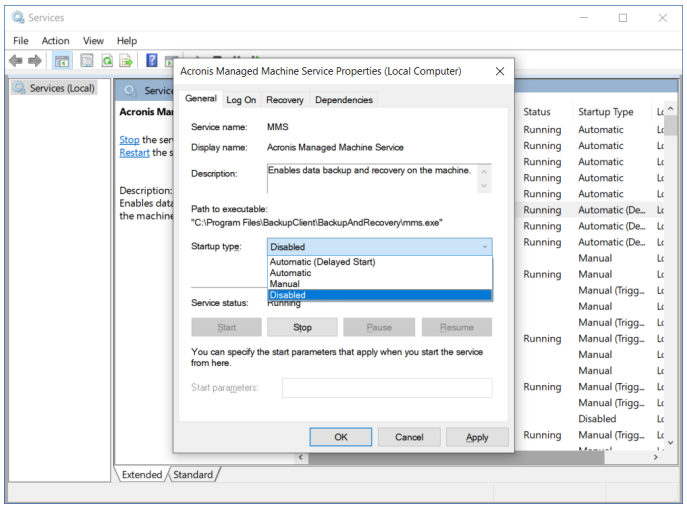
- Le serveur de gestion utilise une base de données Microsoft SQL Server externe. L'instance Microsoft SQL Server s'exécute sur un ordinateur dédié.
- Les agents de protection sont enregistrés sur le serveur de gestion à l'aide de son nom d'hôte, pas de son adresse IP.
- La version du serveur de gestion est Acronis Cyber Protect Update 4 (build 29486) ou une version ultérieure.
- La même version du serveur de gestion est installée sur les machines source et cible.

Opérations sur la machine source

Dans cette phase, vous préparez les données du serveur de gestion d'origine pour la migration.

Pour préparer les données pour la migration

1. Sur l'ordinateur du serveur de gestion d'origine, arrêtez tous les services Acronis.
   a. Ouvrez **Services**, puis désactivez le démarrage des services Acronis, à l'exception des services **Acronis Active Protection** et **Acronis Cyber Protect**.



   b. Ouvrez **Regedit**, puis désactivez les services **Acronis Active Protection** et **Acronis Cyber Protect** en modifiant leurs clés :
      - Dans la clé `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService`, ouvrez la valeur **Start**, puis définissez les données de valeur sur 4.
      - Dans la clé `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService`, ouvrez la valeur **Start**, puis définissez les données de valeur sur 4.
2. Redémarrez l'ordinateur du serveur de gestion, puis indiquez que les services Acronis désactivés ne s'exécutent pas.

Remarque
Deux services, **Acronis Scheduler Service Helper** et **Acronis TIB Mounter Monitor**, sont peut-être toujours en cours d'exécution. Vous pouvez les ignorer sans aucun risque.

3. [Si le composant Cyber Protect Monitor est installé sur la machine du serveur de gestion] Quittez Acronis Cyber Protect Monitor.
4. À l'invite de commandes Windows, modifiez le propriétaire des dossiers `%ProgramData%\Acronis` et `%ProgramFiles%\Acronis` en exécutant les commandes suivantes :

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. Modifiez les autorisations d'accès à ces dossiers et à leurs sous-dossiers en exécutant les commandes suivantes :

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. Copiez les dossiers `%ProgramData%\Acronis` et `%ProgramFiles%\Acronis` dans un partage réseau accessible par le nouvel ordinateur du serveur de gestion.
7. Arrêtez l'ordinateur du serveur de gestion d'origine.

Suivez ensuite la procédure de "Opérations sur la machine cible" (p. 131).

Opérations sur la machine cible

Dans cette phase, vous installez et configurez un nouveau serveur de gestion, puis y migrez les données.

Avant d'effectuer les opérations sur la machine cible, veillez à suivre la procédure indiquée dans "Opérations sur la machine source" (p. 130).

Pour migrer les données vers le nouveau serveur de gestion

1. Définissez le nom d'hôte de l'ordinateur sur lequel vous allez installer le nouveau serveur de gestion. Ce nom doit être identique à celui de l'ordinateur avec le serveur de gestion d'origine.
2. Créez une règle de pare-feu pour bloquer tout le trafic sur le port TCP 9877.
3. Exécutez le programme d'installation d'Acronis Cyber Protect.
   a. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
   b. Cliquez sur **Personnaliser les paramètres d'installation**.
   c. Dans **Que faut-il installer**, sélectionnez uniquement les composants suivants, puis cliquez sur **Terminé**.

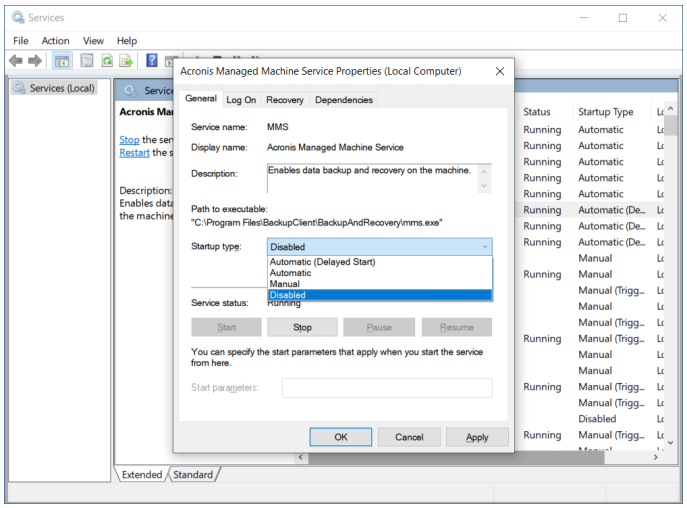
- Serveur de gestion
- Composants pour l'installation à distance
- Bootable Media Builder
- Outil de ligne de commande

d. Dans **Base de données pour le serveur de gestion**, conservez l'option par défaut **Utiliser une base de données intégrée (SQLite)**.

e. Dans **Compte de connexion pour le service de serveur de gestion**, utilisez la même option que sur le serveur de gestion d'origine.

4. Arrêtez tous les services Acronis.

a. Ouvrez **Services**, puis désactivez le démarrage de tous les services Acronis.

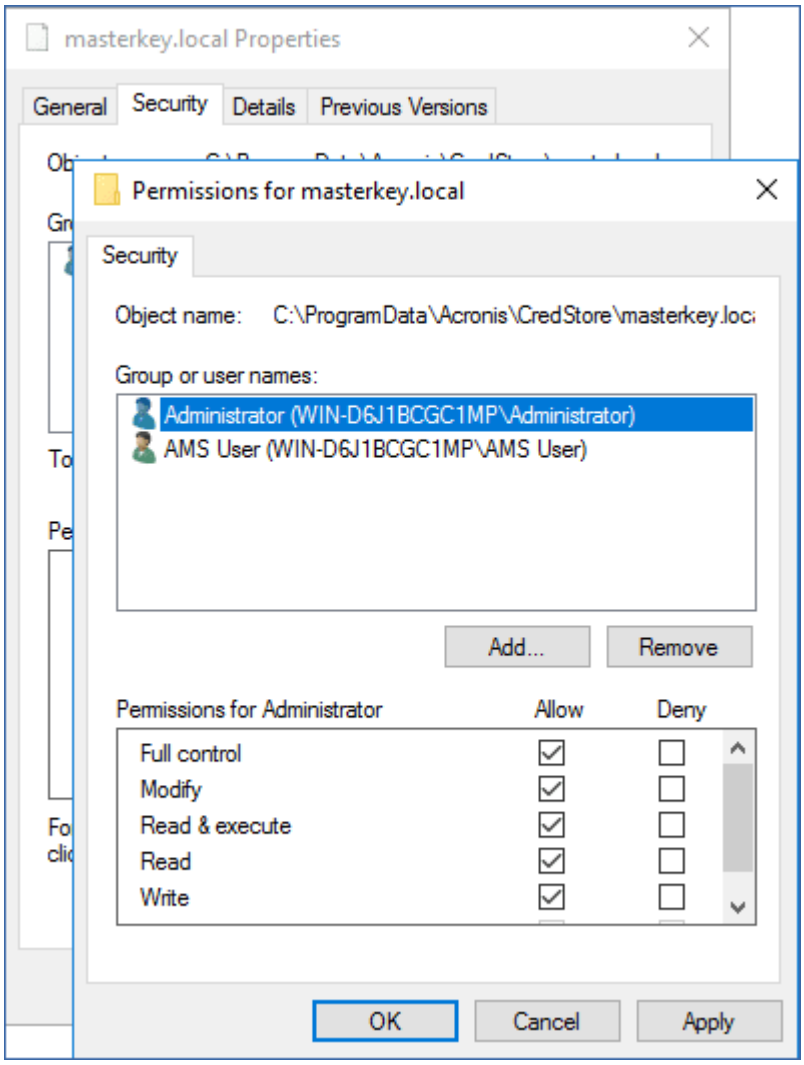


b. Redémarrez l'ordinateur, puis vérifiez que les services Acronis désactivés ne s'exécutent pas.

5. Accédez à `%ProgramData%\Acronis\CredStore`, puis modifiez les autorisations du fichier `masterkey.local` comme suit :

a. Accordez la propriété du fichier au compte utilisateur **Administrateur**.

b. Accordez au compte utilisateur **Administrateur** les autorisations **Contrôle total**.



6. Accédez à `%ProgramData%\Acronis\AMS\AccessVault\config`, puis accordez au compte utilisateur **Administrateur** les autorisations **Contrôle total** pour les fichiers suivants :
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. Remplacez les dossiers suivants par les dossiers que vous avez copiés depuis l'ordinateur du serveur de gestion d'origine vers un partage réseau :
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   Important
   Écrasez les dossiers existants sans les supprimer au préalable.

   Remarque
   Si un message s'affiche pour indiquer que le dossier `%ProgramFiles%\Acronis\ShellExtentions` ne peut pas être remplacé, vous pouvez ignorer ce dossier sans problème.
8. Restaurez les autorisations pour les fichiers suivants :

- `%ProgramData%\Acronis\CredStore\masterkey.local` – Supprimez le compte utilisateur **Administrateur** de la liste des utilisateurs avec autorisations.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` – Accordez au compte utilisateur **Administrateur** uniquement l'autorisation **Lecture**.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` – Accordez au compte utilisateur **Administrateur** uniquement l'autorisation **Lecture**.

9. Créez une jonction de répertoires pour le dossier `NGMP\latest`.
   - À l'invite de commandes Windows, accédez à `%ProgramData%\Acronis`, puis supprimez le `dernier` dossier.

     ```
     cd %ProgramData%\Acronis\NGMP
     ```

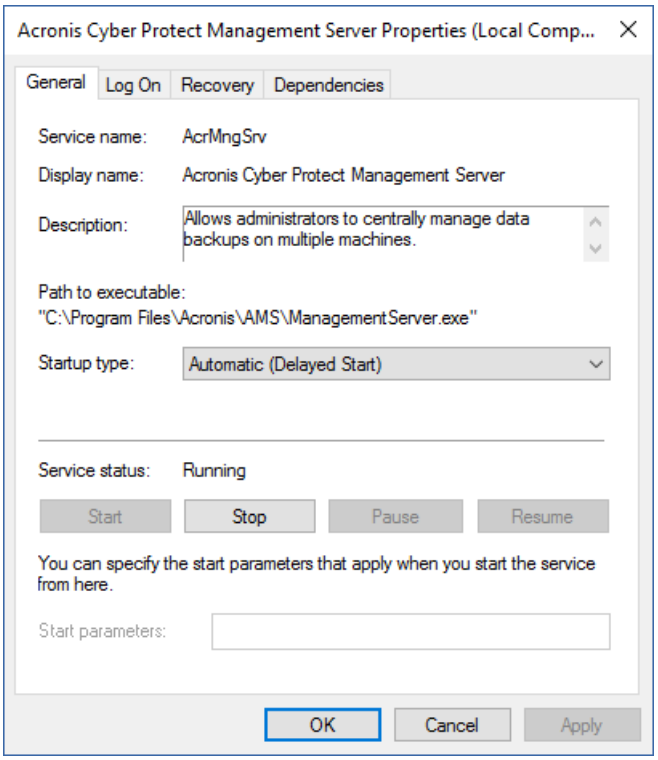
     ```
     rmdir latest
     ```

   - Créez la jonction de répertoire `latest`, puis pointez vers le dossier portant le nom de la version NGMP en cours, par exemple :

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. Faites pointer le nouveau serveur de gestion vers la base de données Microsoft SQL Server utilisée par le serveur de gestion d'origine.
    a. Ouvrez **Regedit**.
    b. Dans la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings`, modifiez la valeur `AmsDmlDbProtocol` en changeant ses données comme suit : `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config`.
11. Ouvrez **Services**, puis activez tous les services Acronis désactivés.

    Configurez le type de démarrage du **serveur de gestion Acronis Cyber Protect** sur **Automatique (démarrage retardé)** et celui de tous les autres services Acronis sur **Automatique**.



12. Dans le pare-feu, autorisez tout le trafic sur le port TCP 9877.
13. Redémarrez l'ordinateur, puis vérifiez que les services Acronis s'exécutent.
14. Exécutez le programme d'installation d'Acronis Cyber Protect et installez les éléments suivants :
    - Agent pour Windows
    - [Facultatif] Cyber Protect Moniteur
15. Redémarrez la machine.

Déploiement Cloud

Activation du compte

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

- **Un lien d'activation du compte.** Cliquez sur le lien et configurez le mot de passe du compte. Conservez votre identifiant, présent sur la page d'activation du compte.
- **Un lien vers la page de connexion donnant accès à la console Web Cyber Protect.** À l'avenir, utilisez ce lien pour accéder à la console. L'identifiant et le mot de passe sont les mêmes que pour l'étape précédente.

Préparation

Etape 1

Choisissez l'agent en fonction de ce que vous allez sauvegarder. Pour obtenir des informations au sujet des agents, reportez-vous à la section "Composants" (p. 48).

Etape 2

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

La page **Ajouter des périphériques** 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 périphériques**. 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 des agents via la stratégie de groupe" (p. 182).

Pour télécharger le programme d'installation de l'agent pour Office 365, cliquez sur l'icône de compte dans l'angle supérieur droit, puis cliquez sur **Téléchargements** > **Agent pour Office 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 de cyber protection. Sans connexion Internet, l'installation ne pourra être effectuée.

Etape 3

Avant de procéder à l'installation, assurez-vous que les pare-feu et les autres composants du système de sécurité de votre réseau (comme un serveur proxy) autorisent les connexions entrantes et sortantes via les ports TCP suivants :

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

  Ces ports sont utilisés pour accéder à la console Web Cyber Protect, pour l'enregistrement des agents, pour le téléchargement des certificats, pour les autorisations utilisateur et pour le téléchargement de fichiers depuis le stockage dans le Cloud.
- Ports entre **7770** et **7800**

  Ces ports permettent aux agents de communiquer avec le serveur de gestion.
- Ports **44445** et **55556**

Ces ports permettent aux agents de transférer des données lors du processus de sauvegarde et de restauration.

Si un serveur proxy est activé dans votre réseau, consultez la section "Paramètres de serveur proxy" (p. 138) afin de vérifier si vous avez besoin de configurer ces paramètres sur chaque ordinateur exécutant 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 **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). 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.

Etape 4

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.

- 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.

Le service Active Protection écoute sur le port TCP **6109**. Vérifiez qu'il n'est pas utilisé par un autre processus.

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`

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, les paramètres du serveur proxy doivent être fournis lors de l'installation ou à l'avance.

Sous Windows

Si un serveur proxy est configuré dans Windows (**Panneau de configuration** > **Options Internet** > **Connexions**), le programme d'installation consulte les paramètres de serveur proxy dans le registre et les utilise automatiquement. Vous pouvez également saisir les paramètres de proxy lors de l'installation, ou les préciser à l'avance en utilisant la procédure décrite ci-dessous. Pour modifier les paramètres de proxy après l'installation, utilisez la même procédure.

Pour préciser les paramètres de proxy sous Windows

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 de protection n'est pas encore installé, vous pouvez l'installer maintenant. Dans le cas contraire, procédez comme suit pour redémarrer l'agent :
   a. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis entrez : **cmd**.
   b. Cliquez sur **OK**.
   c. Exécutez les commandes suivantes :

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

Sous Linux

Exécutez le fichier d'installation avec les paramètres `--http-proxy-host=ADRESSE --http-proxy-port=PORT --http-proxy-login=IDENTIFIANT--http-proxy-password=MOT DE PASSE`. Pour modifier les paramètres de proxy après l'installation, utilisez la procédure décrite ci-dessous.

Pour modifier les paramètres de proxy sous Linux

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, recherchez 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>
```

   - Autrement, copiez les lignes ci-dessus et collez-les dans le fichier entre les balises `<registry name="Global">...</registry>`.

3. Remplacez `ADRESSE` 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 `IDENTIFIANT` et `MOT DE PASSE` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
5. Enregistrez le fichier.
6. Redémarrez l'agent en exécutant la commande suivante dans n'importe quel répertoire :

```
sudo service acronis_mms restart
```

Dans macOS

Vous pouvez saisir les paramètres de proxy lors de l'installation, ou les préciser à l'avance en suivant la procédure décrite ci-dessous. Pour modifier les paramètres de proxy après l'installation, utilisez la même procédure.

Pour préciser les paramètres de proxy sous macOS

1. Créez le fichier **/Library/Application Support/Acronis/Registry/Global.config** et ouvrez-le dans un éditeur de texte comme Text Edit.
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 de protection n'est pas encore installé, vous pouvez l'installer maintenant. Dans le cas contraire, procédez comme suit pour redémarrer l'agent :
   a. Rendez-vous dans **Applications** > **Utilitaires** > **Terminal**
   b. Exécutez les commandes suivantes :

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

Sur le 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 définir les paramètres du serveur proxy, cliquez sur **Outils** > **Serveur proxy**, puis spécifiez l'adresse IP/nom de l'hôte, le port et les informations d'identification du serveur proxy.

Installation des agents

Sous Windows

1. Assurez-vous que la machine est connectée à Internet.
2. Connectez-vous comme administrateur, puis exécutez le programme d'installation.
3. [Facultatif] Cliquez sur **Personnaliser les paramètres d'installation** et procédez aux changements désirés :
   - Pour modifier les composants à installer (en particulier, pour désactiver l'installation de Cyber Protect Monitor et de l'outil de ligne de commande).
   - Pour modifier la méthode d'enregistrement de la machine au sein du service de cyber protection. Vous pouvez passer de l'option **Utiliser la console Cyber Protect** (par défaut) à **Utiliser les identifiants** ou **Utiliser un jeton d'inscription**.
   - Pour modifier le chemin d'installation.
   - Pour modifier le compte du service de l'agent.
   - Pour vérifier ou modifier le nom d'hôte/l'adresse IP, le port et les informations d'identification du serveur proxy. Si un serveur proxy est activé dans Windows, il est détecté et utilisé automatiquement.
4. Cliquez sur **Installer**.
5. [Lors de l'installation de l'agent pour VMware uniquement] Indiquez l'adresse et les informations d'identification du vCenter Server ou de l'hôte ESXi autonome dont les machines virtuelles seront sauvegardées par l'agent, puis cliquez sur **Terminé**. Nous vous conseillons d'utiliser un compte auquel le rôle **Administrateur** a été attribué. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server ou ESXi.
6. [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, veuillez consulter cet article de la base de connaissances.

7. Si vous avez conservé la méthode d'inscription par défaut **Utiliser la console Cyber Protect** à l'étape 3, attendez que l'écran d'enregistrement apparaisse, puis passez à l'étape suivante. Sinon, aucune autre action n'est requise.
8. Effectuez l'une des actions suivantes :
   - Cliquez sur **Enregistrer la machine**. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Web Cyber Protect, consultez les informations d'inscription, puis cliquez sur **Confirmer l'enregistrement**.
   - Cliquez sur **Afficher les informations d'enregistrement**. Le programme d'installation affiche le lien et le code d'enregistrement. Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Dans ce cas, vous devrez saisir le code d'enregistrement dans le formulaire d'enregistrement. Le code d'enregistrement n'est valable qu'une heure.
     Sinon, vous pouvez accéder au formulaire d'enregistrement en cliquant sur **Tous les périphériques** > **Ajouter**, en cherchant **Enregistrement par code**, puis en cliquant sur **Enregistrement**.
9. **Remarque**
   Ne quittez pas le programme d'installation avant d'avoir confirmé l'enregistrement. Pour lancer de nouveau l'enregistrement, vous devrez redémarrer le programme d'installation et cliquer sur **Enregistrer la machine**.

   En conséquence, l'ordinateur sera assigné au compte utilisé pour établir la connexion à la console Web Cyber Protect.

Sous Linux

1. Assurez-vous que la machine est connectée à Internet.
2. En tant qu'utilisateur racine, exécutez le fichier d'installation.
   Si un serveur proxy est activé sur votre réseau, lorsque vous exécutez le fichier, spécifiez le nom d'hôte/adresse IP et le port du serveur au format : `--http-proxy-host=ADRESSE --http-proxy-port=PORT --http-proxy-login=CONNEXION--http-proxy-password=MOT DE PASSE`.
   Si vous souhaitez modifier la méthode par défaut d'enregistrement de la machine dans le service de 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'inscription
- `--skip-registration` : pour ignorer l'inscription

3. Sélectionnez les cases à cocher correspondant aux agents que vous voulez installer. Les agents suivants sont disponibles :
   - **Agent pour Linux**
   - **Agent pour Virtuozzo**

   L'agent pour Virtuozzo ne peut pas être installé sans l'agent pour Linux.
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 de cyber protection, ou attendez que la machine soit enregistrée à l'aide du jeton.
5. Effectuez l'une des actions suivantes :
   - Cliquez sur **Enregistrer la machine**. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Web Cyber Protect, consultez les informations d'inscription, puis cliquez sur **Confirmer l'enregistrement**.
   - Cliquez sur **Afficher les informations d'enregistrement**. Le programme d'installation affiche le lien et le code d'enregistrement. Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Dans ce cas, vous devrez saisir le code d'enregistrement dans le formulaire d'enregistrement. Le code d'enregistrement n'est valable qu'une heure.

     Sinon, vous pouvez accéder au formulaire d'enregistrement en cliquant sur **Tous les périphériques** > **Ajouter**, en cherchant **Enregistrement par code**, puis en cliquant sur **Enregistrement**.
6. **Remarque**
   Ne quittez pas le programme d'installation avant d'avoir confirmé l'enregistrement. Pour lancer de nouveau l'enregistrement, vous devrez redémarrer le programme d'installation et répéter la procédure d'installation.

   En conséquence, l'ordinateur sera assigné au compte utilisé pour établir la connexion à la console Web Cyber Protect.
7. Si UEFI Secure Boot est activé sur la machine, vous êtes informé que vous devez redémarrer le système après l'installation. Veillez à vous rappeler le mot de passe (celui de l'utilisateur racine ou « acronis ») qui doit être utilisé.

Remarque
Lors de l'installation, une nouvelle clé est générée, utilisée pour signer le module `snapapi` et enregistrée en tant que clé MOK (Machine Owner Key). Le redémarrage est obligatoire pour inscrire cette clé. Sans l'inscription de cette clé, l'agent ne sera pas opérationnel. Si vous activez UEFI Secure Boot après l'installation de l'agent, répétez l'installation en incluant l'étape 6.

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

Dans macOS

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**.
5. Si un serveur proxy est activé dans votre réseau, cliquez sur **Agent de protection** dans la barre de menus, puis sur **Paramètres de serveur proxy**. Spécifiez ensuite l'adresse IP/nom de l'hôte, le port et les identifiants 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. Effectuez l'une des actions suivantes :
   - Cliquez sur **Enregistrer la machine**. Dans la fenêtre de navigateur qui s'affiche, connectez-vous à la console Web Cyber Protect, consultez les informations d'inscription, puis cliquez sur **Confirmer l'enregistrement**.
   - Cliquez sur **Afficher les informations d'enregistrement**. Le programme d'installation affiche le lien et le code d'enregistrement. Vous pouvez les copier et effectuer les étapes d'enregistrement sur une autre machine. Dans ce cas, vous devrez saisir le code d'enregistrement dans le formulaire d'enregistrement. Le code d'enregistrement n'est valable qu'une heure.

     Sinon, vous pouvez accéder au formulaire d'enregistrement en cliquant sur **Tous les périphériques** > **Ajouter**, en cherchant **Enregistrement par code**, puis en cliquant sur **Enregistrement**.

10. **Astuce** Ne quittez pas le programme d'installation avant d'avoir confirmé l'inscription. Pour lancer de nouveau l'enregistrement, vous devrez redémarrer le programme d'installation et répéter la procédure d'installation.

En conséquence, l'ordinateur sera assigné au compte utilisé pour établir la connexion à la console Web Cyber Protect.

Changer le compte de connexion sur les machines Windows

À l'écran **Sélectionner les composants**, définissez le compte sous lequel les services seront exécutés en remplissant le champ **Compte d'ouverture de session 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.

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

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.

Privilèges requis pour le compte de connexion

Un agent de protection est exécuté en tant que service de la machine gérée (MMS) sur une machine Windows. Le compte sous lequel l'agent s'exécutera doit avoir des droits spécifiques pour que l'agent fonctionne correctement. Ainsi, l'utilisateur du MMS doit se voir attribuer les privilèges suivants :

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. Dispose de la permission **Contrôle complet** sur le dossier `%PROGRAMDATA%\Acronis` (sous Windows XP et Server 2003, `%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. Ouvrez **Outils administratifs** depuis le **Panneau de configuration** (ou cliquez sur Win+R, saisissez **control admintools**, et appuyez sur Entrée), puis ouvrez **Stratégie de sécurité locale**.
3. Développez **Stratégies locales** et cliquez sur **Attribution des droits d'utilisateur.**
4. Dans le panneau de droite, cliquez avec le bouton droit sur **Connexion en tant que service**, puis sélectionnez **Propriétés**.
5. Cliquez sur le bouton **Ajouter un utilisateur ou un groupe...** pour ajouter un nouvel utilisateur.
6. Dans la fenêtre **Sélectionner des utilisateurs, ordinateurs, comptes de service ou groupes**, trouvez l'utilisateur que vous souhaitez saisir et cliquez sur **OK**.
7. Cliquez sur **OK** dans **les propriétés de Connexion en tant que service** afin d'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**.

Notez qu'il n'est pas recommandé de modifier manuellement les comptes de connexion une fois l'installation terminée.

Installation ou désinstallation sans assistance

Installation ou désinstallation sans assistance sous Windows

Cette section décrit l'installation ou la désinstallation d'agents de protection sans assistance sur une machine sous Windows via Windows Installer (le programme `msiexec`). Dans un domaine Active

Directory, il est également possible d'exécuter une installation sans assistance en passant par la règle de groupe - voir "Déploiement des agents via la stratégie de groupe" (p. 182).

Pendant l'installation, vous pouvez utiliser un fichier appelé **Transformation** (un fichier .mst). Un fichier transformation est un fichier avec des paramètres d'installation. Comme alternative, vous pouvez spécifier les paramètres d'installation directement dans la ligne de commande.

Création du fichier de transformation .mst et extraction des packages d'installation

1. Connectez-vous comme administrateur, puis exécutez le programme d'installation.
2. Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
3. Dans **Que faut-il installer**, sélectionnez les composants que vous souhaitez installer, puis cliquez sur **Terminé**.
   Les packages d'installation pour ces composants seront extraits du programme d'installation.
4. Dans **Paramètres d'enregistrement**, sélectionnez **Utiliser les informations d'identification** ou **Utiliser un jeton d'enregistrement**. Pour en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Etape 1 : Génération d'un jeton d'enregistrement" (p. 183).
5. [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 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, veuillez consulter cet article de la base de connaissances.
6. Vérifiez ou modifiez les autres paramètres d'installation qui seront ajoutés au fichier .mst, puis cliquez sur **Poursuivre**.
7. Sélectionnez le dossier dans lequel la transformation .mst sera générée, ainsi que les packages d'installation .msi et .cab qui seront extraits, puis cliquez sur **Générer**.

Installation du produit en utilisant le fichier de transformation .mst

Dans la ligne de commande, exécutez la commande suivante.

Modèle de commande :

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Où :

- Le <nom package> est le nom du fichier .msi.
- Le <nom de transformation> est le nom du fichier de la transformation.

Exemple de commande :

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

Installation ou désinstallation du produit en spécifiant les paramètres manuellement

Dans la ligne de commande, exécutez la commande suivante.

Modèle de commande (installation) :

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Ici, le <nom package> est le nom du fichier .msi. Tous les paramètres disponibles et leurs valeurs sont décrits dans "Paramètres de base" (p. 148).

Modèle de commande (désinstallation) :

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

La version du package .msi doit être la même que celle du produit que vous souhaitez désinstaller.

Paramètres d'installation ou de désinstallation sans assistance

Cette section décrit les paramètres d'installation ou de désinstallation sans assistance sous Windows En plus de ces paramètres, vous pouvez utiliser d'autres paramètres de `msiexec`, comme décrit dans https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Paramètres d'installation

Paramètres de base

`ADDLOCAL=<list of components>`

Les composants à installer, séparés par des virgules et sans caractères d'espace. Toues les composants spécifiés doivent être extraits du programme d'installation avant l'installation.

La liste complète des composants est la suivante :

Composant	Doit être installé avec	Nombre de bits	Nom / description du composant
MmsMspComponents		32 bits/64 bits	Composants clés pour les agents

BackupAndRecoveryAgent	MmsMspComponents	32 bits/64 bits	Agent pour Windows
ArxAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour SQL
ARADAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32 bits/64 bits	Agent pour Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32 bits/64 bits	Agent pour Oracle
AcronisESXSupport	MmsMspComponents	64 bits	Agent pour VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32 bits/64 bits	Agent pour Hyper-V
CommandLineTool		32 bits/64 bits	Outil de ligne de commande
TrayMonitor	BackupAndRecoveryAgent	32 bits/64 bits	Moniteur Cyber Protect

`TARGETDIR=<path>`

Le dossier où le produit sera installé. Par défaut, ce dossier est : `C:\Program Files\BackupClient`.

`REBOOT=ReallySuppress`

Si le paramètre est spécifié, il est interdit de redémarrer la machine.

`/l*v <log file>`

Si le paramètre est spécifié, le journal d'installation en mode détaillé sera sauvegardé dans le fichier spécifié. Le fichier journal peut être utilisé pour analyser les problèmes d'installation.

`CURRENT_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, 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

`REGISTRATION_ADDRESS`

Il s'agit de l'URL pour le service Cyber Protect. Vous pouvez utiliser ce paramètre avec les paramètres `REGISTRATION_LOGIN`et `REGISTRATION_PASSWORD`, ou avec le paramètre `REGISTRATION_TOKEN`.

- Lorsque vous utilisez `REGISTRATION_ADDRESS` avec les paramètres `REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`, indiquez l'adresse que vous utilisez **pour vous connecter** au service Cyber Protect. Par exemple, `https://cloud.company.com` :

- Lorsque vous utilisez `REGISTRATION_ADDRESS` avec le paramètre `REGISTRATION_TOKEN`, précisez l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protect. Par exemple, `https://eu2-cloud.company.com`.

  Ne pas utiliser `https://cloud.company.com` ici.

`REGISTRATION_LOGIN` et `REGISTRATION_PASSWORD`

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

`REGISTRATION_PASSWORD_ENCODED`

Le mot de passe du compte sous lequel l'agent sera enregistré dans le service Cyber Protect, encodé dans base64. Pour en savoir plus sur comment encoder votre mot de passe, reportez-vous à « Enregistrement manuel de machines ».

`REGISTRATION_TOKEN`

Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Vous pouvez en générer un dans la console Web, comme décrit dans Déploiement des agents via la règle de groupe.

`REGISTRATION_REQUIRED={0,1}`

Définissez la fin de l'installation en cas d'échec de l'enregistrement. Si la valeur est `1`, l'installation échoue également. La valeur par défaut est `0`, donc si vous n'indiquez pas ce paramètre, l'installation réussit même si l'agent n'est pas enregistré.

Paramètres supplémentaires

Pour définir le compte de connexion pour le service de l'agent dans Windows, utilisez l'un des paramètres suivants :

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`

  Si la valeur est `1`, l'agent s'exécutera sous le compte **système local**.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`

  Si la valeur est `1`, l'agent s'exécutera sous le compte nouvellement créé, intitulé **Acronis Agent User**.
- `MMS_SERVICE_USERNAME= <user name>` et `MMS_SERVICE_PASSWORD=<password>`

  Utilisez ces paramètres pour indiquer un compte existant sous lequel l'agent sera exécuté.

Pour en savoir plus sur les comptes de connexion, reportez-vous à « Changer le compte de connexion sur les machines Windows ».

`SET_ESX_SERVER={0,1}`

- Si la valeur est `0`, l'agent pour VMware installé ne sera pas connecté à un vCenter Server ou un hôte ESXi. Si la valeur est `1`, spécifiez les paramètres suivants :
  - `ESX_HOST= <host name>`

    Le nom d'hôte ou l'adresse IP du vCenter Server ou de l'hôte ESXi.
  - `ESX_USER= <user name>` et `ESX_PASSWORD=<password>`

    Informations d'identification pour accéder au vCenter Server ou à l'hôte ESXi.

`HTTP_PROXY_ADDRESS= <IP address>` et `HTTP_PROXY_PORT=<port>`

Le serveur proxy HTTP utilisé par l'agent. Sans ces paramètres, aucun serveur proxy ne sera utilisé.

`HTTP_PROXY_LOGIN= <login>` et `HTTP_PROXY_PASSWORD=<password>`

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Si la valeur est `0` ou si le paramètre n'est pas spécifié, l'agent utilisera le serveur proxy uniquement pour la sauvegarde et la reprise depuis le Cloud. Si la valeur est `1`, l'agent se connectera aussi au serveur de gestion via le serveur proxy.

Paramètres de désinstallation

`REMOVE={ <list of components> |ALL}`

Les composants sont supprimés, séparés par des virgules et sans caractères d'espace. Si la valeur est `ALL`, tous les composants du produit seront désinstallés.

En complément, vous pouvez spécifier le paramètre suivant :

`DELETE_ALL_SETTINGS={0, 1}`

Si la valeur est `1`, les paramètres de configuration, de tâches et de journaux des produits seront supprimés.

Exemples

- Installation de l'agent pour Windows, de l'outil de ligne de commande et du moniteur de cyberprotection. Enregistrement de la machine dans le service Cyber Protect 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,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_SYSTEM_
ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
REGISTRATION_PASSWORD=johnspassword
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et du moniteur de cyberprotection. Création d'un compte de connexion pour le service de l'agent dans Windows. Enregistrement de la machine dans le service Cyber Protect 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-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande, de l'Agent pour Windows et du moniteur de cyberprotection. Enregistrement de la machine dans le service Cyber Protect à l'aide d'un nom d'utilisateur et encodé dans un mot de passe base64.

```
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://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Installation de l'agent pour Windows, de l'outil de ligne de commande et du moniteur de cyberprotection. Enregistrement de la machine dans le service Cyber Protect 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-cloud.company.com
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
```

- Désinstallation de tous les agents et suppression de leurs journaux, tâche et paramètres de configuration.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

Installation et désinstallation sans assistance 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.

Pour installer ou désinstaller un agent de protection

1. Ouvrir l'application Terminal.

2. Effectuez l'une des actions 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, le `<nom package>` est le nom du package d'installation (un fichier .i686 ou .x86_64). Tous les paramètres disponibles et leurs valeurs sont décrits dans « Paramètres d'installation ou de désinstallation sans assistance ».
- 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>
  ```

  Il se peut que cette approche soit utile si vous ne souhaitez pas saisir d'informations sensibles dans la ligne de commande. Dans ce cas, vous pouvez indiquer les paramètres de configuration dans un fichier texte séparé et vous assurer que vous seul pouvez y accéder.Ajoutez chaque paramètre sur une nouvelle ligne, suivi par la valeur souhaitée, par exemple :

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

  ou

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

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

3. Si UEFI Secure Boot est activé sur la machine, vous êtes informé que vous devez redémarrer le système après l'installation. Veillez à vous rappeler le mot de passe (celui de l'utilisateur racine ou « acronis ») qui doit être utilisé. 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.

Si vous activez UEFI Secure Boot après l'installation de l'agent, répétez l'installation en incluant l'étape 3. Dans le cas contraire, les sauvegardes échoueront.

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 et d'enregistrement (par exemple, paramètres `--login` et `--password` ; `--rain` et paramètres `--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 caractères d'espace. Les composants suivants sont disponibles pour le package d'installation .x86_64 :

Composant	Description du composant
BackupAndRecoveryAgent	Agent pour Linux
AgentForPCS	Agent pour Virtuozzo
OracleAgentFeature	Agent pour Oracle

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

Aussi bien l'agent pour Virtuozzo que l'agent pour Oracle nécessitent que l'agent pour Linux soit également installé.

Le package d'installation .i686 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 Protect, 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.

`{-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, 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 Protect. 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. Vous pouvez en générer un dans la console Web, comme décrit dans Déploiement des agents via la règle de groupe.

  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 Protect.

    Vous n'avez pas à inclure ce paramètre de façon explicite lorsque vous utilisez les paramètres `--login` et `--password` pour l'enregistrement, car l'installateur utilise la bonne adresse par défaut, c'est-à-dire l'adresse que vous utilisez pour **vous connecter** au service Cyber Protect.

Par exemple :

Toutefois, lorsque vous utilisez `{-C|--rain=}` avec le paramètre `--token`, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protect. Par exemple :

- `--register-with-credentials`

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

- `--skip-registration`

  Utilisez ce paramètre si vous avez besoin d'installer l'agent, mais que vous avez l'intention de l'enregistrer dans le service Cyber Protect ultérieurement. Pour en savoir plus sur la façon de procéder, reportez-vous à « Enregistrement manuel de machines ».

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 reprise 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. 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. L'utilisation de cette option n'est pas recommandée.

`--skip-svc-start`

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

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`.

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-cloud.company.com --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 ses journaux, tâches et paramètres de configuration.

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

Installation et désinstallation sans assistance sous macOS

Cette section décrit l'installation, l'enregistrement et la désinstallation de l'agent de protection en mode sans assistance sur un ordinateur sous macOS via la ligne de commande. Pour en savoir plus sur le téléchargement du fichier d'installation (.dmg), reportez-vous à « Ajout d'une machine exécutant macOS ».

Pour installer l'agent pour Mac

1. Créez un répertoire temporaire dans lequel vous monterez le fichier d'installation (.dmg).

```
mkdir <dmg_root>
```

Remplacez `<racine_dmg>` par le nom de votre choix.

2. Montez le fichier .dmg.

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

Remplacez `<fichier_dmg>` par le nom du fichier d'installation. Par exemple, **AcronisAgentMspMacOSX64.dmg**.

3. Exécutez le programme d'installation.

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

4. Détachez le fichier d'installation (.dmg).

```
hdiutil detach <dmg_root>
```

Exemples

-

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
```

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

```
hdiutil detach mydirectory
```

Pour enregistrer l'agent pour Mac

Effectuez l'une des actions suivantes :

- Enregistrez l'agent sous un compte spécifique, à l'aide d'un nom d'utilisateur et d'un mot de passe.

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

Ici :

`<adresse du service Cyber Protect>` est l'adresse que vous utilisez pour vous **connecter** au service Cyber Protect. Par exemple :

`<nom d'utilisateur>` et `<mot de passe>` sont les identifiants du compte sous lequel l'agent sera enregistré. Il ne peut pas s'agir d'un compte administrateur partenaire.

- Vous pouvez également enregistrer l'agent à l'aide d'un jeton d'enregistrement.

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

Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Vous pouvez en générer un dans la console Web Cyber Protect, comme décrit dans Déploiement des agents via la règle de groupe.

Lorsque vous utilisez un jeton d'enregistrement, vous devez préciser l'adresse exacte du centre de données. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protect. Par exemple :

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

Exemples

Enregistrement à l'aide d'un nom d'utilisateur et d'un mot de passe.

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

Enregistrement avec un jeton.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://eu2-cloud company.com --token D91D-DC46-4F0B
  ```

Pour désinstaller l'agent pour Mac

Exécuter la commande suivante :

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

Pour supprimer tous les journaux, toutes les tâches et tous les paramètres de configuration lors de la désinstallation, exécutez la commande suivante :

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

Enregistrement manuel de machines

En plus d'enregistrer une machine dans le service Cyber Protect lors de l'installation de l'agent, vous pouvez également l'enregistrer à l'aide de l'interface de ligne de commande. Il se peut que vous deviez procéder ainsi si vous avez installé l'agent, mais que l'enregistrement automatique a échoué par exemple, ou si vous souhaitez enregistrer une machine existante sous un nouveau compte.

Pour enregistrer une machine

À l'invite de commande de l'ordinateur sur lequel l'agent est installé, exécutez l'une des commandes suivantes :

- Pour enregistrer un ordinateur sous le compte actuel :

  ```
  <path to the registration tool> -o register -s mms -t cloud --update
  ```

  - Le `<chemin d'accès à l'outil d'enregistrement>` est :
    - Sous Windows : `%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - Sous Linux : `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - sous macOS : `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- Pour enregistrer un ordinateur sous un autre compte :

  ```
  <path to the registration tool> -o register -t cloud -a <service address> -u <user name> -p <password>
  ```

  - `<nom d'utilisateur>` et `<mot de passe>` sont les identifiants du compte sous lequel l'agent sera enregistré. Il ne peut pas s'agir d'un compte administrateur partenaire.

    La valeur `<adresse du service>` est l'URL que vous utilisez **pour vous connecter** au service Cyber Protect. Par exemple, `https://cloud.company.com`.

- Pour enregistrer un ordinateur avec un jeton d'inscription :

  ```
  <path to the registration tool> -o register -t cloud -a <service address> --token <token>
  ```

  - Le jeton d'enregistrement est une série de 12 caractères, séparés par des traits d'union en trois segments. Pour en savoir plus sur comment en générer un, reportez-vous à « Déploiement des agents via la stratégie de groupe ».

    Lorsque vous utilisez un jeton d'inscription, vous devez préciser l'adresse exacte du centre de données sous la forme `<adresse du service>`. Il s'agit de l'URL que vous voyez **une fois que vous êtes connecté** au service Cyber Protect. Par exemple, `https://eu2-cloud.company.com`.

Ne pas utiliser `https://cloud.company.com` ici.

Pour désenregistrer une machine

À l'invite de commandes de l'ordinateur sur lequel l'agent est installé, exécutez cette commande :

```
<path to the registration tool> -o unregister
```

Exemples

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t
cloud --update
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

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

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

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --
update
```

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

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

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

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

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

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

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

Mots de passe contenant 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 :

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

Exemple (pour Windows) :

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

Si vous recevez toujours une erreur :

- Encodez votre mot de passe au format base64 sur https://www.base64encode.org/.
- Dans la ligne de commande, indiquez le mot de passe encodé à l'aide du paramètre -b ou --base64.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

Exemple (pour Windows) :

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

Déploiement de l'agent pour oVirt (appliance virtuelle)

Pour plus d'informations sur le déploiement et la configuration de l'agent pour oVirt (appliance virtuelle), reportez-vous à la documentation Cyber Protection Cloud.

Déploiement de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle)

Pour plus d'informations sur le déploiement et la configuration de l'agent pour Virtuozzo Hybrid Infrastructure (appliance virtuelle), reportez-vous à la documentation Cyber Protection Cloud.

Découverte automatique des machines

La découverte automatique vous permet d'effectuer les actions suivantes :

- Automatiser l'installation des agents de protection ainsi que l'inscription des ordinateurs sur le serveur de gestion en détectant les ordinateurs dans votre domaine Active Directory ou votre réseau local.
- Installer et mettre à jour des agents de protection sur plusieurs machines.
- Grâce à la synchronisation avec Active Directory, facilitez le provisionnement de ressources et la gestion des ordinateurs dans un domaine Active Directory important.

Prérequis

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.

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 **Périphériques multiples** du panneau **Ajouter des périphériques**.

L'installation à distance des agents est prise en charge uniquement pour les machines 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.

Fonctionnement de la découverte automatique

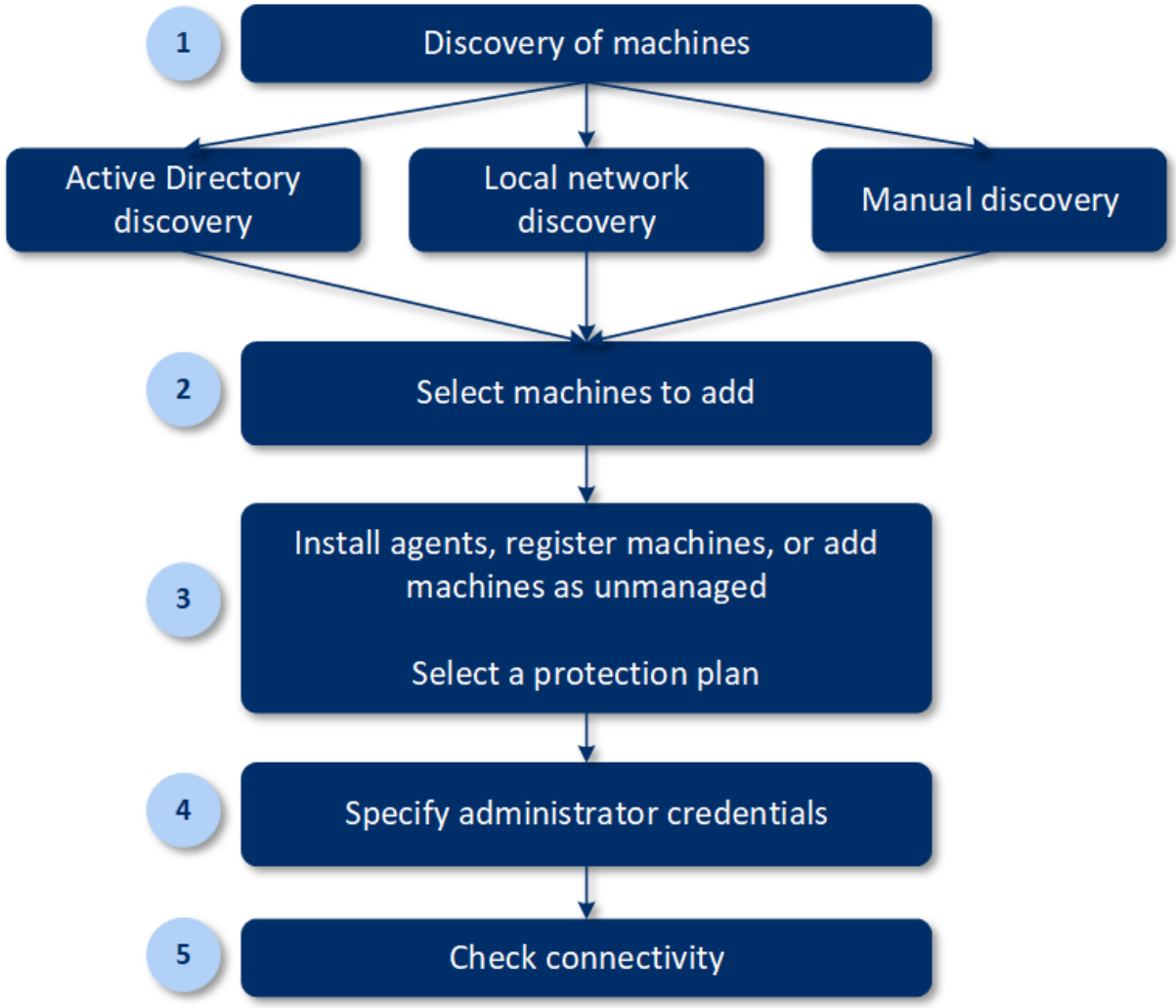
Lors d'une découverte sur le réseau local, l'agent de découverte collecte les informations suivantes pour chaque ordinateur du réseau à l'aide de la découverte NetBIOS, de Web Service Discovery (WSD) et du tableau ARP (Address Resolution Protocol) :

- Nom d'hôte (nom d'hôte NetBIOS/court)
- Nom de domaine pleinement qualifié (FQDN)
- Domaine/Groupe de travail
- Adresses IPv4/IPv6

- Adresses MAC
- Système d'exploitation (nom/version/famille)
- Catégorie de machine (poste de travail, serveur, contrôleur de domaine)

Lors d'une découverte dans Active Directory, l'agent de découverte, en sus de la liste ci-dessus, collecte des informations concernant l'unité d'organisation (UO) des ordinateurs ainsi que des informations plus détaillées concernant leur nom et leur système d'exploitation. Toutefois, les adresses IP et MAC ne sont pas collectées.

Le diagramme suivant résume le processus de découverte automatique.



1. Sélectionnez la méthode de découverte :
   - Découverte dans Active Directory
   - Découverte sur le réseau local
   - Découverte manuelle : en utilisant l'adresse IP ou le nom d'hôte d'un ordinateur, ou en important une liste d'ordinateurs à partir d'un fichier

Les résultats d'une découverte dans Active Directory ou d'une découverte sur le réseau local excluent les ordinateurs sur lesquels des agents de protection sont installés.

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 locataire auquel le compte appartient.

2. Sélectionnez les ordinateurs que vous souhaitez ajouter à votre client.
3. Sélectionnez comment ajouter ces ordinateurs :
   - Installez un agent de protection et des composants supplémentaires sur les ordinateurs, et inscrivez-les dans la console Web.
   - Inscrivez les ordinateurs dans la console Web (si un agent de protection était déjà installé).
   - Ajoutez les ordinateurs à la console Web en tant qu'**ordinateurs 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 Web.
4. Fournissez les identifiants administrateur pour les ordinateurs sélectionnés.
5. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.

   Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.
6. Vérifiez que vous pouvez vous connecter aux ordinateurs à l'aide des identifiants fournis.

Les ordinateurs qui s'affichent dans la console Web Cyber Protect entrent dans les catégories suivantes :

- **Découvert** : ordinateurs qui sont découverts, mais sur lesquels l'agent de protection n'est pas installé.
- **Géré** : ordinateurs sur lesquels l'agent de protection est installé.
- **Non protégé** : ordinateurs auxquels le plan de protection n'est pas appliqué. Les ordinateurs non protégés sont des ordinateurs découverts et des machines gérées auxquels aucun plan de protection n'est appliqué.
- **Protégé** : ordinateurs auxquels un plan de protection est appliqué.

Découverte automatique et découverte manuelle

Avant de démarrer la découverte, assurez-vous de respecter les Prérequis.

Découvrir des machines

1. Dans la console Web, accédez à **Périphériques** > **Tous les périphériques**.
2. Cliquez sur **Ajouter**.
3. Dans **Périphériques multiples**, cliquez sur **Windows uniquement**. L'assistant de découverte s'ouvre.
4. [Si votre organisation comporte des unités] Sélectionnez une unité. Ensuite, dans **Agent de découverte**, vous pourrez sélectionner les agents associés à l'unité sélectionnée et à ses unités enfant.
5. Sélectionnez l'agent de découverte qui exécutera l'analyse pour détecter les machines.
6. Sélectionnez la méthode de découverte :
   - **Rechercher dans Active Directory**. Assurez-vous que la machine sur laquelle l'agent de découverte est installé est membre du domaine Active Directory.
   - **Analyser le réseau local**. Si l'agent de découverte sélectionné ne trouve aucune machine, sélectionnez un autre agent de découverte.
   - **Spécifier manuellement ou importer à partir d'un fichier**. Définissez manuellement les machines à ajouter, ou importez-les à partir d'un fichier texte.
7. [Si la méthode de découverte sur Active Directory est sélectionnée] Sélectionnez comment rechercher des machines :
   - **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.
8. [Si la méthode de découverte sur Active Directory ou sur le réseau local est sélectionnée] Servez-vous d'une liste pour sélectionner les machines que vous souhaitez ajouter.

   [Si la méthode de découverte manuelle est sélectionnée] Spécifiez les adresses IP ou les noms d'hôte, ou importez la liste des machines à partir d'un fichier texte. Le fichier doit contenir des adresses IP/noms d'hôte, un par ligne. Voici un exemple de fichier :

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   Après l'ajout manuel ou l'importation de machines à partir d'un fichier, l'agent essaie d'effectuer un ping des machines ajoutées et de définir leur disponibilité.
9. Sélectionnez quoi faire après la découverte :
   - **Installez les agents et enregistrez les machines**. Vous pouvez sélectionner les composants à installer sur les machines en cliquant sur **Sélectionner les composants**. Pour en savoir plus, reportez-vous à la section « Sélection des composants à installer ». Vous pouvez installer jusqu'à 100 agents simultanément.

À l'écran **Sélectionner les composants**, définissez le compte sous lequel les services seront exécutés en remplissant le champ **Compte d'ouverture de session 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.

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.

- **Enregistrer des machines avec des agents installés**. Cette option est utilisée si l'agent est déjà installé sur des machines et que vous devez uniquement les enregistrer dans Cyber Protect. Si aucun agent n'est trouvé au sein des machines, elles seront ajoutées en tant que machines **non gérées**.
- **Ajouter en tant que machines non gérées**. L'agent ne sera pas installé sur les machines. Vous pourrez les afficher dans la console Web et installer ou enregistrer l'agent ultérieurement.

[Si l'action post découverte **Installez les agents et enregistrez les machines** est sélectionnée] **Redémarrer l'ordinateur si nécessaire :** si l'option est activée, la machine sera redémarrée autant de fois que nécessaire pour terminer l'installation.

Le redémarrage de la machine peut être nécessaire dans l'un des cas suivants :

- L'installation des prérequis est terminée et un redémarrage est requis pour continuer l'installation.
- L'installation est terminée, mais un redémarrage est nécessaire, car certains fichiers sont verrouillés lors de l'installation.
- L'installation est terminée, mais un redémarrage est nécessaire pour d'autres logiciels installés précédemment.

[Si l'option **Redémarrer l'ordinateur si nécessaire** est sélectionnée] **Ne pas redémarrer si l'utilisateur est connecté :** si l'option est activée, la machine ne redémarrera pas automatiquement si l'utilisateur est connecté au système. Par exemple, si un utilisateur est en train de travailler alors que l'installation requiert un redémarrage, le système ne sera pas redémarré.

Si les prérequis ont été installés, mais que le redémarrage n'a pas été effectué, car un utilisateur était connecté, vous devrez redémarrer la machine et recommencer l'installation pour terminer l'installation de l'agent.

Si les prérequis ont été installés, mais que le redémarrage n'a pas été effectué, vous devrez redémarrer la machine.

[Si votre organisation comporte des unités] **Unité où enregistrer les machines :** sélectionnez l'unité où vos machines seront enregistrées.

Si vous avez sélectionné l'une des deux premières actions post-découverte, vous avez également la possibilité d'appliquer le plan de protection aux machines. Si vous possédez plusieurs plans de protection, vous pouvez sélectionner celui à utiliser.

10. Fournissez les identifiants de l'utilisateur qui dispose de droits d'administrateur pour toutes les machines.

    Important
    Notez que 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 informations d'identification d'administrateur personnalisées, vous devrez effectuer des préparatifs manuels supplémentaires, comme décrit dans Ajout d'une machine fonctionnant sous Windows > Préparation.

11. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.

    Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.

12. Le système vérifie la connectivité à toutes les machines. En cas d'échec de connexion à certaines des machines, vous pouvez modifier leurs identifiants.

Une fois la découverte des machines démarrée, vous trouverez les tâches correspondantes dans l'activité **Tableau de bord** > **Activités** > **Découverte de machines**.

Sélection des composants à installer

Vous trouverez la description des composants obligatoires et supplémentaires dans le tableau suivant :

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 Hyper-V	Cet agent sauvegarde des machines virtuelles Hyper-V et sera installé sur des hôtes Hyper-V. Il sera installé s'il est sélectionné et si un rôle Hyper-V est détecté sur une machine.
Agent pour SQL	Cet agent sauvegarde des bases de données SQL Server et sera installé sur des machines exécutant Microsoft SQL Server. Il sera 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 sera installé sur des machines exécutant le rôle de boîte aux lettres de Microsoft SQL Server. Il sera 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 sera installé sur des contrôleurs de domaine. Il sera 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 sera installé sur des machines Windows ayant un accès réseau à vCenter Server. Il sera installé s'il est sélectionné.
Agent pour Office 365	Cet agent sauvegarde des boîtes aux lettres Microsoft 365 vers une destination locale, et sera installé sur des machines Windows. Il sera installé s'il est sélectionné.
Agent pour Oracle	Cet agent sauvegarde des bases de données Oracle et sera installé sur des machines exécutant Oracle Database. Il sera installé s'il est sélectionné.
Cyber Protect Moniteur	Ce composant permet à un utilisateur de contrôler l'exécution des tâches en cours dans la zone de notification, et sera installé sur des machines Windows. Il sera installé s'il est sélectionné.
Outil de ligne de commande	Cyber Protect 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. Il sera installé s'il est sélectionné.
Bootable Media Builder	Ce composant permet aux utilisateurs de créer un support de démarrage et, s'il est sélectionné, sera installé sur des ordinateurs Windows.

Gestion des machines découvertes

Une fois le processus de découverte effectué, vous trouverez toutes les machines découvertes dans **Périphériques** > **Machines non gérées**.

Cette section est divisée en sous-sections en fonction de la méthode de découverte utilisée. La liste complète des paramètres de machine s'affiche ci-dessous (elle peut varier en fonction de la méthode de découverte) :

Nom	Description
Nom	Le nom de la machine. L'adresse IP s'affichera si le nom de la machine ne peut pas être découvert.
Adresse IP	L'adresse IP de la machine.
Type de découverte	La méthode de découverte utilisée pour détecter la machine.
Unité d'organisation	L'unité d'organisation à laquelle appartient la machine dans Active Directory. Cette colonne s'affiche si vous consultez la liste des machines dans **Machines non gérées** > **Active Directory**.
Système d'exploitation	Le système d'exploitation installé sur la machine.

Il existe une section **Exceptions**, où vous pouvez ajouter les machines à ignorer lors du processus de découverte. Par exemple, si vous ne souhaitez pas que des machines spécifiques soient découvertes, vous pouvez les ajouter à la liste.

Pour ajouter une machine à la section **Exceptions**, sélectionnez-la dans la liste, puis cliquez sur **Ajouter aux exceptions**. Pour retirer une machine de la section **Exceptions**, accédez à **Machines non gérées** > **Exceptions**, sélectionnez la machine, puis cliquez sur **Retirer des exceptions**.

Vous pouvez installer l'agent de protection et enregistrer un lot de machines découvertes dans Cyber Protect en les sélectionnant dans la liste et en cliquant sur **Installer et enregistrer**. L'assistant ouvert vous permet aussi d'assigner le plan de protection à un lot de machines.

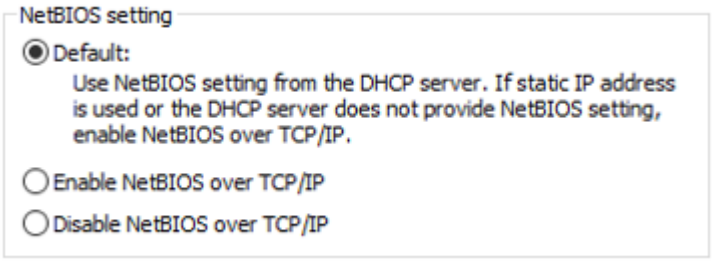
Une fois l'agent de protection installé sur des machines, ces machines s'afficheront dans la section **Périphériques** > **Machines avec des agents**.

Pour vérifier l'état de la protection, accédez à **Tableau de bord** > **Présentation** et ajoutez le widget **État de protection** ou le widget **Machines découvertes**.

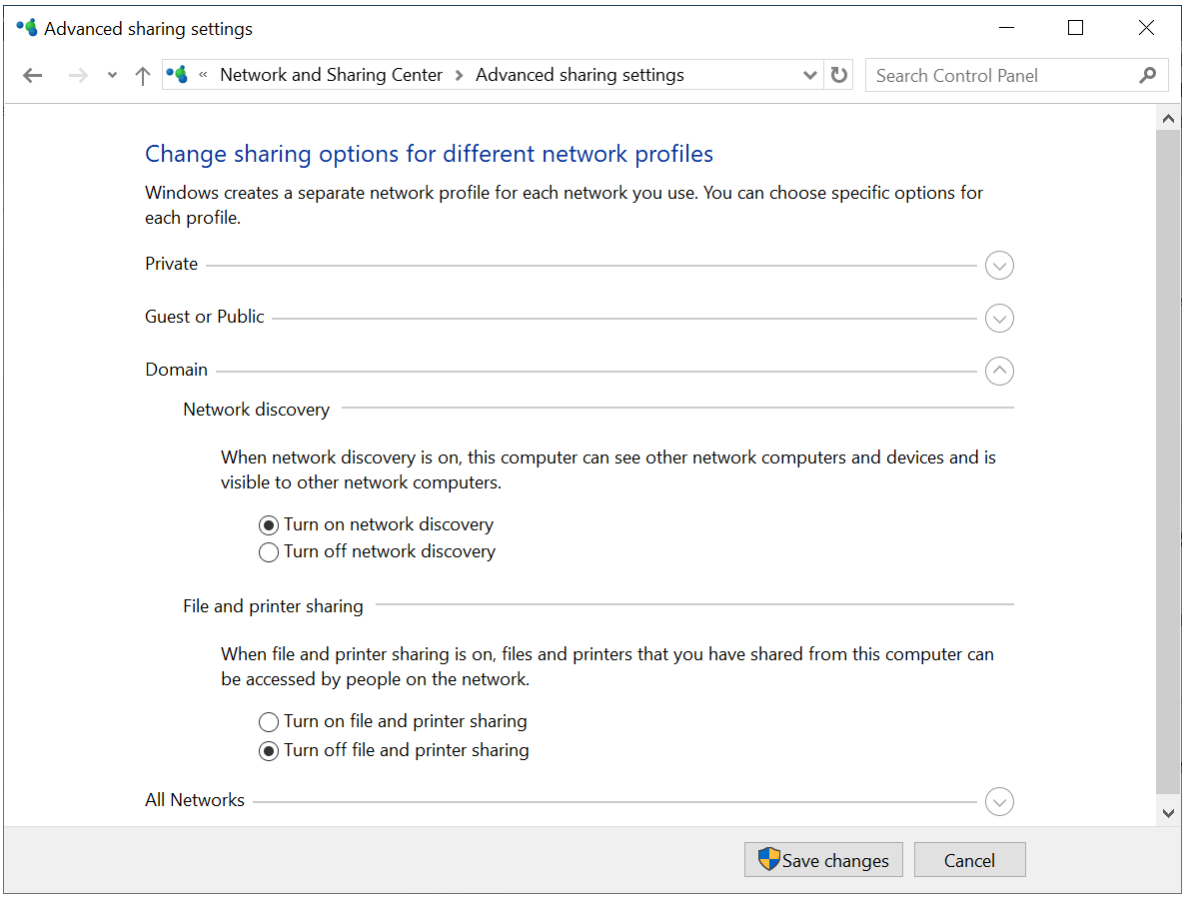
Dépannage

Si vous rencontrez le moindre problème avec la fonctionnalité de découverte automatique, essayez les solutions 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.



- Vérifiez que le service **Hôte du fournisseur de découverte de fonctions** est en cours d'exécution sur l'ordinateur qui se charge de la découverte, ainsi que sur les ordinateurs à découvrir.
- Vérifiez que le service **Publication des ressources de découverte de fonctions** est en cours d'exécution sur les ordinateurs à découvrir.

Déploiement de l'agent pour VMware (matériel virtuel) à partir d'un modèle OVF

Avant de commencer

Configuration système requise pour l'agent

Par défaut, 4 Go de RAM et 2 vCPU sont attribués au matériel virtuel, ce qui est optimal et suffisant pour la plupart des opérations. Nous vous recommandons d'augmenter ces ressources à 8 Go de RAM et 4 vCPU si la bande passante du trafic de sauvegarde est susceptible de dépasser 100 Mo par seconde (par exemple sur les réseaux 10 Gbit), afin d'améliorer les performances de sauvegarde.

Les propres disques virtuels du matériel 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.

Remarque
Les API vStorage doivent être installées sur l'hôte ESXi pour autoriser la sauvegarde de machines virtuelles. Voir https://kb.acronis.com/content/14931.

De combien d'agents ai-je besoin ?

Même si un matériel virtuel est capable de protéger un environnement vSphere tout entier, une bonne pratique consiste à déployer un matériel virtuel 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 le matériel virtuel 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 au matériel virtuel). Pour plus d'informations importantes à prendre en compte, consultez l'article « Utilisation d'un stockage attaché localement ».

Désactiver le planificateur de ressources partagées (PRP) automatique pour l'agent

Si le matériel virtuel est déployé sur un cluster vSphere, veillez à désactiver le vMotion automatique pour celui-ci.Dans les paramètres RPR du cluster, activez des niveaux d'automatisation de machine virtuelle individuels, puis définissez **Niveau d'automatisation** du matériel virtuel sur **Désactivé**.

Déploiement du modèle OVF

Emplacement du modèle OVF

Le modèle OVF consiste en un fichier .ovf et deux fichiers .vmdk.

Dans les déploiements sur site

Une fois l'installation du serveur de gestion terminée, le package OVF de l'appliance virtuelle se trouve dans le dossier **%ProgramFiles%\Acronis\ESXAppliance** (sous Windows) ou **/usr/lib/Acronis/ESXAppliance** (sous Linux).

Dans les déploiements Cloud

1. Cliquez sur **Tous les périphériques** > **Ajouter** > **VMware ESXi** > **Matériel virtuel (OVF)**.
   L'archive ZIP est téléchargée sur votre machine.
2. Décompressez l'archive ZIP.

Déploiement du modèle OVF

1. Assurez-vous que les fichiers de modèle OVF sont accessibles à partir de la machine exécutant vSphere Client.
2. Lancez le client vSphere et connectez-vous au vCenter Server.
3. 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 dans les déploiements Cloud, assurez-vous de sélectionner un réseau qui autorise une connexion Internet, afin que l'agent puisse s'enregistrer correctement dans le Cloud. Lors de la configuration de connexions réseau dans les déploiements sur site, sélectionnez un réseau qui inclut le serveur de gestion.

Configuration du matériel virtuel

1. **Démarrage de l'appareil virtuel**
   Dans le vSphere Client, affichez **Inventaire**, cliquez avec le bouton droit de la souris sur le nom du matériel virtuel, puis sélectionnez **Alimentation** > **Mettre sous tension**. Sélectionnez l'onglet **Console**.
2. **Serveur proxy**
   Si un serveur proxy est activé sur votre réseau :
   a. Pour démarrer l'interface de commande, appuyez sur CTRL+SHIFT+F2 lorsque vous vous trouvez dans l'interface utilisateur du matériel virtuel.
   b. Ouvrez le fichier **/etc/Acronis/Global.config** dans un éditeur de texte.

c. Effectuez l'une des actions suivantes :
   - Si les paramètres de proxy ont été précisés lors de l'installation de l'agent, recherchez 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>
     ```

   - Autrement, copiez les lignes ci-dessus et collez-les dans le fichier entre les balises `<registry name="Global">...</registry>`.

d. Remplacez `ADRESSE` par la nouvelle adresse IP/nom d'hôte de serveur proxy et `PORT` par la valeur décimale du numéro de port.
e. Si votre serveur proxy nécessite une authentification, remplacez `IDENTIFIANT` et `MOT DE PASSE` par les informations de connexion au serveur proxy. Dans le cas contraire, supprimez ces lignes du fichier.
f. Enregistrez le fichier.
g. Ouvrez le fichier **/opt/acronis/etc/aakore.yaml** dans un éditeur de texte.
h. Trouvez 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
   ```

i. 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.
j. Exécutez la commande **`reboot`**.

Sinon, ignorez cette étape.

3. **Paramètres réseau**

   La connexion réseau de l'agent est configurée automatiquement en utilisant le protocole de configuration d'hôte dynamique (Dynamic Host Configuration Protocol - DHCP). Pour modifier la configuration par défaut, sous **Options de l'agent**, dans **eth0**, cliquez sur **Modifier** et spécifiez les paramètres réseau souhaités.

4. **vCenter/ESX(i)**

   Sous **Options de l'agent**, dans **vCenter/ESX(i)**, cliquez sur **Modifier** et spécifiez le nom du serveur vCenter ou son adresse IP. L'agent pourra sauvegarder et restaurer toute machine virtuelle gérée par le serveur vCenter.

   Si vous n'utilisez pas un serveur vCenter, précisez le nom ou l'adresse IP de l'hôte ESXi pour lequel vous voulez sauvegarder et restaurer les machines virtuelles. Normalement, les sauvegardes s'exécutent plus rapidement quand l'agent sauvegarde les machines virtuelles hébergées sur son propre hôte.

Spécifiez les identifiants que l'agent utilisera pour se connecter au vCenter Server ou ESXi. Nous vous conseillons d'utiliser un compte auquel le rôle **Administrateur** a été attribué. Dans le cas contraire, veuillez fournir un compte avec les privilèges nécessaires sur le vCenter Server ou ESXi.

Vous pouvez cliquer sur **Vérifier la connexion** pour vous assurer que les informations d'identification d'accès sont exactes.

5. **Serveur de gestion**
   a. Sous **Options de l'agent**, dans **Serveur de gestion**, cliquez sur **Modifier**.
   b. Dans **Nom/IP du serveur**, effectuez l'une des actions suivantes :
      - Pour un déploiement sur site, sélectionnez **Local**. Spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé.
      - Pour un déploiement dans le Cloud, sélectionnez **Cloud**. Le logiciel affiche l'adresse du service de cybeprotection. Sauf indication contraire, ne modifiez pas cette adresse.
   c. Dans **Nom d'utilisateur** et **Mot de passe**, effectuez l'une des actions suivantes :
      - Pour un déploiement sur site, spécifiez le nom d'utilisateur et le mot de passe d'un administrateur de serveur de gestion.
      - Pour un déploiement dans le Cloud, spécifiez le nom d'utilisateur et le mot de passe du service de cyber protection. L'agent et les machines virtuelles gérées par celui-ci seront enregistrés sous ce compte.
6. **Fuseau horaire**

   Sous **Machine virtuelle**, dans **Fuseau horaire**, cliquez sur **Modifier**. Sélectionnez le fuseau horaire de votre emplacement afin de vous assurer que les opérations planifiées sont exécutées au bon moment.
7. **[Facultatif] Stockages locaux**

   Vous pouvez connecter un disque supplémentaire au matériel virtuel pour que l'agent pour VMware puisse effectuer des sauvegardes sur ce stockage connecté localement.

   Ajoutez le disque en modifiant les paramètres de la machine virtuelle et cliquez sur **Actualiser**. Le lien **Créer un stockage** devient disponible. Cliquez sur ce lien, sélectionnez le disque puis donnez-lui un nom.

Déploiement de l'agent pour HC3 de Scale Computing (matériel virtuel)

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

Lorsque vous déployez l'appliance virtuelle, vous pouvez choisir parmi différentes combinaisons de vCPU et RAM. 2 vCPU et 4 Gio de RAM sont optimaux et suffisants pour la plupart des opérations. Nous vous recommandons d'augmenter ces ressources à 4 vCPU et 8 Gio de RAM si la bande passante du trafic de sauvegarde est susceptible de dépasser 100 Mo par seconde (par exemple sur les réseaux 10 Gbit), afin d'améliorer les performances de sauvegarde.

Les propres disques virtuels du matériel n'occupent pas plus de 6 Go de stockage.

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 gère un nombre égal de machines.

La redistribution automatique a lieu lorsqu'un déséquilibre de charge entre les agents atteint 20 %. Cela peut se produire, par exemple, lorsqu'une machine ou un agent est ajouté ou supprimé. 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 distribuées 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 l'interface Web Cyber Protect.

Vous pouvez voir le résultat de la distribution automatique :

- Dans la colonne **Agent** pour chaque machine virtuelle dans la section **Tous les périphériques**
- Dans la section **Machines virtuelles attribuées** du volet **Détails** lorsqu'un agent est sélectionné dans **Paramètres** > **Agents**

Déploiement de l'appliance virtuelle

1. Connectez-vous à votre compte Cyber Protect.
2. Cliquez sur **Périphériques** > **Tous les périphériques** > **Ajouter** > **Scale Computing HC3**.
3. Sélectionnez le nombre d'appliances virtuelles à déployer.
4. Indiquez l'adresse IP ou le nom d'hôte du cluster Scale Computing HC3.
5. Spécifiez les identifiants d'un compte dont le rôle **Création/Modification de MV** est attribué dans ce cluster.
6. Indiquez un partage réseau qui sera utilisé pour le stockage temporaire du fichier image de l'appliance virtuelle. Un minimum de 2 Go d'espace libre est nécessaire.

7. Spécifiez les identifiants d'un compte disposant d'un accès en lecture/écriture à ce partage réseau.
8. Cliquez sur **Déployer**.

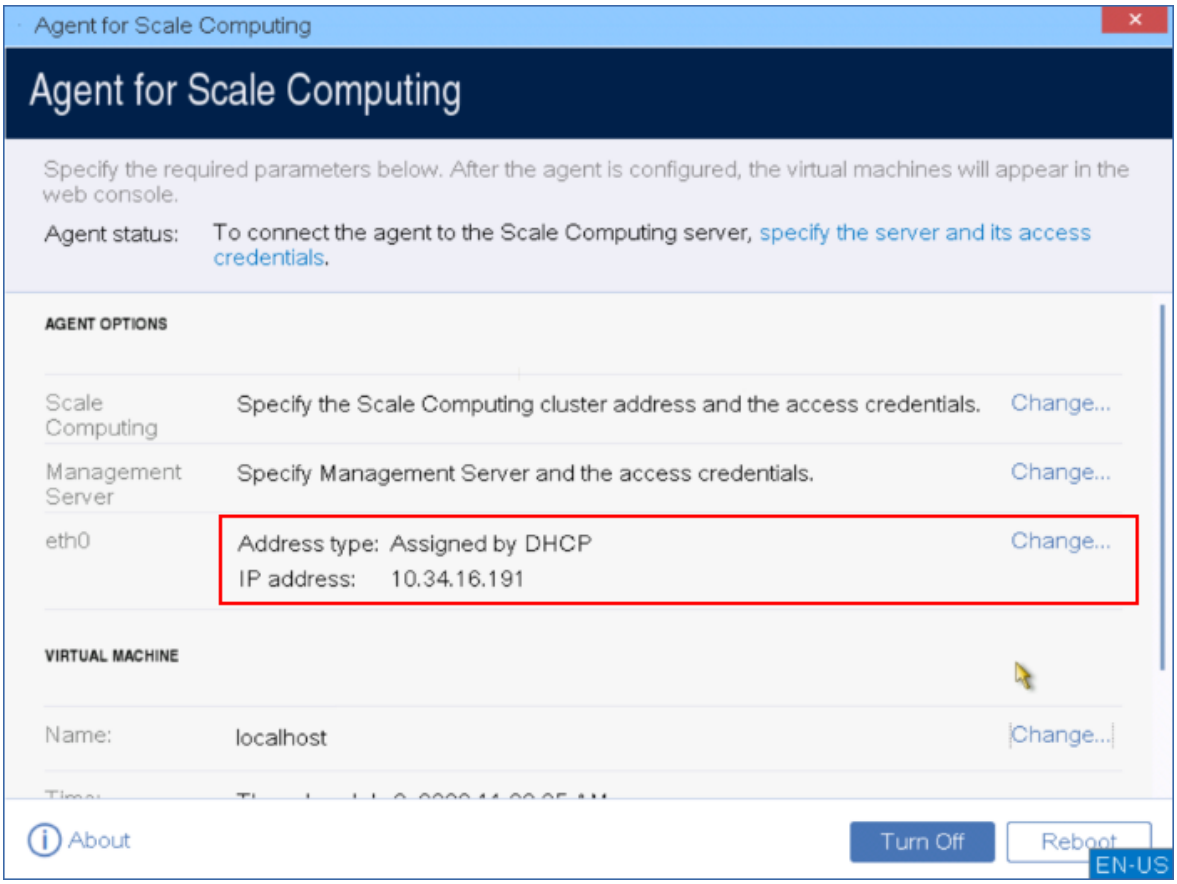
Une fois le déploiement terminé, configurez l'appliance virtuelle.

Configuration du matériel virtuel

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 serveur de gestion Cyber Protect.

Pour configurer l'appareil virtuel

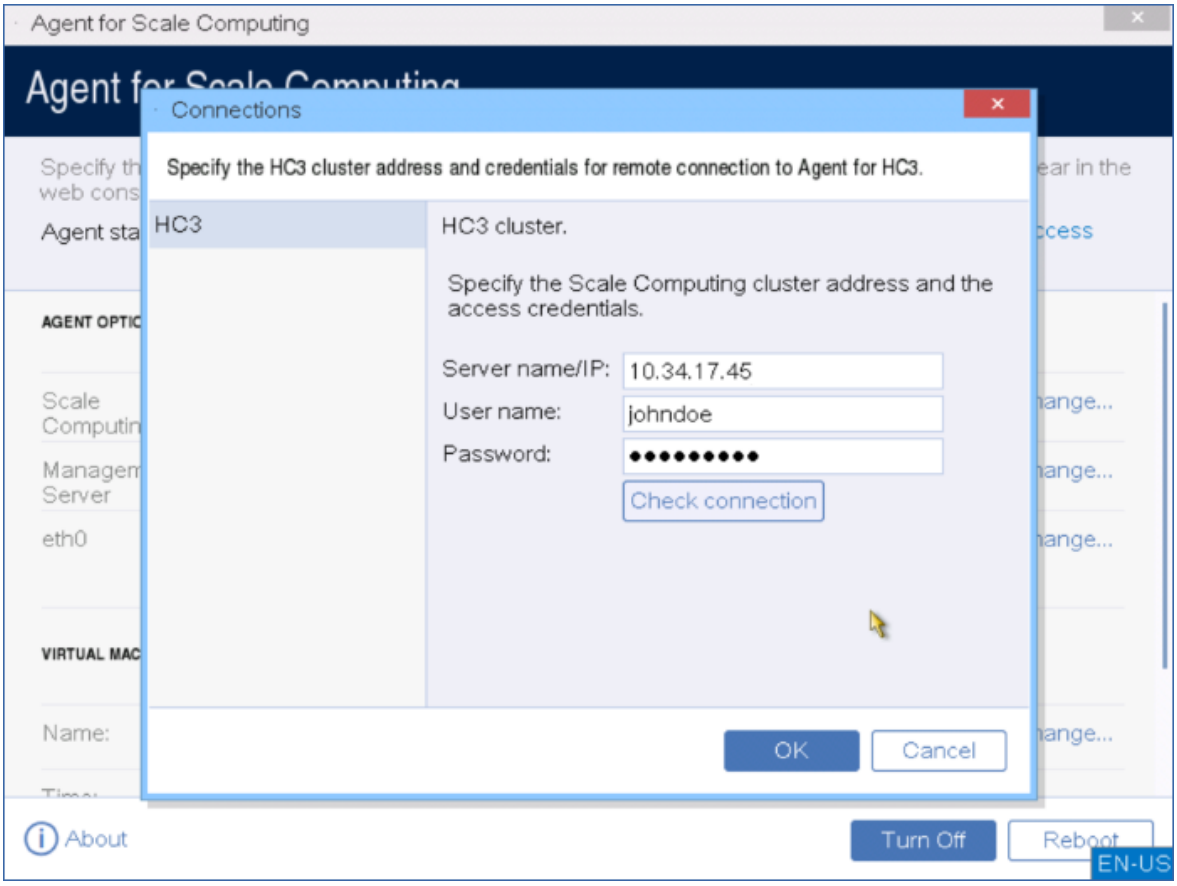
1. Connectez-vous à votre compte Scale Computing HC3.
2. Sélectionnez la machine virtuelle avec l'agent que vous devez configurer, puis cliquez sur **Console**.
3. Configurez les interfaces réseau de l'appliance. Vous aurez peut-être une ou plusieurs interfaces à configurer, selon le nombre de réseaux que l'appliance utilise. 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.



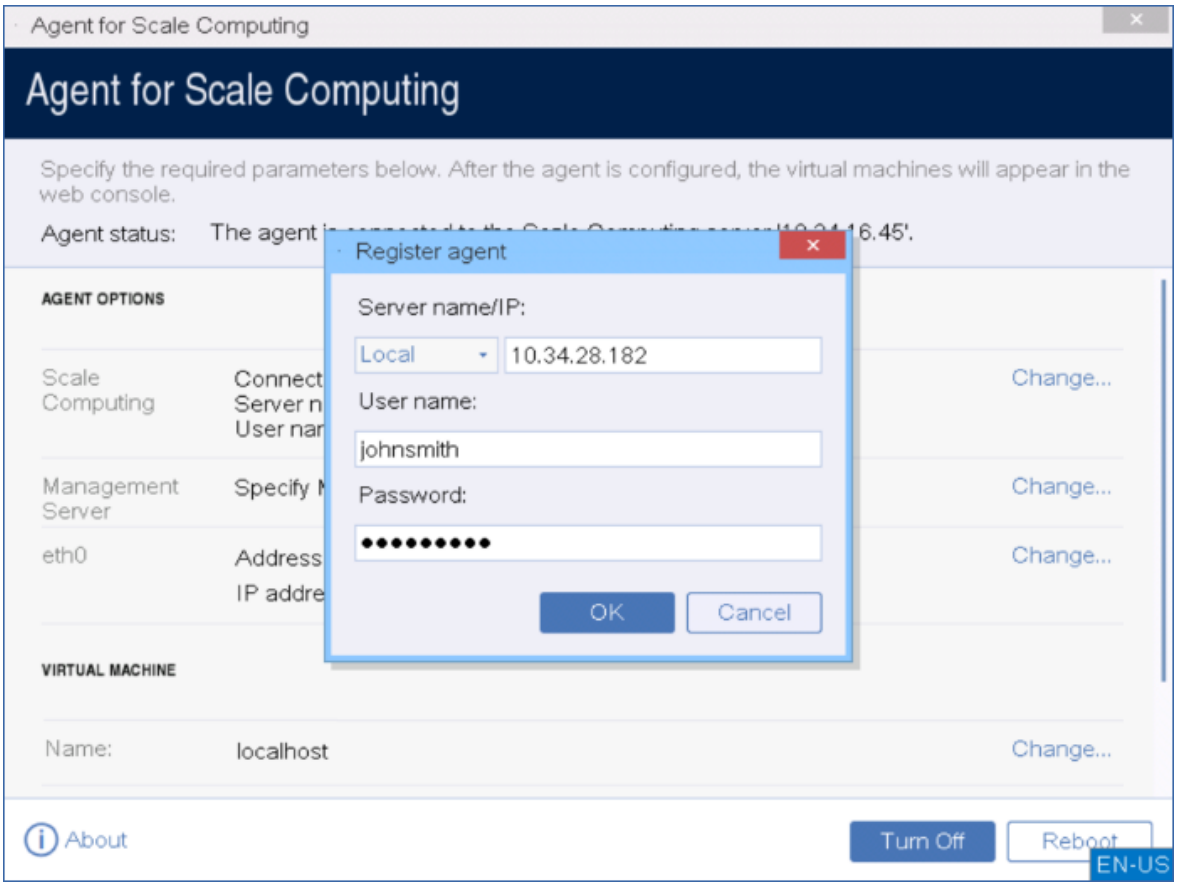
4. Indiquez l'adresse et les identifiants du cluster Scale Computing HC3 :

- Nom DNS ou adresse IP du cluster.
- Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les identifiants du compte Scale Computing HC3 qui possède les rôles appropriés.

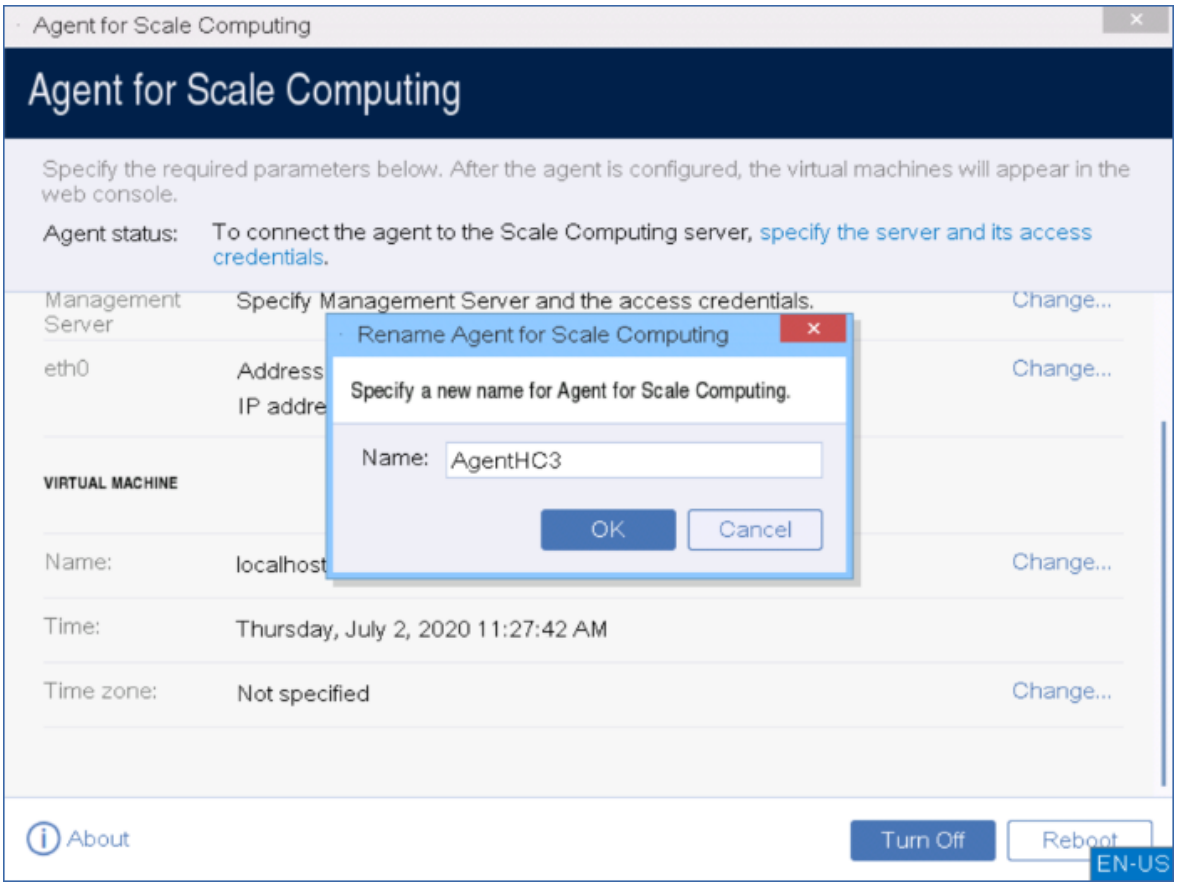
Vous pouvez cliquer sur **Vérifier la connexion** pour vous assurer que les informations d'identification d'accès sont exactes.



5. Indiquez l'adresse et les identifiants du serveur de gestion Cyber Protect pour y accéder.



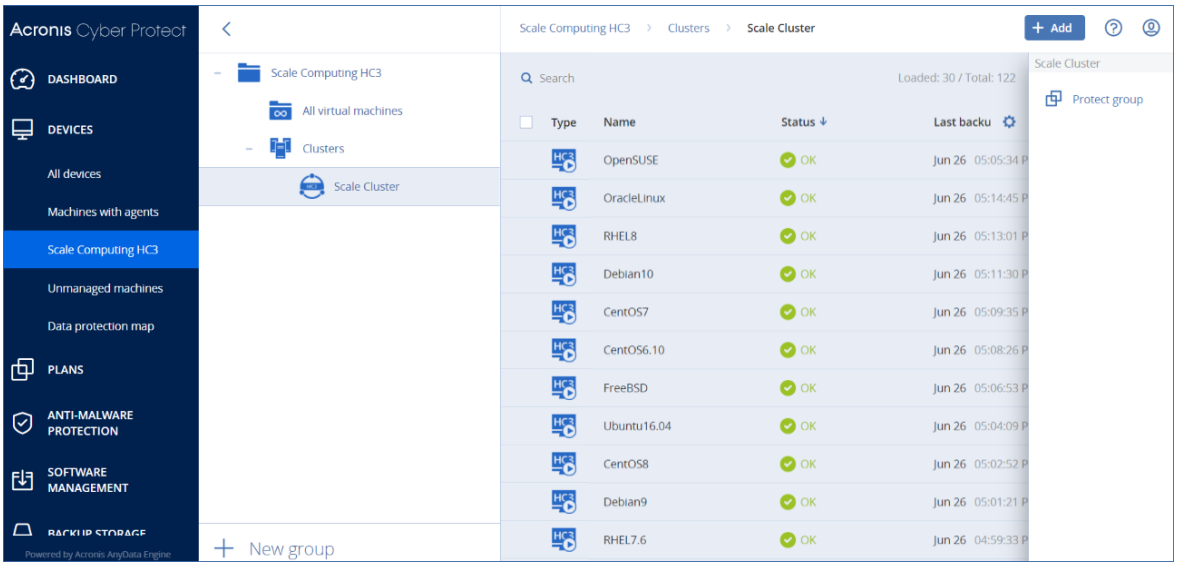
6. [Facultatif] Spécifiez un nom pour l'agent. Ce nom apparaîtra dans la console Web Cyber Protect.



7. [Facultatif] Sélectionnez le fuseau horaire de votre emplacement afin de vous assurer que les opérations planifiées sont exécutées au bon moment.

Pour protéger les machines virtuelles du cluster Scale Computing HC3

1. Connectez-vous à votre compte Cyber Protect.
2. Accédez à **Périphériques** > **Scale Computing HC3**> <votre cluster>, ou recherchez vos ordinateurs dans **Périphériques** > **Tous les périphériques**.
3. Sélectionnez les machines souhaitées 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, ainsi que pour le déploiement d'appliances virtuelles.

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 d'appliance virtuelle	Création/Modification de MV

Déploiement des agents via la stratégie de groupe

Vous pouvez installer (ou déployer) de manière centrale l'agent pour Windows sur des machines membres d'un domaine de répertoire actif, à l'aide de la stratégie de groupe.

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

Avant de procéder au déploiement de l'agent, veuillez vous assurer que :

- Vous avez un domaine Active Directory avec un contrôleur de domaine exécutant Microsoft Windows Server 2003 ou une version ultérieure.
- Vous êtes un membre du groupe **Domain Admins** dans le domaine.

- Vous avez téléchargé le programme d'installation **Tous les agents pour l'installation dans Windows**. Le lien pour le téléchargement est disponible à la page **Ajouter des terminaux** de la console Web Cyber Protect.

Etape 1 : Génération d'un jeton d'enregistrement

Un jeton d'inscription transmet votre identité au programme d'installation sans stocker votre identifiant et votre mot de passe pour la console Web Cyber Protect. Par conséquent, vous pouvez enregistrer autant de machines que vous le souhaitez sur votre compte. Pour plus de sécurité, un jeton a une durée de validité limitée.

Générer un jeton d'enregistrement

1. Connectez-vous à la console Web Cyber Protect grâce aux identifiants du compte auquel les ordinateurs doivent être attribués.
2. Cliquez sur **Tous les périphériques** > **Ajouter**.
3. Cherchez **Jeton d'enregistrement**, puis cliquez sur **Générer**.
4. Spécifiez la durée de validité du jeton, puis cliquez sur **Générer le jeton**.
5. Copiez le jeton ou notez-le par écrit. Assurez-vous d'enregistrer le jeton si vous en avez besoin ultérieurement.
   Vous pouvez cliquer sur **Gérer les jetons actifs** pour afficher et gérer les jetons déjà générés. Notez que pour des raisons de sécurité, ce tableau n'affiche pas l'intégralité des valeurs de jeton.

Étape 2 : Création du fichier de transformation .mst et extraction du paquet d'installation

1. Connectez-vous en tant qu'administrateur sur n'importe quelle machine du domaine.
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. Démarrez le programme d'installation.
4. Cliquez sur **Créer des fichiers .mst et .msi pour une installation sans assistance**.
5. Vérifiez ou modifiez les paramètres d'installation qui seront ajoutés au fichier .mst. Quand vous renseignez la méthode de connexion au serveur de gestion, sélectionnez **Utiliser un jeton d'enregistrement**, puis saisissez le jeton généré.
6. Cliquez sur **Continuer**.
7. Dans **Sauvegardez les fichiers dans**, spécifiez le chemin d'accès au dossier que vous avez créé.
8. Cliquez sur **Générer**.

En conséquence, le fichier de transformation .mst est généré et les packages d'installation .msi et .cab sont extraits vers le dossier que vous avez créé.

Étape 3 : Configuration des objets de stratégie de groupe

1. Connectez-vous au contrôleur du domaine en tant qu'administrateur de domaine. Si le domaine possède plus d'un contrôleur de domaine, connectez-vous sur l'un d'entre eux en tant qu'administrateur de domaine.
2. Si vous prévoyez de déployer l'agent dans une unité organisationnelle, assurez-vous que celle-ci existe dans le domaine. Sinon, ignorez cette étape.
3. Dans le menu **Démarrer**, pointez sur **Outils administratifs** puis cliquez sur **Utilisateurs et ordinateurs Active Directory** (sous Windows Server 2003) ou **Gestion des stratégies de groupe** (sous Windows Server 2008 ou version ultérieure).
4. Sous Windows Server 2003 :
   - Cliquez avec le bouton droit de la souris 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**.

   Sous Windows Server 2008 ou version ultérieure :
   - Cliquez avec le bouton droit de la souris sur le nom du domaine ou l'unité d'organisation, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici.**.
5. Nommez le nouvel objet de la Stratégie de groupe **Agent pour Windows.**
6. Ouvrez l'objet de la Stratégie de groupe **Agent pour Windows** pour le modifier, comme suit :
   - Dans Windows Server 2003, cliquez sur l'objet de la Stratégie de groupe, puis cliquez sur **Modifier**.
   - Dans Windows Server 2008 ou version ultérieure, sous **Objets de la stratégie de groupe**, faites un clic droit avec la souris sur l'objet Stratégie de groupe, puis cliquez sur **Modifier**.
7. Dans le composant logiciel enfichable de l'Editeur d'objet Stratégie de groupe, développez **Configuration de l'ordinateur**.
8. Sous Windows Server 2003 et Windows Server 2008 :
   - Développez **Paramètres du logiciel**.

   Sous Windows Server 2012 ou version ultérieure :
   - Développez **Stratégies** > **Paramètres du logiciel**.
9. Cliquez avec le bouton droit de la souris sur **Installation du logiciel**, placez le pointeur sur **Nouveau**, puis cliquez sur **Package**.
10. Sélectionnez le package .msi d'installation de l'agent dans le dossier partagé que vous avez créé précédemment, puis cliquez sur **Ouvrir**.
11. Dans la boîte de dialogue **Déployer le logiciel**, cliquez sur **Avancées**, puis sur **OK**.
12. Dans l'onglet **Modifications**, cliquez sur **Ajouter**, puis sélectionnez le fichier de transformation .mst préalablement créé.
13. Cliquez sur **OK** pour fermer la boîte de dialogue **Déployer le logiciel**.

Mise à jour d'appliances virtuelles

Déploiements sur site

Pour mettre à jour une appliance virtuelle (Agent pour VMware ou Agent pour Scale Computing HC3) dont la version est antérieure à la version 15.24426 (publiée en septembre 2020), suivez la procédure détaillée dans "Mise à jour des agents" (p. 186).

Pour mettre à jour une appliance virtuelle vers la version 15.24426 ou ultérieure

1. Téléchargez le package de mise à jour comme décrit dans http://kb.acronis.com/latest.
2. Enregistrez les fichiers `.tar.bz` dans le répertoire suivant de l'ordinateur du serveur de gestion :
   - Windows : `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux : `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. Dans la console Web Cyber Protect, cliquez sur **Paramètres** > **Agents**.
   Le logiciel affiche la liste des machines. Les ordinateurs dont les appliances virtuelles sont obsolètes sont marqués d'un point d'exclamation orange.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez effectuer une mise à jour des appliances virtuelles. Ces ordinateurs doivent être en ligne.
5. Cliquez sur **Mettre à jour l'agent**.
6. Sélectionnez l'agent de déploiement.
7. Spécifiez les informations d'identification d'un compte disposant de privilèges d'administration sur la machine cible.
8. Sélectionnez le nom ou l'adresse IP que l'agent utilisera pour accéder au serveur de gestion.
   Par défaut, le nom du serveur est choisi. Vous devrez peut-être modifier ce paramètre si le serveur DNS ne parvient pas à résoudre le nom vers l'adresse IP, ce qui engendre une erreur lors de l'enregistrement de l'appliance virtuelle.

La progression de la mise à jour est affichée dans l'onglet **Activités**.

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

Déploiement Cloud

Pour obtenir des informations sur comment mettre à jour une appliance virtuelle dans un déploiement dans le Cloud, consultez la section Mise à jour des agents dans la documentation Cloud.

Mise à jour des agents

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 machine, 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 ici https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Pour connaître la version de l'agent, sélectionnez la machine, puis cliquez sur **Détails**.

Vous pouvez mettre à jour des agents en utilisant la console Web Cyber Protect ou en les réinstallant selon les méthodes proposées. Pour mettre à jour plusieurs agents en même temps, procédez comme suit.

Pour mettre à jour des agents à l'aide de la console Web Cyber Protect

1. [Uniquement dans des déploiements sur site] Mettez à jour le serveur de gestion.
2. [Uniquement dans des déploiements sur site] Assurez-vous que les packages d'installation sont présents sur l'ordinateur avec le serveur de gestion. Pour connaître les étapes exactes, reportez-vous à « Ajout d'une machine fonctionnant sous Windows » > « Packages d'installation ».
3. Dans la console Web Cyber Protect, cliquez sur **Paramètres** > **Agents**.
   Le logiciel affiche la liste des machines. Les machines dont la version des agents est obsolète sont marquées d'un point d'exclamation orange.
4. Sélectionnez les machines sur lesquelles vous souhaitez effectuer une mise à jour des agents. Ces machines doivent être en ligne.
5. Cliquez sur **Mettre à jour l'agent**.
6. Sélectionnez l'agent de déploiement.
7. Spécifiez les informations d'identification d'un compte disposant de privilèges d'administration sur la machine cible.
8. Sélectionnez le nom ou l'adresse IP du serveur de gestion que l'agent utilisera pour accéder à ce serveur.
   Par défaut, le nom du serveur est sélectionné. Vous devrez peut-être sélectionner l'adresse IP si le serveur de gestion comporte plusieurs interfaces réseau ou si vous rencontrez des problèmes de DNS qui provoquent l'échec de l'inscription de l'agent.
9. [Uniquement dans des déploiements sur site] La progression de la mise à jour est affichée dans l'onglet **Activités**.

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

Pour mettre à jour les définitions Cyber Protect sur un ordinateur

1. Cliquez sur **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur sur lequel vous souhaitez effectuer une mise à jour des définitions de Cyber Protect, 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 attribuer le rôle Responsable de la mise à jour, cliquez sur **Détails**, puis, dans la section **Définitions de Cyber Protect**, activez **Utilisez cet agent pour télécharger et distribuer des correctifs et des mises à jour**.

Pour effacer les données en cache sur un agent

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 niveau vers Acronis Cyber Protect 15

Vous pouvez mettre à niveau un produit de version précédente vers Acronis Cyber Protect 15 des façons suivantes :

- Directement, sans désinstaller le produit précédent.
  Cette option est disponible uniquement pour Acronis Backup 12.5 Update 5 (version 16180) et les versions ultérieures.
- En désinstallant le produit précédent et en installant une nouvelle copie de Acronis Cyber Protect 15.
  Cette option est disponible pour tous les produits éligibles. Pour plus d'informations sur ces produits, veuillez consulter cet article de la base de connaissances.

Remarque
Nous vous recommandons de sauvegarder votre système avant la mise à niveau. Vous pourrez ainsi rétablir la configuration originale si votre mise à niveau échoue.

Pour démarrer la mise à niveau, exécutez le programme d'installation et suivez les instructions qui s'affichent à l'écran.

Le serveur de gestion d'Acronis Cyber Protect 15 est rétrocompatible avec les agents de la version 12.5 et les prend en charge. Toutefois, ces agents ne sont pas compatibles avec les fonctionnalités Cyber Protect.

La mise à niveau des agents n'interfère pas avec les jeux de sauvegardes existants ni avec leurs paramètres.

Désinstallation du produit

Si vous souhaitez supprimer des composants de produit individuels d'une machine, lancez le programme d'installation, choisissez de modifier le produit et désélectionnez les composants que vous voulez supprimer. Les liens vers les programmes d'installation se trouvent sur la page **Téléchargements** (cliquez sur l'icône de compte dans le coin supérieur droit > **Téléchargements**).

Si vous souhaitez supprimer tous les composants de produit d'une machine, suivez les étapes décrites ci-dessous.

Avertissement !
Pour les déploiements sur site, faites très attention lors de la sélection des composants à désinstaller.

Si vous désinstallez le serveur de gestion par erreur, la console Web Cyber Protect deviendra indisponible et vous ne serez plus en mesure de sauvegarder ni de restaurer les ordinateurs enregistrés sur le serveur de gestion désinstallé.

Sous Windows

1. Connectez-vous en tant qu'administrateur.
2. Accédez au **Panneau de configuration**, puis sélectionnez **Programmes et fonctionnalités** (**Ajout ou suppression de programmes** sous Windows XP) > **Acronis Cyber Protect** > **Désinstaller**.
3. [Facultatif] Cochez la case **Supprimer les journaux et les paramètres de configuration**.
   Ne cochez pas cette case si vous désinstallez un agent et que vous envisagez de le réinstaller ultérieurement. Si vous cochez cette case, il se peut que l'ordinateur soit dupliqué dans la console Web Cyber Protect et que les sauvegardes de l'ancien ordinateur ne soient pas associées au nouveau.
4. Confirmez votre choix.

Sous Linux

1. En tant qu'utilisateur racine, exécutez **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Facultatif] Cochez la case **Nettoyer toutes les traces de produit (supprimer les paramètres de configuration, d'emplacements de stockage, de tâches, de journaux du produit)**.
   Ne cochez pas cette case si vous désinstallez un agent et que vous envisagez de le réinstaller ultérieurement. Si vous cochez cette case, il se peut que l'ordinateur soit dupliqué dans la console Web Cyber Protect et que les sauvegardes de l'ancien ordinateur ne soient pas associées au nouveau.
3. Confirmez votre choix.

Dans macOS

1. Double-cliquez sur le fichier d'installation (.dmg).
2. Patientez pendant 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.

Suppression de l'agent pour VMware (matériel virtuel)

1. Lancez le client vSphere et connectez-vous au vCenter Server.
2. Si l'appliance virtuelle est sous tension, effectuez un clic droit sur celle-ci, puis cliquez sur **Alimentation** > **Mettre hors tension**. Confirmez votre choix.
3. Si l'appliance virtuelle utilise un stockage attaché localement sur un disque virtuel et que vous voulez conserver les données sur ce disque, procédez comme suit :
   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**. Sous **Options de suppression**, cliquez sur **Supprimer de la machine virtuelle**.
   c. 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.

Suppression de machines de la console Web Cyber Protect

Après la désinstallation d'un agent, celui-ci sera désenregistré du serveur de gestion, et l'ordinateur sur lequel l'agent a été installé sera automatiquement supprimé de la console Web Cyber Protect.

Toutefois, si durant l'opération la connexion au serveur de gestion est interrompue, en raison d'un problème réseau par exemple, il est possible que l'agent soit désinstallé, mais que son ordinateur s'affiche toujours dans la console Web. Dans ce cas, vous devez supprimer manuellement l'ordinateur de la console Web.

Pour supprimer manuellement un ordinateur de la console Web

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez l'ordinateur sur lequel l'agent est installé.
3. Cliquez sur **Supprimer**.

Accéder à la console Web Cyber Protect

Pour accéder à la console Web Cyber Protect, saisissez l'adresse de la page de connexion dans la barre d'adresse du navigateur Web, puis connectez-vous comme décrit ci-dessous.

Déploiement sur site

L'adresse de la page de connexion est l'adresse IP ou le nom de la machine sur laquelle le serveur de gestion est installé.

Les protocoles HTTP et HTTPS sont pris en charge sur le même port TCP, qui peut être configuré pendant l'installation du serveur de gestion. Le port par défaut est 9877.

Vous pouvez configurer le serveur de gestion pour empêcher l'accès à la console Web Cyber Protect via HTTP et pour utiliser un certificat SSL tiers.

Sous Windows

Si le serveur de gestion est installé sur Windows, il existe deux façons de se connecter à la console Web Cyber Protect :

- Cliquez sur **Se connecter** pour vous connecter en tant qu'utilisateur Windows actuel.
  Il s'agit de la manière la plus simple de se connecter depuis la machine sur laquelle le serveur de gestion est installé.
  Si le serveur de gestion est installé sur une autre machine, cette méthode fonctionne dans les conditions suivantes :
  - La machine depuis laquelle vous vous connectez se situe dans le même domaine Active Directory que le serveur de gestion.
  - Vous êtes connecté en tant qu'utilisateur de domaine.

  Nous vous recommandons de configurer votre navigateur Web pour l'authentification Windows intégrée. Sinon, le navigateur demandera un nom d'utilisateur et un mot de passe. Toutefois, vous pouvez désactiver cette option.
- Cliquez sur **Entrer le nom d'utilisateur et le mot de passe**, puis spécifiez le nom d'utilisateur et le mot de passe.

Dans tous les cas, votre compte doit figurer dans la liste des administrateurs de serveur de gestion. Par défaut, cette liste contient le groupe **Administrateurs** sur la machine exécutant le serveur de gestion. Pour plus d'informations, consultez la page « Administrateurs et unités ».

Pour désactiver l'option Se connecter en tant qu'utilisateur Windows actuel

1. Sur l'ordinateur sur lequel le serveur de gestion est installé, accédez à `C:\Program Files\Acronis\AccountServer`.
2. Ouvrez le fichier **account_server.json** pour le modifier.
3. Accédez à la section « connectors », puis supprimez les lignes suivantes :

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Naviguez jusqu'à la section « checksum », puis modifiez la valeur de « sum » comme suit :

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. Redémarrez Acronis Service Manager Service, comme décrit dans « Utilisation d'un certificat émis par une autorité de certification approuvée ».

Sous Linux

Si le serveur de gestion est installé sous Linux, indiquez le nom d'utilisateur et le mot de passe d'un compte de la liste des administrateurs de serveur de gestion. Par défaut, cette liste contient seulement l'utilisateur **root** sur la machine exécutant le serveur de gestion. Pour plus d'informations, consultez la page « Administrateurs et unités ».

Déploiement Cloud

L'adresse de la page de connexion est https://backup.acronis.com/. Le nom d'utilisateur et le mot de passe sont ceux de votre compte Acronis.

Si votre compte a été créé par l'administrateur de sauvegarde, vous devez activer le compte et définir le mot de passe en cliquant sur le lien inclus dans votre e-mail d'activation.

Changement de la langue

Lorsque vous êtes connecté, vous pouvez modifier la langue de l'interface Web en cliquant sur l'icône du compte dans le coin supérieur droit.

Configuration d'un navigateur Web pour l'authentification Windows intégrée

L'authentification Windows intégrée est possible si vous accédez à la console Web Cyber Protect depuis un ordinateur exécutant Windows et n'importe quel navigateur pris en charge.

Nous vous recommandons de configurer votre navigateur Web pour l'authentification Windows intégrée. Sinon, il demandera un nom d'utilisateur et un mot de passe.

Configuration d'Internet Explorer, Microsoft Edge, Opera et Google Chrome

Si la machine où s'exécute le navigateur est dans le même domaine Active Directory que celle exécutant le serveur de gestion, ajoutez la page de connexion de la console à la liste de sites **intranet locaux**.

Sinon, ajoutez la page de connexion de la console à la liste des **sites de confiance** et activez le paramètre **Connexion automatique avec le nom d'utilisateur et le mot de passe actuel**.

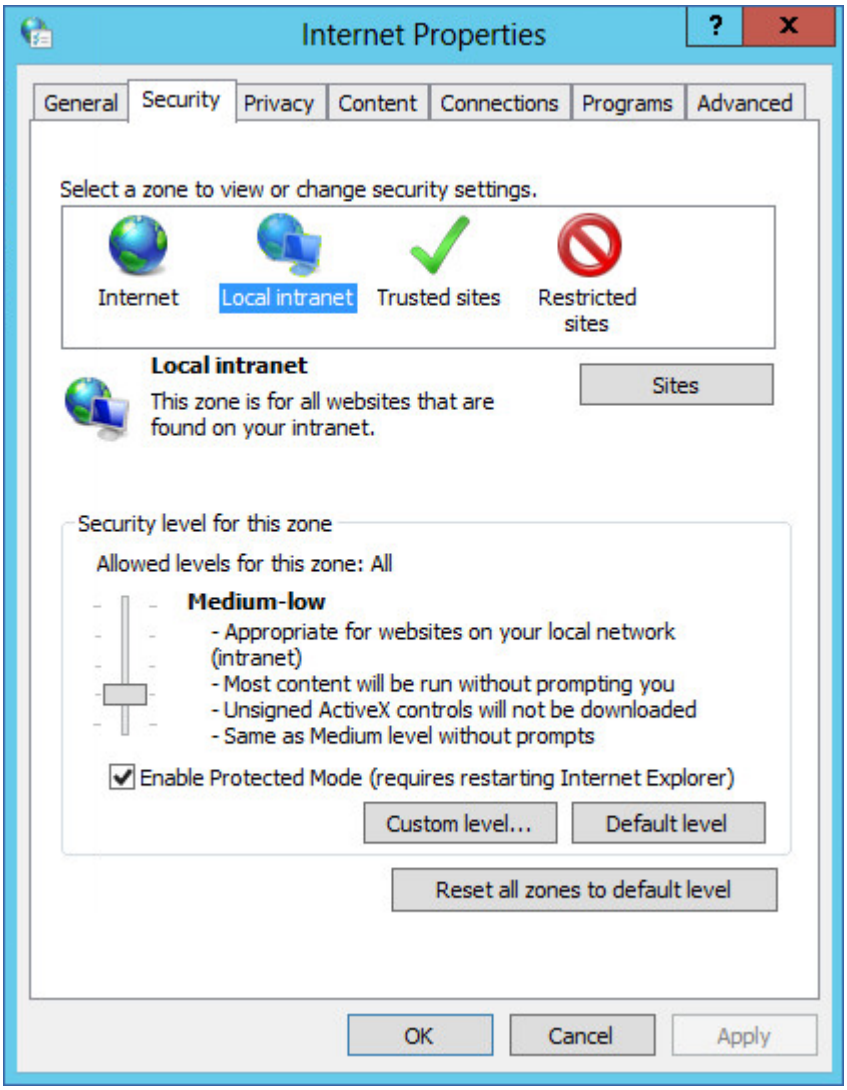
Des instructions étape par étape sont fournies plus loin dans cette section. Ces navigateurs utilisant les paramètres de Windows, il est également possible de les configurer avec des stratégies de groupe dans un domaine Active Directory.

Configuration de Mozilla Firefox

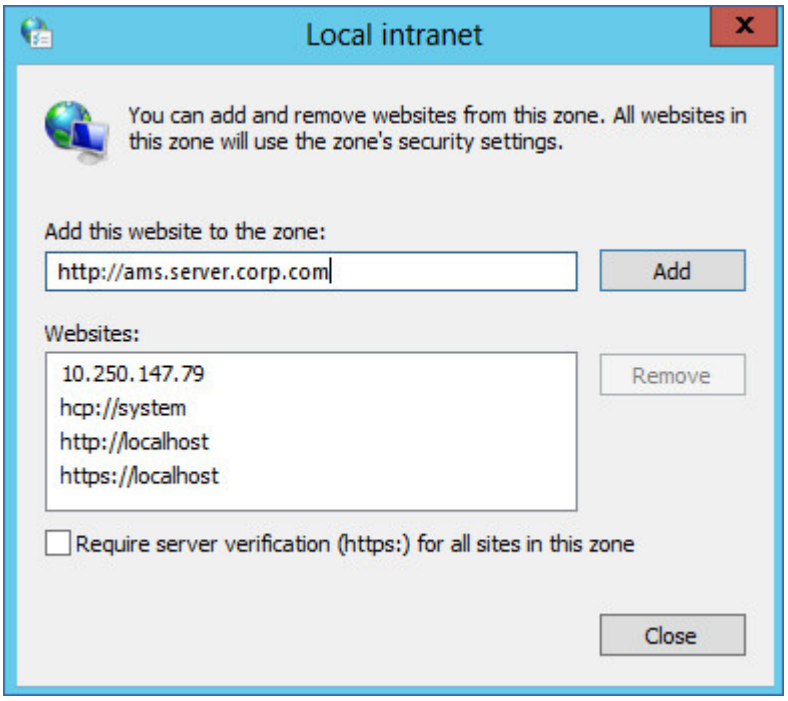
1. Dans Firefox, atteignez l'URL `about:config`, puis cliquez sur le bouton **J'accepte le risque**.
2. Dans le champ de **recherche**, cherchez la préférence `network.negotiate-auth.trusted-uris`.
3. Double-cliquez dessus, puis saisissez l'adresse de la page de connexion de la console Web Cyber Protect.
4. Répétez les étapes 2 et 3 pour la préférence `network.automatic-ntlm-auth.trusted-uris`.
5. Fermez la fenêtre `about:config`.

Ajout de la console à la liste des sites intranet locaux

1. Allez dans **Panneau de configuration** > **Options Internet**.
2. Dans l'onglet **Sécurité**, sélectionnez **Intranet local**.



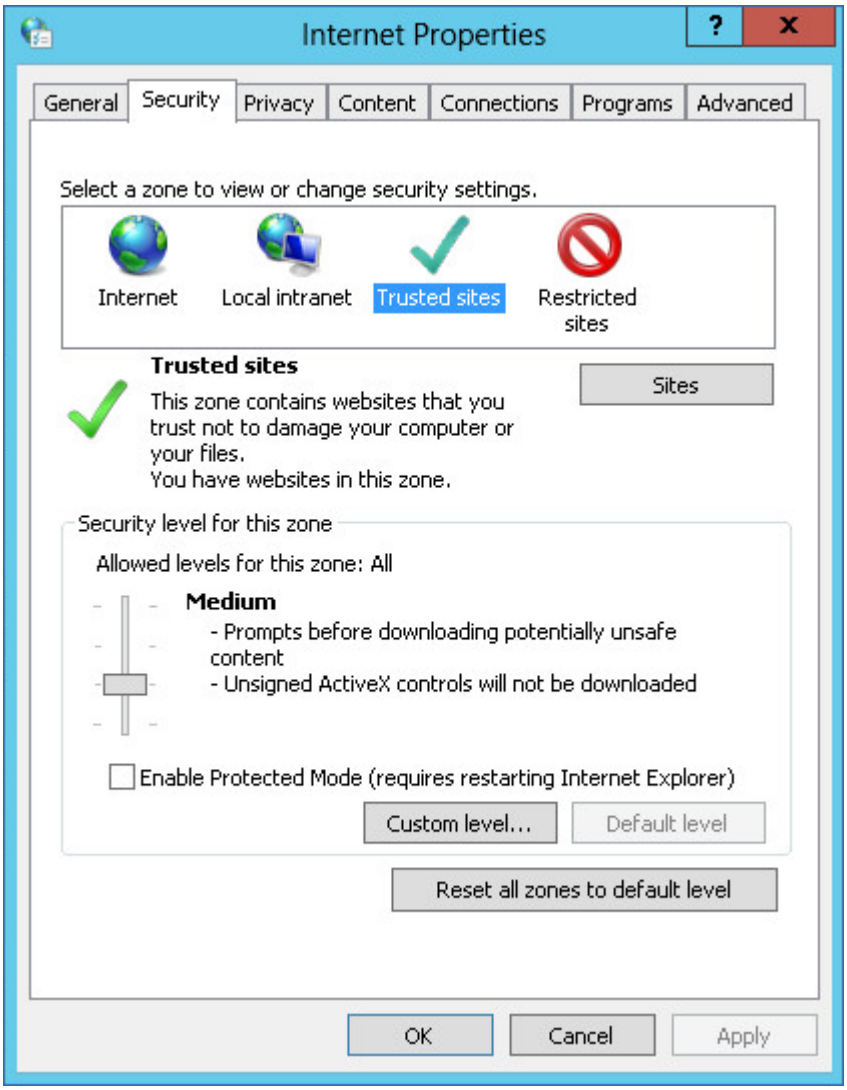
3. Cliquez sur **Sites**.
4. Dans **Ajouter ce site Web à la zone**, saisissez l'adresse de la page de connexion de la console Web Cyber Protect, puis cliquez sur **Ajouter**.



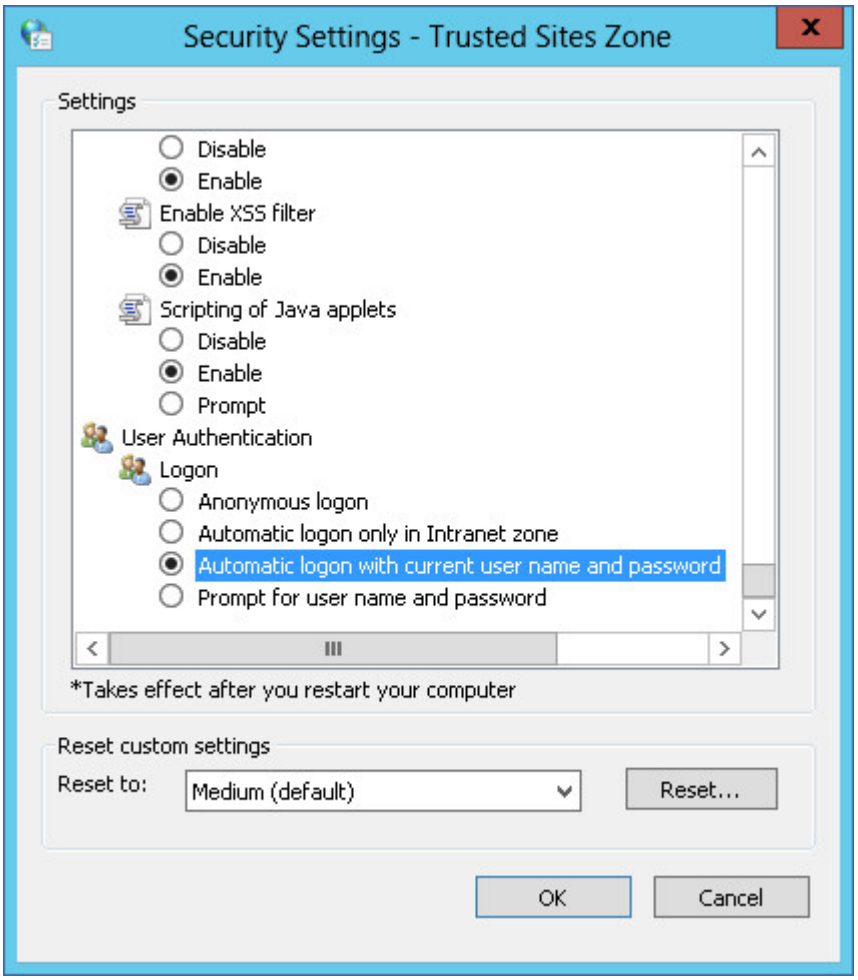
5. Cliquez sur **Fermer**.
6. Cliquez sur **OK**.

Ajout de la console à la liste des sites de confiance

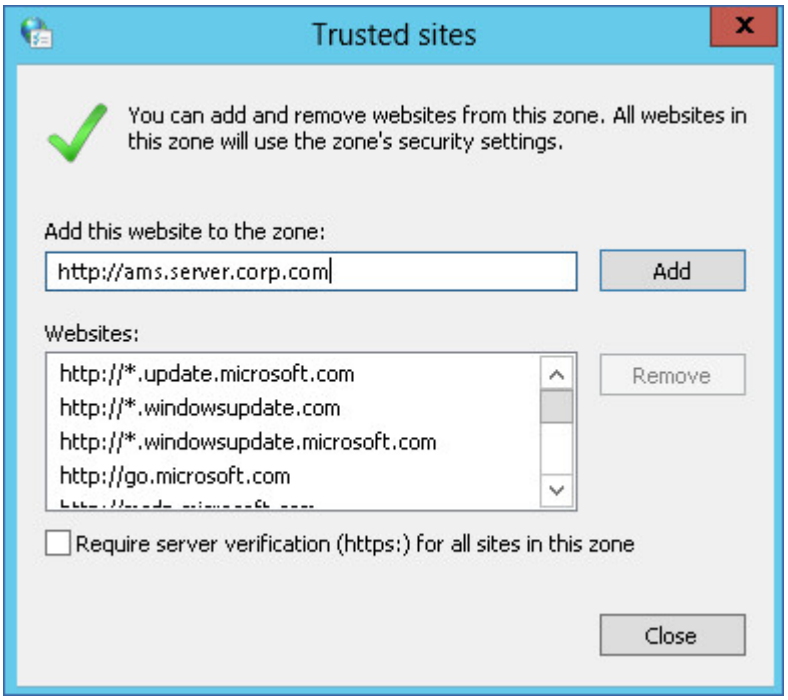
1. Allez dans **Panneau de configuration** > **Options Internet**.
2. Dans l'onglet **Sécurité**, sélectionnez **Sites de confiance**, puis cliquez sur **Niveau personnalisé**.



3. Dans **Connexion**, sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuels**, puis cliquez sur **OK**.



4. Dans l'onglet **Sécurité**, avec **Sites de confiance** toujours sélectionné, cliquez sur **Sites**.
5. Dans **Ajouter ce site Web à la zone**, saisissez l'adresse de la page de connexion de la console Web Cyber Protect, puis cliquez sur **Ajouter**.



6. Cliquez sur **Fermer**.
7. Cliquez sur **OK**.

Autoriser uniquement les connexions HTTPS à la console Web

Par mesure de sécurité, vous pouvez empêcher les utilisateurs d'accéder à la console Web Cyber Protect via le protocole HTTP, et autoriser uniquement les connexions HTTPS.

Pour autoriser uniquement les connexions HTTPS à la console Web

1. Sur la machine exécutant le serveur de gestion, ouvrez le fichier de configuration suivant avec un éditeur de texte :
   - Sous Windows : `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Sous Linux : `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. Localisez la section suivante :

   ```
   "tls": {
     "auto_redirect" : false,
     "cert_file": "cert.pem",
   ```

3. Modifiez la valeur `"auto_redirect" false` en `true`.
   Si la ligne `"auto_redirect"` est manquante, ajoutez-la manuellement :

   ```
   "auto_redirect": true,
   ```

4. Sauvegardez le fichier `api_gateway.json`.

Important
Veillez à ne pas supprimer par accident des virgules, parenthèses et guillemets dans le fichier de configuration.

5. Redémarrez Acronis Service Manager Service comme décrit ci-dessous.

Pour redémarrer Acronis Service Manager Service sous Windows

Sous Windows

1. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis entrez : **cmd**.
2. Cliquez sur **OK**.
3. Exécutez les commandes suivantes :

```
net stop asm
net start asm
```

Sous Linux

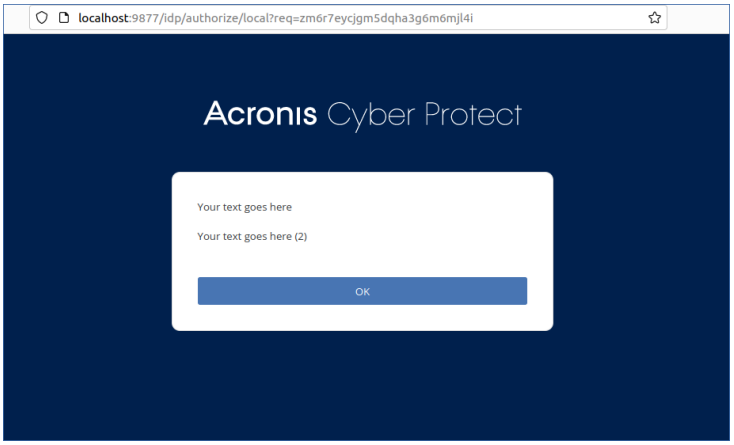
1. Ouvrir l'application **Terminal**.
2. Exécuter la commande suivante dans n'importe quel répertoire :

```
sudo service acronis_asm restart
```

Ajout d'un message personnalisé à la console Web

Vous pouvez ajouter un message personnalisé à la console Web Cyber Protect.

Ce message s'affiche avant chaque tentative de connexion.



Prérequis

Si des plans de protection sont appliqués à l'ordinateur sur lequel s'exécute le serveur de gestion, vérifiez que la fonctionnalité d'autoprotection est désactivée. Sinon, vous ne pourrez pas modifier le

fichier de configuration.

Pour plus d'informations sur la désactivation ou l'activation de la fonctionnalité d'autoprotection, consultez "Autoprotection" (p. 529).

Pour ajouter un message personnalisé à la console Web

Sous Windows

1. Connectez-vous à l'ordinateur sur lequel le serveur de gestion est installé. Votre compte doit disposer des droits d'administrateur.
2. Accédez à `%Program Files%\Acronis\AccountServer`.
3. [Facultatif] Créez une copie de sauvegarde du fichier `AccountServer.zip`.
4. Accédez à `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
5. Extrayez le fichier JSON correspondant à la langue que vous utilisez dans la console Web Cyber Protect. Par exemple, si vous utilisez l'anglais, extrayez le fichier `en.json`.

   Remarque
   Pour pouvoir modifier le fichier, vous devez l'extraire, pas seulement l'ouvrir en double cliquant dessus.

6. Ouvrez le fichier extrait pour le modifier. Vous pouvez utiliser un éditeur de texte tel que le Bloc-notes ou Notepad++.
7. Accédez à la ligne suivante, puis ajoutez une virgule à la fin :

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

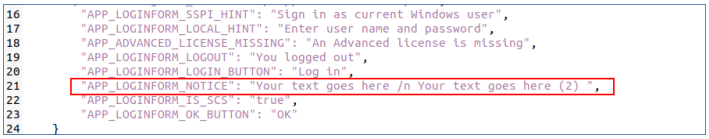
8. Sous la ligne `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"`, ajoutez les lignes suivantes :

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

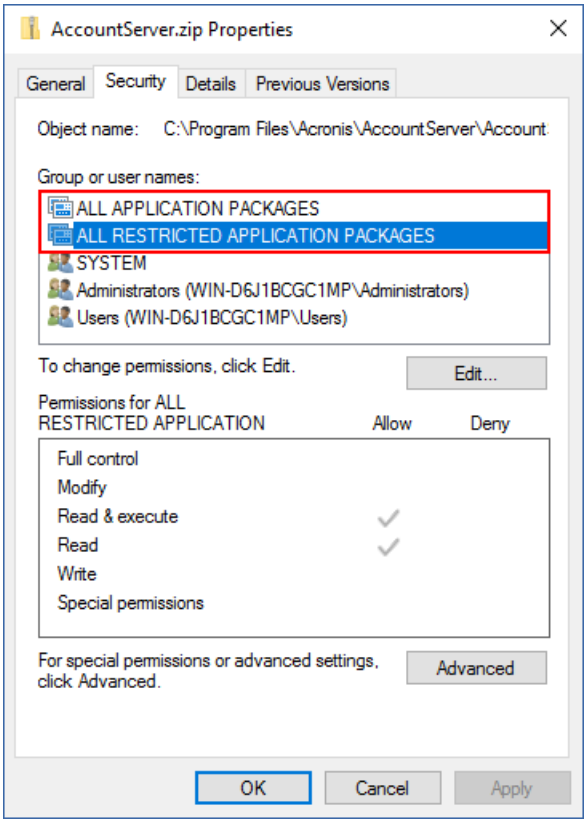
   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   Par exemple :

9. Enregistrez les modifications, puis replacez le fichier JSON modifié dans le dossier `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
10. Cliquez avec le bouton droit sur le fichier `AccountServer.zip`, puis accédez à **Propriétés** > **Sécurité** pour vérifier que les clés `ALL APPLICATION PACKAGES` et `ALL RESTRICTED APPLICATION PACKAGES` sont ajoutées sous **Noms de groupes ou d'utilisateurs**

avec les droits **Lire** et **Lire et exécuter**.



Remarque
Si la clé `ALL RESTRICTED APPLICATION PACKAGES` est manquante, supprimez `ALL APPLICATION PACKAGES` de cette liste, puis rajoutez-la. `ALL RESTRICTED APPLICATION PACKAGES` apparaît automatiquement lorsque vous ajoutez `ALL APPLICATION PACKAGES`.

11. Redémarrez le service **Acronis Service Manager** comme décrit dans "Pour redémarrer le service Acronis Service Manager" (p. 204).

Sous Linux

1. Connectez-vous à l'ordinateur sur lequel le serveur de gestion est installé.
2. Accédez à `/usr/lib/Acronis/AccountServer`.
3. Vérifiez que vous disposez des autorisations d'écriture pour le fichier `AccountServer.zip`.
4. [Facultatif] Créez une copie de sauvegarde du fichier `AccountServer.zip`.
5. Accédez à `/usr/lib/Acronis/AccountServer/static/locale`.
6. Extrayez le fichier JSON correspondant à la langue que vous utilisez dans la console Web Cyber Protect. Par exemple, si vous utilisez l'anglais, extrayez le fichier `en.json`.
7. Ouvrez le fichier extrait pour le modifier.
8. Accédez à la ligne suivante, puis ajoutez une virgule à la fin :

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

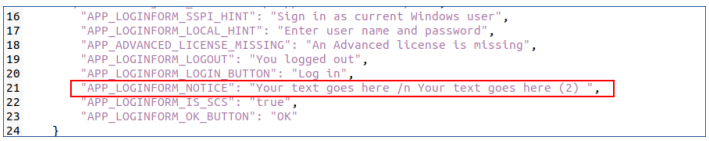
9. Sous la ligne `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"`, ajoutez les lignes suivantes :

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

Par exemple :



10. Enregistrez les modifications, puis replacez le fichier JSON modifié dans le dossier `/usr/lib/Acronis/AccountServer/static/locale`.
11. Redémarrez le service **Acronis Service Manager** comme décrit dans "Pour redémarrer le service Acronis Service Manager" (p. 204).

Paramètres de certificat SSL

Cette section décrit comment effectuer les tâches suivantes :

- Configurer un agent de protection utilisant un certificat SSL (Secure Socket Layer) auto-signé généré par le serveur de gestion.
- Remplacer le certificat SSL auto-signé généré par le serveur de gestion par un certificat émis par une autorité de certification approuvée, telle que GoDaddy, Comodo ou GlobalSign. Si vous faites cette modification, le certificat utilisé par le serveur de gestion sera approuvé sur toutes les machines. L'alerte de sécurité de votre navigateur n'apparaîtra pas quand vous vous connecterez à la console Web Cyber Protect via le protocole HTTPS.

Vous pouvez également configurer le serveur de gestion pour empêcher l'accès à la console Web Cyber Protect via HTTP en redirigeant tous les utilisateurs vers la version HTTPS.

Utilisation d'un certificat auto-signé

Pour configurer un agent de protection sous Windows

1. Sur la machine sur laquelle l'agent est installé, ouvrez l'éditeur du registre.
2. Localisez la clé de registre suivante : **HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. Définissez la valeur de **VerifyPeer** sur **0**.
4. Vérifiez que la valeur **VerifyHost** est définie **0**.
5. Redémarrer le service de machine gérée (MMS) :

a. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis tapez : **cmd**.

b. Cliquez sur **OK**.

c. Exécutez les commandes suivantes :

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

Pour configurer un agent de protection sous Linux

1. Sur la machine sur laquelle l'agent est installé, ouvrez le fichier **/etc/Acronis/BackupAndRecovery.config** pour le modifier**.**
2. Accédez à la clé **CurlOptions**, puis définissez la valeur de **VerifyPeer** sur **0**. Vérifiez que la valeur de **VerifyHost** est également définie sur **0**.
3. Enregistrez vos modifications.
4. Redémarrez le service de machine gérée (MMS) en exécutant la commande suivante dans n'importe quel répertoire :

```
sudo service acronis_mms restart
```

Pour configurer un agent de protection sous macOS

1. Sur la machine sur laquelle l'agent est installé, arrêtez le service de machine gérée (MMS) :
   a. Rendez-vous dans **Applications** > **Utilitaires** > **Terminal**
   b. Exécuter la commande suivante :

```
sudo launchctl stop acronis_mms
```

2. Ouvrez le fichier **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** pour le modifier.
3. Accédez à la clé **CurlOptions**, puis définissez la valeur de **VerifyPeer** sur **0**. Vérifiez que la valeur de **VerifyHost** est également définie sur **0**.
4. Enregistrez vos modifications.
5. Démarrer le service de machine gérée (MMS) en exécutant la commande suivante dans Terminal :

```
sudo launchctl starts acronis_mms
```

Utilisation d'un certificat émis par une autorité de certification approuvée

Pour configurer les paramètres du certificat SSL

1. Assurez-vous que vous disposez de tous les éléments suivants :

Si vous utilisez des fichiers de certificat et de clé	Si vous utilisez un fichier PFX
Le fichier de certificat (au format .pem)	Le fichier PFX
Le fichier avec la clé privée pour le certificat (en général au format .key)	
Le mot de passe de la clé privée (si la clé est protégée par un mot de passe)	Le mot de passe pour un fichier PFX, si le fichier est protégé par un mot de passe

2. Copiez les fichiers sur la machine exécutant le serveur de gestion.
3. Sur cette machine, ouvrez le fichier de configuration suivant avec un éditeur de texte :
   - Sous Windows : `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Sous Linux : `/var/lib/Acronis/ApiGateway/api_gateway.json`
4. Localisez la section suivante :

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. Spécifiez le chemin d'accès complet au fichier du certificat ou au fichier PFX entre les guillemets à la ligne `"cert_file"`.

   Par exemple :

Système d'exploitation	Si vous utilisez une paire de certificat et de clé	Si vous utilisez un fichier .pfx
Windows (attention aux barres obliques inversées)	`"cert_file": "C:/certificate/local-domain.ams.pem"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"cert_file": "/home/user/local-domain.ams.pem"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

6. Spécifiez le chemin d'accès complet au fichier de clé privée ou au fichier PFX qui contient la clé du certificat entre les guillemets à la ligne `"key_file"`.

   Un fichier PFX inclut habituellement aussi bien le certificat que sa clé. Dans ce cas, à la ligne `"key_file"`, spécifiez le même chemin d'accès qu'à l'étape précédente.

   Par exemple :

Système d'exploitation	Si vous utilisez une paire de certificat et de clé	Si vous utilisez un fichier .pfx
Windows (attention aux barres obliques inversées)	`"key_file": "C:/certificate/private.key"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"key_file": "/home/user/private.key"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

7. [Facultatif] Spécifiez le mot de passe entre les guillemets à la ligne `"passphrase"` si la clé privée ou le fichier PFX est protégé par un mot de passe.

   Par exemple : `"passphrase": "my password"`

   Remarque

   Si la ligne `"passphrase": ""`, est manquante dans votre fichier de configuration `api_gateway.json`, ajoutez-la manuellement.

   Par exemple :

   ```
   "tls": {
       "cert_file": "cert.pem",
       "key_file": "key.pem",
       "passphrase": "my password",
   }
   ```

8. Sauvegardez le fichier `api_gateway.json`.

   Important

   Veillez à ne pas supprimer par accident des virgules, parenthèses et guillemets dans le fichier de configuration.

9. Redémarrez Acronis Service Manager Service comme décrit ci-dessous.

Pour redémarrer le service Acronis Service Manager

Sous Windows

1. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis entrez : **cmd**.
2. Cliquez sur **OK**.
3. Exécutez les commandes suivantes :

   ```
   net stop asm
   net start asm
   ```

Sous Linux

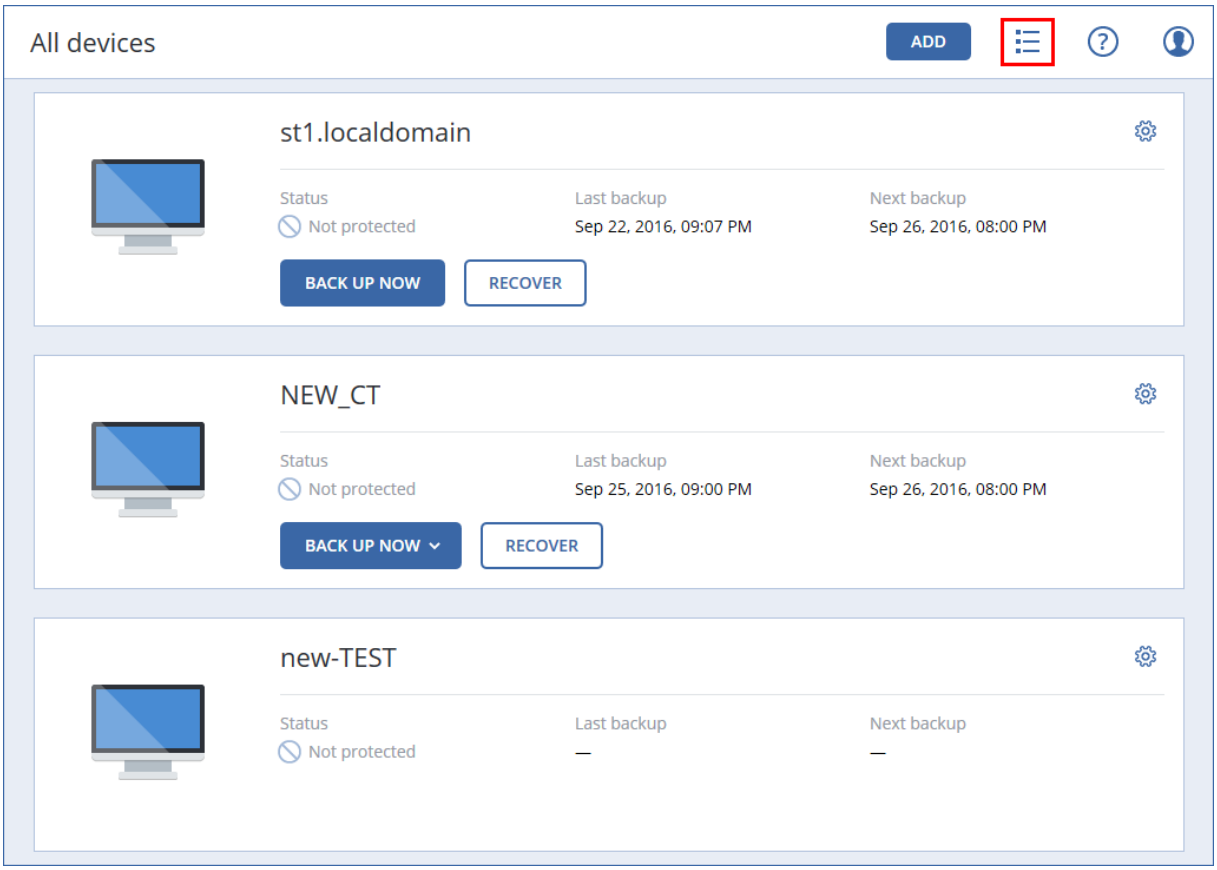
1. Ouvrir l'application **Terminal**.
2. Exécuter la commande suivante dans n'importe quel répertoire :

```
sudo service acronis_asm restart
```

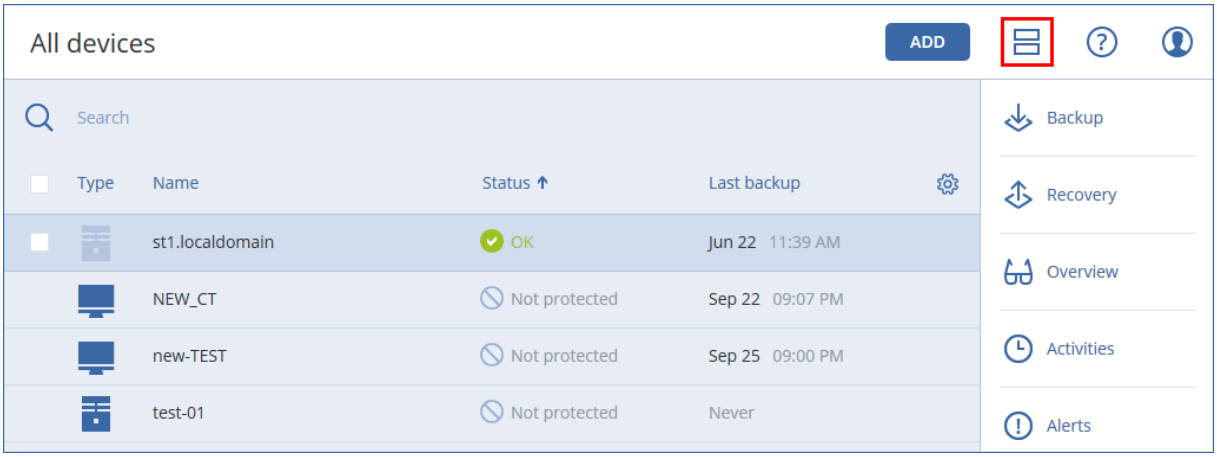
Affichage de la console Web Cyber Protect

La console Web Cyber Protect possède deux modes d'affichage différents : un mode d'affichage simple et un mode d'affichage tableau. Afin de passer d'un mode d'affichage à l'autre, cliquez sur l'icône correspondante dans l'angle supérieur droit.

Le mode d'affichage simple prend en charge un petit nombre de machines.



L'e mode d'affichage tableau est activé automatiquement lorsque le nombre de machines est 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 machine passe en ligne ou hors ligne, un certain temps est nécessaire avant que son état soit modifié dans la console Web Cyber Protect.

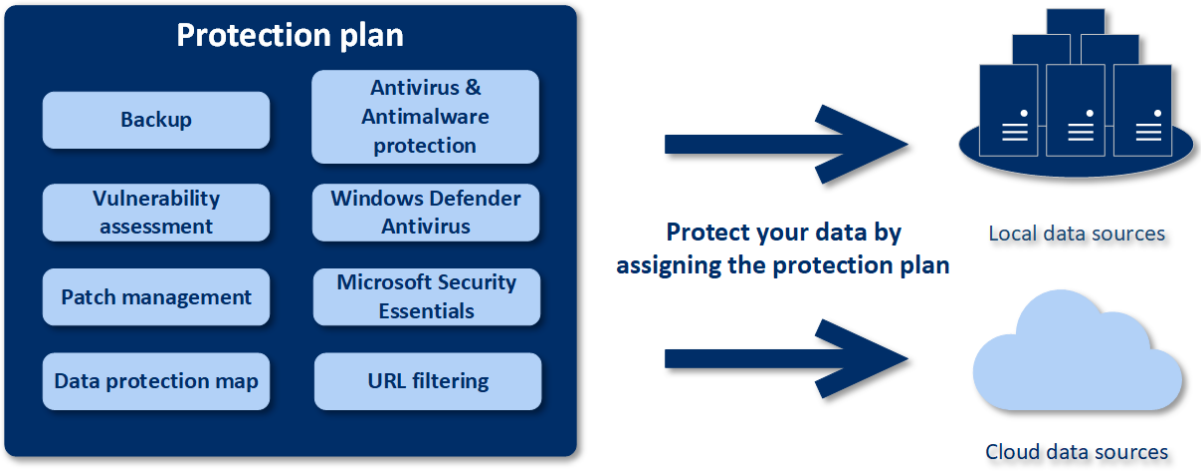
L'état des machines est vérifié toutes les minutes. Si l'agent installé sur cette machine n'est pas en train de transférer des données, et que cinq vérifications consécutives ne donnent aucun résultat, la machine s'affiche comme hors ligne. La machine s'affiche à nouveau comme en ligne lorsqu'elle répond à une vérification d'état ou commence à transférer des données.

Plan et modules de protection

Le plan de protection est un plan qui combine plusieurs modules de protection des données, notamment les suivants :

- Sauvegarde : vous permet de sauvegarder vos sources de données vers un stockage local ou dans le Cloud.
- Protection contre les virus et les malwares : vous permet de vérifier vos ordinateurs grâce à la solution antimalware intégrée.
- Filtrage d'URL : vous permet de protéger vos machines des menaces provenant d'Internet en bloquant l'accès aux URL et contenus téléchargeables malveillants.
- Antivirus Windows Defender : vous permet de gérer les paramètres de l'antivirus Windows Defender afin de protéger votre environnement.
- Microsoft Security Essentials : vous permet de gérer les paramètres de Microsoft Security Essentials afin de protéger votre environnement.
- Évaluation des vulnérabilités – vérifie automatiquement la présence de vulnérabilités dans les produits Microsoft et tiers installés sur vos machines, et vous prévient le cas échéant.
- Gestion des correctifs : vous permet d'installer des correctifs et des mises à jour pour les produits Microsoft et tiers sur vos machines afin de corriger les vulnérabilités identifiées.
- Carte de la protection des données : vous permet de découvrir les données afin de suivre l'état de protection des fichiers importants.

Le plan de protection vous permet de protéger totalement vos sources de données contre les menaces internes et externes. En activant et désactivant différents modules et en configurant leurs paramètres, vous pouvez élaborer des plans flexibles permettant de répondre aux différents besoins de votre entreprise.



Création d'un plan de protection

Un plan de protection peut être appliqué à plusieurs machines, soit au moment de sa création, soit plus tard. Lorsque vous créez un plan, le système vérifie le système d'exploitation et le type de

périphérique (par exemple, poste de travail, machine virtuelle, etc.) et affiche uniquement les modules de plan applicables à vos périphériques.

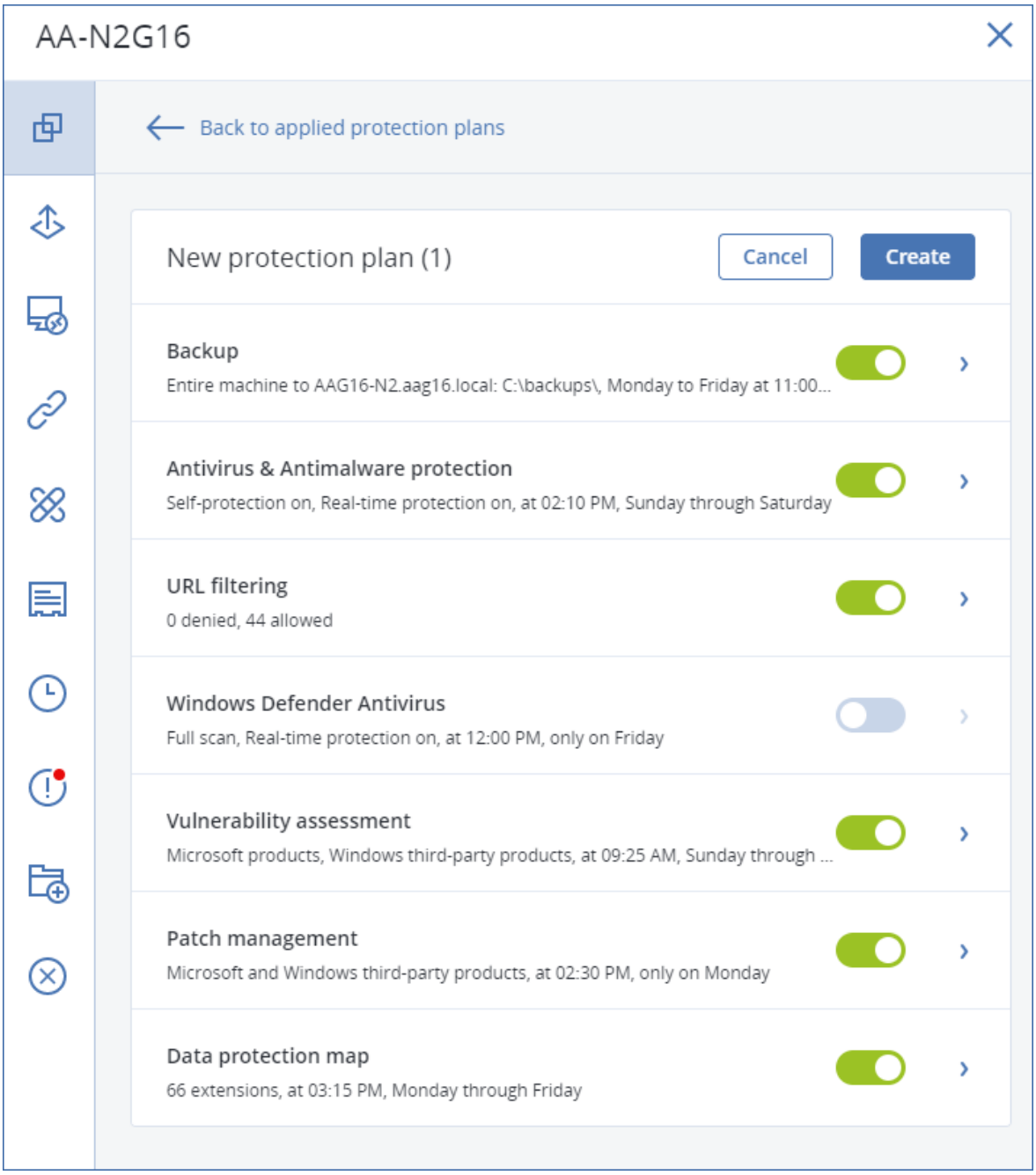
Un plan de protection peut être créé de deux manières différentes :

- Dans la section **Périphériques** : vous sélectionnez le ou les appareils à protéger, puis créez un plan pour eux.
- Dans la section **Plans** : vous créez un plan, puis sélectionnez les machines auxquelles l'appliquer.

Choisissons la première possibilité.

Créer votre premier plan de protection

1. Dans la console Web 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**. Le plan de protection s'affichera, avec ses paramètres par défaut.



4. [Facultatif] Pour modifier le nom du plan de protection, cliquez sur l'icône en forme de crayon à côté de son nom.
5. [Facultatif] Pour activer ou désactiver un module de plan de protection, cliquez sur l'interrupteur à côté du nom du module.
6. [Facultatif] Pour configurer les paramètres du module de sauvegarde, cliquez sur la section correspondante du plan de protection.
7. Lorsque vous avez terminé, cliquez sur **Créer**.

Les modules Sauvegarde, Protection contre les virus et les malwares, Évaluation des vulnérabilités, Gestion des correctifs et Carte de la protection des données peuvent être exécutés à la demande, en cliquant sur **Exécuter maintenant**.

Résolution des conflits de plan

Un plan de protection peut avoir les états suivants :

- **Actif :** un plan est attribué à des appareils et exécuté sur ces derniers.
- **Inactif** : un plan est attribué à des appareils, mais il est désactivé et non exécuté sur ces derniers.

Application de plusieurs plans à un appareil

Vous pouvez appliquer plusieurs plans de protection à un seul appareil. Vous obtiendrez alors une combinaison de différents plans de protection attribués à un seul appareil. Par exemple, vous pouvez appliquer un plan pour lequel seul le module Protection contre les virus et les malwares est activé, et un autre pour lequel seul le module Sauvegarde est activé. Les plans de protection peuvent être combinés uniquement s'ils n'ont pas de modules en commun. Si les mêmes modules sont activés dans plusieurs plans de protection, vous devez résoudre les conflits qui existent entre eux.

Résolution des conflits de plan

Conflits de plans avec des plans déjà appliqués

Lorsque vous créez un nouveau plan sur un ou plusieurs périphériques qui présentent des plans qui entrent en conflit avec le nouveau plan, vous devez résoudre le conflit de l'une des manières suivantes :

- Créez un nouveau plan, appliquez-le, puis désactivez tous les plans qui ont déjà été appliqués et qui sont en conflit.
- Créez un nouveau plan, puis désactivez-le.

Lorsque vous modifiez un plan sur un ou plusieurs périphériques qui présentent des plans qui entrent en conflit avec la modification appliquée, vous devez résoudre le conflit de l'une des manières suivantes :

- Enregistrez les modifications appliquées au plan, puis désactivez tous les plans en conflit déjà appliqués.
- Enregistrez les modifications appliquées au plan, puis désactivez-le.

Plan de périphérique en conflit avec un plan de groupe

Si le périphérique fait partie d'un groupe de périphériques auquel un plan de groupe est attribué et que vous essayez d'attribuer un nouveau plan au périphérique, le système vous demandera de résoudre le conflit de l'une des manières suivantes :

- Supprimez un périphérique du groupe, puis appliquez un nouveau plan au périphérique.
- Appliquez un nouveau plan au groupe tout entier, ou modifiez le plan de groupe actuel.

Problème de licence

Le quota attribué à un périphérique doit être suffisant pour que le plan de protection puisse être exécuté, mis à jour ou appliqué. Pour résoudre le problème de licence, effectuez l'une des actions suivantes :

- Désactivez les modules non pris en charge par le quota attribué et continuez à utiliser le plan de protection.
- Modifiez manuellement le quota attribué : accédez à **Périphériques** > **<périphérique particulier>** > **Détails** > **Quota de service**. Retirez ensuite le quota existant et attribuez-en un autre.

Opérations avec les plans de protection

Pour en savoir plus sur la création d'un plan de protection, consultez la section Création d'un plan de protection.

Actions disponibles avec un plan de protection

Vous pouvez exécuter les opérations suivantes avec un plan de protection :

- Renommer le plan
- Activer/désactiver des modules et modifiez les paramètres de chaque module
- Activer/désactiver un plan

  Un plan désactivé ne sera pas exécuté sur le périphérique sur lequel il est appliqué.

  Cette action est utile pour les administrateurs qui prévoient de protéger le même périphérique avec le même plan plus tard. Le plan n'est pas révoqué du terminal et, pour restaurer la protection, l'administrateur doit seulement réactiver le plan.
- Attribuer un plan à des terminaux ou à des groupes de terminaux
- Révoquer un plan d'un terminal

  Un plan révoqué n'est plus appliqué à un périphérique.

  Cette action est utile pour les administrateurs qui n'ont pas besoin de protéger rapidement le même périphérique avec le même plan. Pour restaurer la protection d'un plan révoqué, l'administrateur doit connaître le nom de ce plan, le sélectionner dans la liste des plans disponibles et le réappliquer au terminal souhaité.
- Importer/exporter un plan

  Remarque
  Vous ne pouvez importer que les plans de protection créés dans Acronis Cyber Protect 15. Les plans de protection créés dans les versions antérieures sont incompatibles avec Acronis Cyber Protect 15.

- Supprimer un plan

Appliquer un plan de protection existant

1. Sélectionnez les machines que vous souhaitez protéger.
2. Cliquez sur **Protection**. Si un plan de protection est déjà appliqué aux machines sélectionnées, cliquez sur **Ajouter un plan**.
3. Le logiciel affiche les plans de protection existants.
4. Sélectionnez la protection nécessaire, puis cliquez sur **Appliquer**.

Modifier un plan de protection

1. Si vous souhaitez modifier le plan de protection de toutes les machines auxquelles il est appliqué, sélectionnez l'une d'entre elles. Sinon, sélectionnez les machines pour lesquelles vous souhaitez modifier le plan de protection.
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 de protection, puis cliquez sur **Modifier**.
5. Pour modifier les paramètres du plan, cliquez sur la section correspondante dans le volet du plan de protection.
6. Cliquez sur **Enregistrer les modifications**.
7. Pour modifier le plan de protection pour toutes les machines auxquelles il est appliqué, cliquez sur **Appliquer les modifications à ce plan de protection**. Sinon, cliquez sur **Créer un plan de protection pour les périphériques sélectionnés uniquement**.

Pour retirer un plan de protection de plusieurs machines

1. Sélectionnez les machines desquelles vous voulez retirer le plan de protection.
2. Cliquez sur **Protection**.
3. Si plusieurs plans de protection sont appliqués aux machines, sélectionnez le plan de protection que vous souhaitez retirer.
4. Cliquez sur l'icône en forme de points de suspension située à côté du nom du plan de protection, puis cliquez sur **Retirer**.

Supprimer un plan de protection

1. Sélectionnez n'importe quelle machine à laquelle le plan de protection que vous voulez supprimer est appliqué.
2. Cliquez sur **Protection**.
3. Si plusieurs plans de protection sont appliqués à la machine, sélectionnez le plan de protection que vous souhaitez retirer.
4. Cliquez sur l'icône en forme de points de suspension située à côté du nom du plan de protection, puis cliquez sur **Supprimer**.

   Le plan de protection est alors retiré de toutes les machines et est totalement supprimé de l'interface Web.

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.

Remarque
Pour les déploiements sur site, si le serveur de gestion ne répertorie que les licences standard, il est impossible d'appliquer un plan de protection à plusieurs machines physiques. Chaque machine physique doit disposer de son propre plan de protection.

Créer votre premier plan de protection avec module de sauvegarde activé

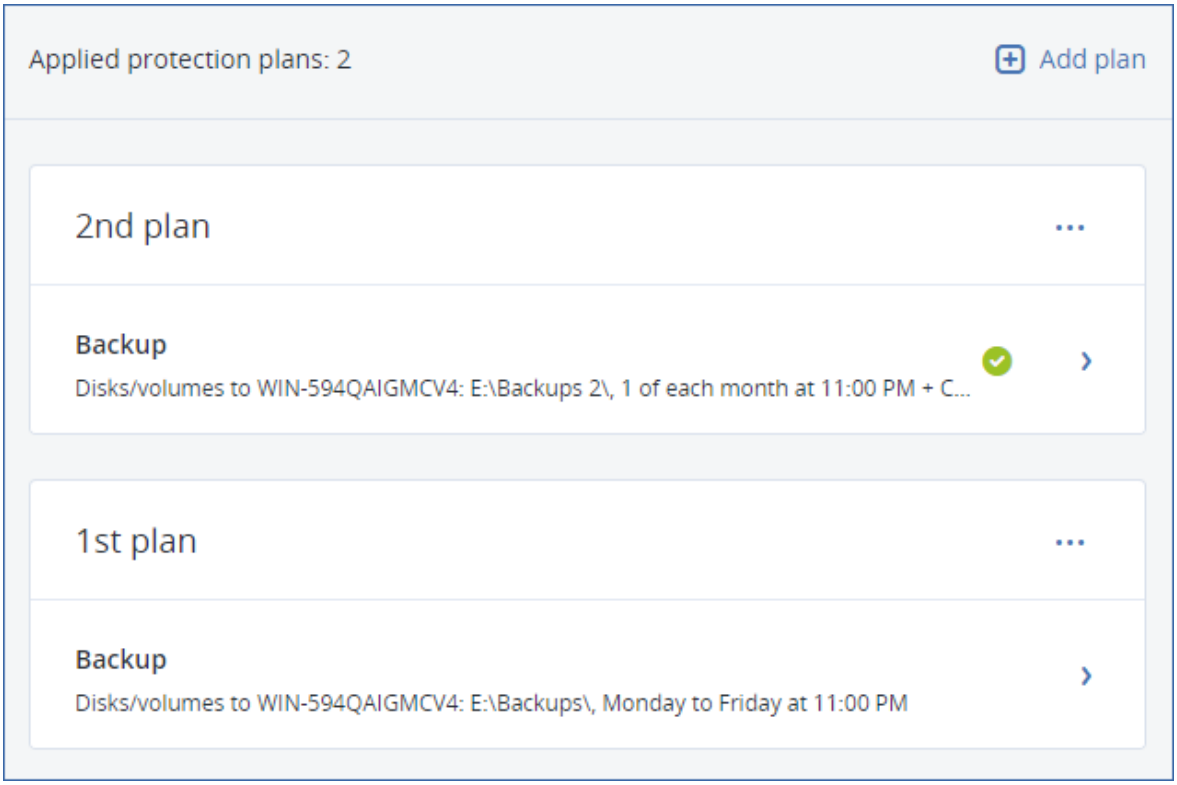
1. Sélectionnez les machines que vous voulez sauvegarder.
2. Cliquez sur **Protection**.
   Le logiciel affiche les plans de protection appliqués à la machine. Si aucun plan n'est encore appliqué à la machine, vous verrez le plan de protection par défaut qui peut être appliqué. Vous

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

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 le module de sauvegarde

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

Le tableau suivant récapitule les paramètres du module de sauvegarde disponibles. Aidez-vous du tableau pour créer le plan de protection qui correspond au mieux à vos besoins.

QUOI SAUVEGARDER	ÉLÉMENTS A SAUVEGARDER Méthodes de sélection	OÙ SAUVEGARDER	PLANIFICATION Modèles de sauvegarde (non adapté au	DURÉE DE CONSERVATION

			Cloud)	
Disques/volumes (machines physiques)	Sélection directe Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau Serveur SFTP* NFS* Secure Zone* Emplacement géré* Périphérique à bandes*	Toujours incrémentielle (fichier unique)* Toujours complète Complète hebdo., incrémentielle journ. Complète mens., différentielle hebdo., incrémentielle journ. (GFS) Personnalisée (C-D-I)	Par âge des sauvegardes (règle unique/par lot de sauvegarde) Par nombre de sauvegardes Par volume total de sauvegardes* Conserver indéfiniment
Disques/volumes (machines virtuelles)	Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau Serveur SFTP* NFS* Emplacement géré* Périphérique à bandes*		
Fichiers (machines physiques uniquement)	Sélection directe Règles de stratégie Filtres de fichiers	Cloud Dossier local Dossier réseau Serveur SFTP* NFS* Secure Zone* Emplacement géré* Périphérique à bandes	Toujours complète Complète hebdo., incrémentielle journ. Complète mens., différentielle hebdo., incrémentielle journ. (GFS) Toujours incrémentielle (fichier unique)* Personnalisée (C-D-I)	
Configuration ESXi	Sélection directe	Dossier local Dossier réseau Serveur SFTP NFS*		

<table>
<tr><td>État du système (déploiements Cloud uniquement)</td><td>Sélection directe</td><td>Cloud
Dossier local
Dossier réseau</td><td rowspan="3">Toujours complète
Sauvegarde complète hebdomadaire, incrémentielle quotidienne
Personnalisée (C-I)</td><td rowspan="4"></td></tr>
<tr><td>Bases de données SQL</td><td>Sélection directe</td><td rowspan="2">Cloud
Dossier local
Dossier réseau
Emplacement géré*
Périphérique à bandes</td></tr>
<tr><td>Bases de données Exchange</td><td>Sélection directe</td></tr>
<tr><td>Boîtes aux lettres Exchange</td><td>Sélection directe</td><td rowspan="2">Cloud
Dossier local
Dossier réseau
Emplacement géré*</td><td rowspan="2">Toujours incrémentielle (fichier unique)</td></tr>
<tr><td>Boîtes aux lettres Microsoft 365</td><td>Sélection directe</td><td>Par âge des sauvegardes (règle unique/par lot de sauvegarde)
Par nombre de sauvegardes
Conserver indéfiniment</td></tr>
</table>

* Voir les limites ci-dessous.

Limites

Serveur SFTP et périphérique à bandes

- Ces emplacements ne peuvent pas être utilisés comme destination pour des sauvegardes de machines sous macOS.
- Ces emplacements ne peuvent pas être utilisés comme destination pour des sauvegardes reconnaissant les applications.

- Le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** n'est pas disponible lors de la sauvegarde vers ces emplacements.
- La règle de rétention **Par volume total de sauvegardes** n'est pas disponible pour ces emplacements.

NFS

- La sauvegarde vers des partages NFS n'est pas disponible sous Windows.
- Le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** pour les fichiers (machines physiques) n'est pas disponible lors de la sauvegarde vers des partages NFS.

Secure Zone

- Il est impossible de créer Secure Zone sur un Mac.

Emplacement géré

- Un emplacement géré avec déduplication ou chiffrement ne peut pas être sélectionné comme destination :
  - si le modèle de sauvegarde est défini sur **Toujours incrémentielle (fichier unique)** ;
  - si le format de sauvegarde est défini sur **Version 12** ;
  - Pour les sauvegardes de niveau disque de machines sous macOS
  - Pour les sauvegardes de boîtes aux lettres Exchange et Microsoft 365.
- La règle de rétention **Par volume total de sauvegardes** n'est pas disponible pour un emplacement géré avec la déduplication activée.

Toujours incrémentielle (fichier unique)

- Le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** n'est pas disponible lors de la sauvegarde sur un serveur SFTP ou un périphérique à bandes.
- Le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** pour les fichiers (machines physiques) est disponible uniquement lorsque l'emplacement de la sauvegarde principale est Acronis Cloud.

Par volume total de sauvegardes

- La règle de rétention **Par volume total de sauvegardes** n'est pas disponible :
  - si le modèle de sauvegarde est défini sur **Toujours incrémentielle (fichier unique)** ;
  - lors d'une sauvegarde sur un serveur SFTP, un périphérique à bandes ou un emplacement géré avec la déduplication activée.

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 configurer une telle sauvegarde, dans **Quoi sauvegarder**, sélectionnez **Toute la machine**.

Important
Les lecteurs externes, comme les lecteurs flash USB ou les disques durs USB, ne sont pas inclus dans la sauvegarde de **Toute la machine**. Pour sauvegarder ces disques, configurez une sauvegarde volume **Disques/volumes**. Pour plus d'informations sur la sauvegarde de disque, reportez-vous à "Sélection de disques/volumes" (p. 220).

Sélection de disques/volumes

Une sauvegarde de niveau disque contient une copie d'un disque ou d'un volume sous forme compacte. Vous pouvez restaurer des disques individuels, des volumes ou des fichiers depuis une sauvegarde de niveau disque. La sauvegarde d'une machine dans son intégralité correspond à une sauvegarde de tous ses disques non amovibles.

Remarque
Par défaut, le dossier racine OneDrive est exclu des opérations de sauvegarde. Si vous choisissez de sauvegarder des fichiers et dossiers OneDrive spécifiques, ils seront sauvegardés. Les fichiers qui ne sont pas disponibles sur l'appareil auront un contenu non valide dans l'archive.

Il existe deux façons de sélectionner des disques/volumes : directement sur chaque machine ou à l'aide de règles de stratégie. Vous avez la possibilité d'exclure des fichiers d'une sauvegarde de disque en paramétrant les filtres de fichiers.

Sélection directe

La sélection directe n'est disponible que pour les machines physiques. Pour activer la sélection directe de disques et volumes sur une machine virtuelle, vous devez installer l'agent de protection sur son système d'exploitation invité.

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 machines comprises dans le plan de protection, cochez les cases à côté des disques ou des volumes à sauvegarder.
5. Cliquez sur **Valider**.

Utilisation des 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.
   Les règles de stratégie seront appliquées à l'ensemble des machines du plan de protection. Si parmi les données d'une machine, aucune ne répond à au moins l'une des règles au moment où la sauvegarde commence, cette dernière échouera.
5. Cliquez sur **Valider**.

Règles pour Windows, Linux et macOS

- `[Tous les volumes]` sélectionne tous les volumes des machines exécutant Windows et tous les volumes montés sur les machines exécutant Linux ou macOS.

Règles pour Windows

- Lettre de lecteur (par exemple, **C:**) sélectionne le volume correspondant à la lettre de lecteur indiquée.
- `[Volumes fixes (machines physiques)]` sélectionne l'ensemble des volumes des machines physiques, autres que les supports amovibles. Les volumes fixes incluent les volumes sur les périphériques SCSI, ATAPI, ATA, SSA, SAS et SATA, et sur les matrices RAID.
- `[DÉMARRAGE+DISQUE SYSTÈME]` sélectionne le volume système et le volume de démarrage. Cette combinaison correspond à l'ensemble de données minimum nécessaire à la restauration du système d'exploitation depuis la sauvegarde.
- `[DÉMARRAGE+DISQUE SYSTÈME (machines physiques)]` sélectionne tous les volumes du disque sur lequel le volume de démarrage et le volume système sont situés. Si le volume de démarrage et le volume système ne sont pas situés sur le même disque, rien ne sera sélectionné. Cette règle ne s'applique qu'aux machines physiques.
- `[Disque 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.

Règles pour Linux

- `/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, saisissez :

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Règles pour macOS

- `[Disque 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.

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) :
  - 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 7, les points de restauration Windows ne sont pas sauvegardés.
  - Si l'option de sauvegarde **service de cliché instantané des volumes (VSS)** 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.

Sélection de fichiers/dossiers

La sauvegarde de niveau fichier est disponible pour les machines physiques et les machines virtuelles sauvegardées par un agent installé dans le système invité.

Une sauvegarde de niveau fichier n'est pas suffisante pour restaurer le système d'exploitation. Choisissez la sauvegarde de fichiers si vous planifiez de ne protéger que certaines données (le projet en cours, par exemple). Ceci réduira la taille de la sauvegarde, économisant ainsi de l'espace de stockage.

Remarque
Par défaut, le dossier racine OneDrive est exclu des opérations de sauvegarde. Si vous choisissez de sauvegarder des fichiers et dossiers OneDrive spécifiques, ils seront sauvegardés. Les fichiers qui ne sont pas disponibles sur l'appareil auront un contenu non valide dans l'archive.

Il existe deux façons de sélectionner des fichiers : directement sur chaque machine ou à l'aide de règles de stratégie. Ces deux méthodes vous permettent d'affiner votre sélection en paramétrant les filtres de fichiers.

Sélection directe

1. Dans **Quoi sauvegarder**, sélectionnez **Fichiers/dossiers**.
2. Cliquez sur **Éléments à sauvegarder**.
3. Dans **Sélectionner les éléments à sauvegarder**, sélectionnez **Directement**.
4. Pour chacune des machines du plan de protection :
   a. Cliquez sur **Sélectionner les fichiers et dossiers**.
   b. Cliquez sur **Dossier local** ou sur **Dossier réseau**.
      Le partage doit être accessible depuis la machine sélectionnée.
   c. Naviguez vers les fichiers/dossiers partagés souhaités ou indiquez leur chemin, puis cliquez sur la flèche. Si vous y êtes invité, spécifiez le nom d'utilisateur et le mot de passe requis pour accéder au dossier partagé.
      La sauvegarde d'un dossier avec accès anonyme n'est pas prise en charge.
   d. Sélectionnez les fichiers/dossiers souhaités.
   e. Cliquez sur **Valider**.

Utilisation des règles de stratégie

1. Dans **Quoi sauvegarder**, sélectionnez **Fichiers/dossiers**.
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.
   Les règles de stratégie seront appliquées à l'ensemble des machines du plan de protection. Si parmi les données d'une machine, aucune ne répond à au moins l'une des règles au moment où la sauvegarde commence, cette dernière échouera.
5. Cliquez sur **Valider**.

Règles de sélection pour Windows

- Chemin complet vers le fichier ou dossier, par exemple **D:\Work\Text.doc** ou **C:\Windows**.
- Modèles :

- `[All Files]` sélectionne tous les fichiers sur tous les volumes de la machine.
- `[All Profiles Folder]` sélectionne le dossier où se trouvent tous les profils des utilisateurs (généralement, **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 (généralement, **C:\ProgramData** ou **C:\Documents and Settings\All Users**).
  - `%PROGRAMFILES%` sélectionne le dossier des fichiers programmes (par exemple, **C:\Program Files**).
  - `%WINDIR%` sélectionne le dossier sélectionne le dossier où se trouve 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 des fichiers programmes, saisissez : **%PROGRAMFILES%\Java**.

Règles de sélection pour Linux

- 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**.
  - `/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.
- Modèles :
  - `[Tous les dossiers profils]` sélectionne **/home**. Dossier où se trouvent par défaut tous les profils des utilisateurs.

Règles de sélection pour macOS

- Chemin complet vers un fichier ou un répertoire.
- Modèles :
  - `[Tous les dossiers profils]` sélectionne **/Users**. Dossier où se trouvent par défaut tous les profils des utilisateurs.

Exemples :

- Pour sauvegarder **file.txt** sur votre bureau, spécifiez **/Users/<nom d'utilisateur>/Desktop/file.txt**, où <nom d'utilisateur> correspond à votre nom d'utilisateur.
- Pour sauvegarder l'ensemble des répertoires personnels de tous les utilisateurs, indiquez **/Users**.
- Pour sauvegarder le répertoire dans lequel les applications sont installées, indiquez **/Applications**.

Sélection de l'état du système

La sauvegarde de l'état du système est disponible pour les ordinateurs exécutant Windows 7 et versions ultérieures.

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
- 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.
- Pour sauvegarder la configuration ESXi, l'agent pour VMware utilise une connexion SSH à l'hôte ESXi sur le port TCP 22. Assurez-vous que votre pare-feu ne bloque pas cette connexion.
- Vous devez connaître le mot de passe du compte « root » sur l'hôte ESXi.

Limites

- La sauvegarde de la configuration ESXi n'est pas prise en charge pour VMware vSphere 7.0.
- Une configuration ESXi ne peut pas être sauvegardée sur le stockage dans le Cloud.

Pour sélectionner une configuration ESXi

1. Cliquez sur **Périphériques** > **Tous les périphériques**, puis sélectionnez les hôtes ESXi que vous voulez sauvegarder.
2. Cliquez sur **Sauvegarder**.
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.

Protection continue des données (CDP)

Les sauvegardes sont généralement effectuées de manière régulière, mais à des intervalles plutôt longs, pour des questions de performance. Si le système est soudainement endommagé, les modifications des données qui ont eu lieu entre la dernière sauvegarde et la panne du système seront perdues.

La fonctionnalité **protection continue des données** vous permet de sauvegarder les modifications apportées aux données sélectionnées entre les sauvegardes planifiées, et ce de manière continue :

- En suivant les modifications apportées à des fichiers/dossiers spécifiques
- En suivant les modifications apportées à des fichiers par des applications spécifiques

Vous pouvez sélectionner des fichiers particuliers pour une protection continue des données, à partir des données sélectionnées pour une sauvegarde. Le système sauvegardera toute modification apportée à ces fichiers. Vous pourrez récupérer ces fichiers comme ils étaient lors de leur dernière modification.

Pour le moment, la fonctionnalité de **protection continue des données** n'est prise en charge que pour les systèmes d'exploitation suivants :

- Windows 7 et versions ultérieures
- Windows Server 2008 R2 et versions ultérieures

Système de fichiers pris en charge : NTFS uniquement, dossier local uniquement (les dossiers partagés ne sont pas pris en charge).

L'option **Protection continue des données** n'est pas compatible avec l'option **Sauvegarde d'applications**.

Remarque
Les fonctionnalités entre les différentes éditions varient. Certaines des fonctionnalités décrites dans cette section peuvent être indisponibles avec votre licence. Pour obtenir des informations détaillées sur les fonctionnalités incluses dans chaque édition, consultez la section Comparaison des éditions Acronis Cyber Protect 15 incluant le déploiement dans le cloud.

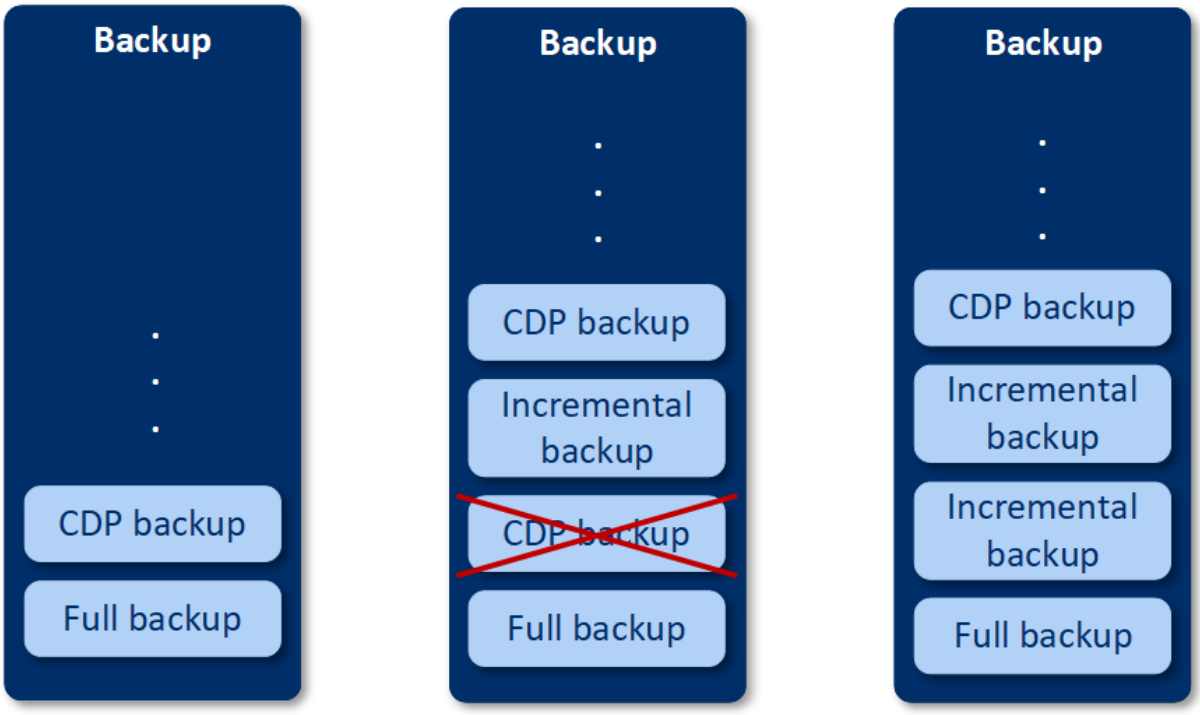
Fonctionnement

Choisissons d'appeler la sauvegarde créée de manière continue « Sauvegarde CDP ». Pour que la sauvegarde avec protection continue des données soit créée, une sauvegarde complète ou incrémentielle doit avoir été créée au préalable.

Lorsque vous exécutez le plan de protection avec module Sauvegarde pour la première fois et que la **protection continue des données** est activée, une sauvegarde complète est d'abord créée. Juste après cela, la sauvegarde CDP pour les fichiers/dossiers sélectionnés ou modifiés sera créée. La sauvegarde CDP contient toujours les données que vous avez sélectionnées, dans leur dernier état. Lorsque vous apportez des modifications aux fichiers/dossiers sélectionnés, aucune nouvelle sauvegarde CDP n'est créée. Toutes les modifications sont enregistrées dans la même sauvegarde CDP.

Lorsque vient le moment d'effectuer une sauvegarde incrémentielle planifiée, la sauvegarde CDP est abandonnée, et une nouvelle sauvegarde CDP est créée juste après la sauvegarde incrémentielle.

Par conséquent, la sauvegarde CDP est toujours la dernière sauvegarde de la chaîne de sauvegarde qui dispose de la version la plus à jour des fichiers/dossiers protégés.



Si vous disposez déjà d'un plan de protection avec module de sauvegarde activé et que vous décidez d'activer la **protection continue des données**, la sauvegarde CDP sera créée juste après avoir activé l'option, car la chaîne de sauvegarde possède déjà des sauvegardes complètes.

Sources et destinations de données prises en charge pour la protection continue des données

Pour que la protection continue des données fonctionne correctement, vous devez spécifier les éléments suivants pour les sources de données suivantes :

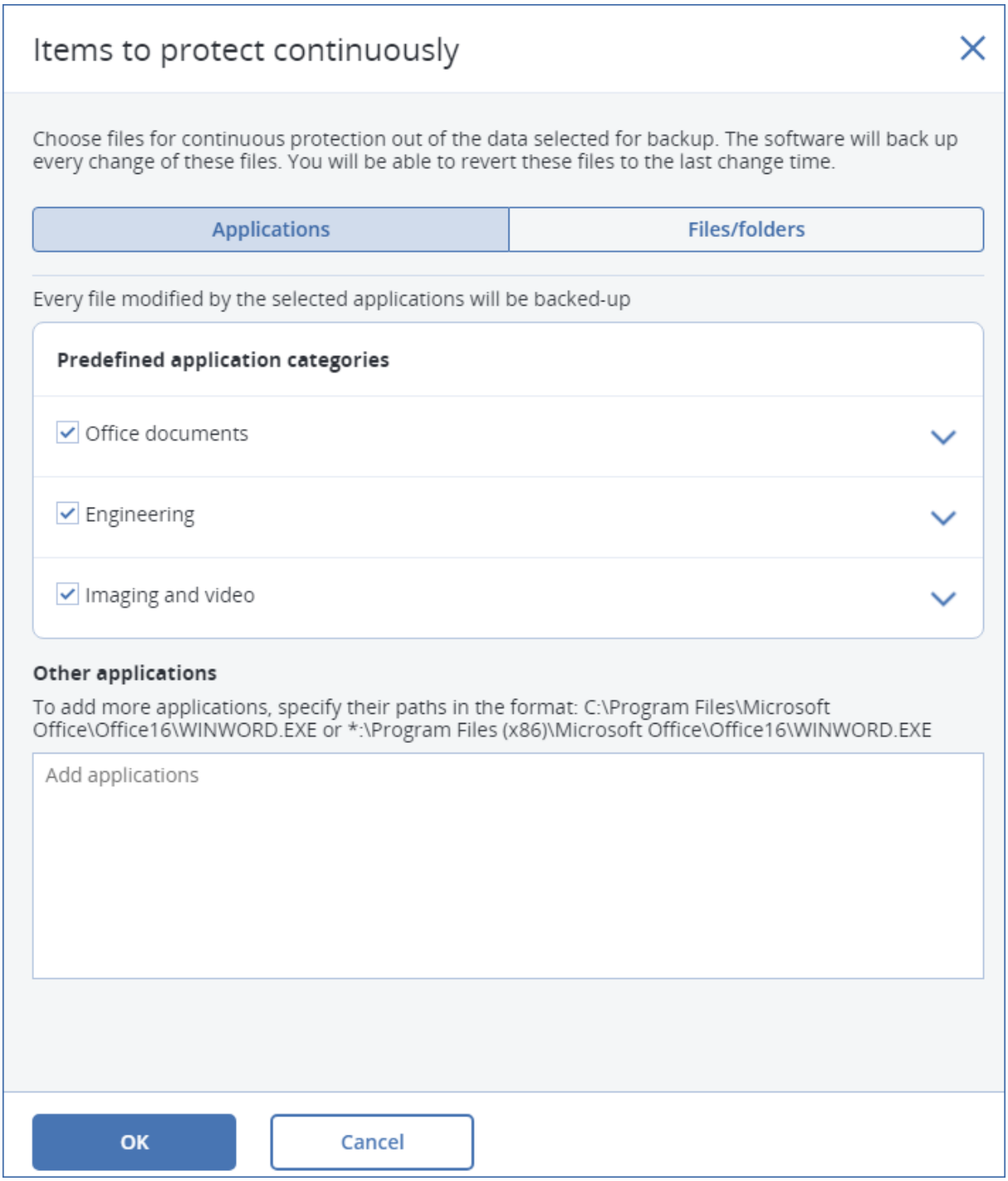
Quoi sauvegarder	Éléments à sauvegarder
Toute la machine	Vous devez spécifier des fichiers/dossiers ou des applications.
Disques/volumes	Vous devez spécifier des disques/volumes, ainsi que des fichiers/dossiers ou des applications.
Fichiers/dossiers	Vous devez spécifier des fichiers/dossiers. Vous pouvez spécifier des applications (facultatif).

Les destinations de sauvegarde suivantes sont prises en charge pour la protection continue des données :

- Dossier local
- Dossier réseau
- Emplacement défini par un script
- Stockage dans le Cloud
- Acronis Cyber Infrastructure

Protéger les périphériques avec la protection continue des données

1. Dans la console Web Cyber Protect, créez un plan de protection avec le module **Sauvegarde** activé.
2. Activez l'option **Protection continue des données (CDP)**.
3. Spécifiez les **Éléments à protéger continuellement** :
   - **Applications** (tout fichier modifié par les applications sélectionnées sera sauvegardé). Nous vous recommandons d'utiliser cette option pour protéger vos documents Office avec la sauvegarde CDP.



- Vous pouvez sélectionner les applications à partir des catégories prédéfinies ou spécifier d'autres applications en définissant le chemin d'accès à leur fichier exécutable. Utilisez l'un des formats suivants :

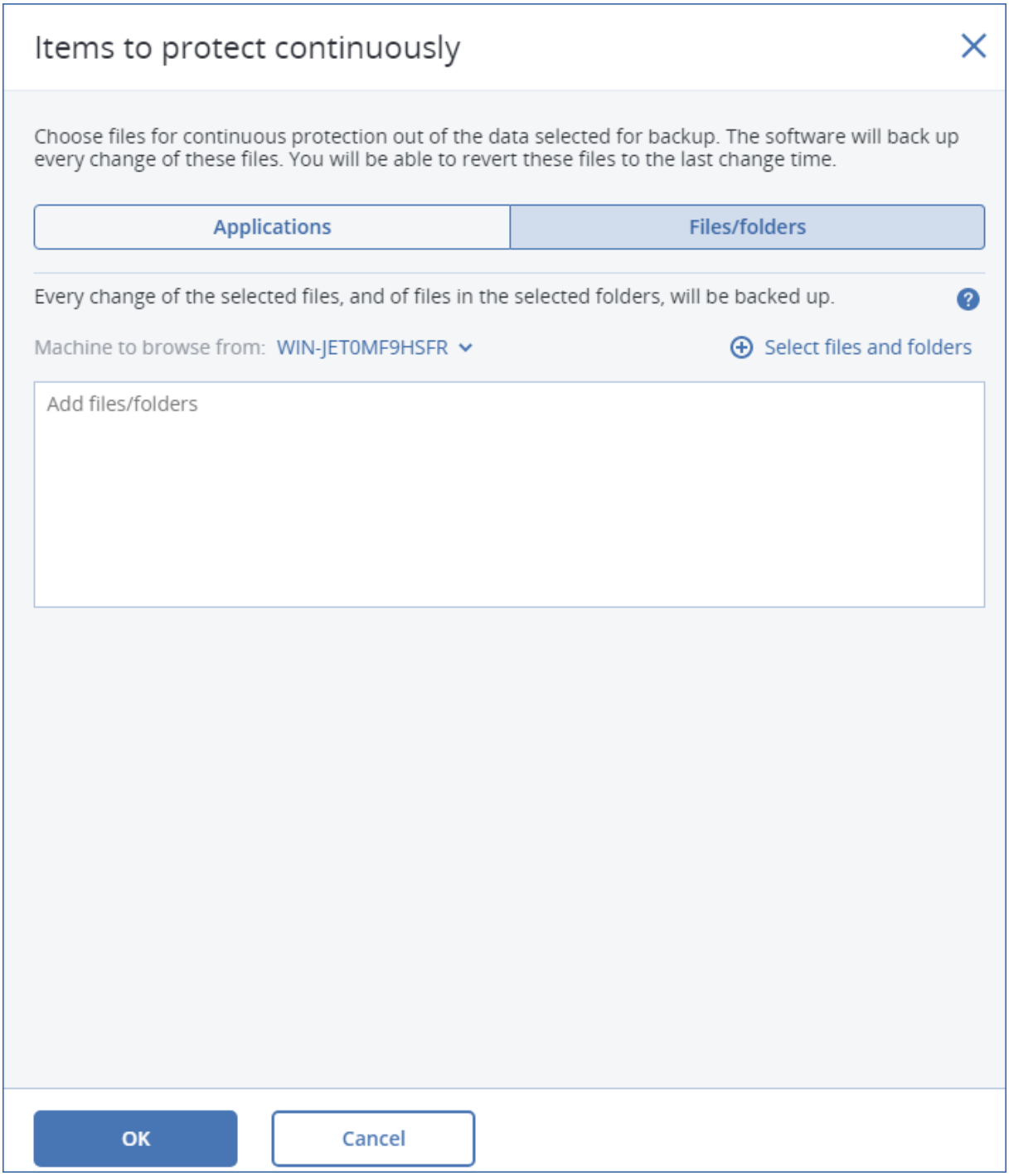
  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  OR

  `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

  - **Fichiers/dossiers** (tout fichier modifié dans le ou les emplacements spécifiés sera

sauvegardé). Nous vous recommandons d'utiliser cette option pour protéger les fichiers et dossiers qui sont modifiés de manière continue.



1. **Machine à parcourir :** spécifiez la machine dont vous souhaitez sélectionner les fichiers/dossiers pour la protection continue des données.

   Cliquez sur **Sélectionner les fichiers et dossiers** pour sélectionner les fichiers/dossiers sur la machine spécifiée.

Important
Si vous spécifiez manuellement un dossier entier dont les fichiers seront sauvegardés de manière continue, utilisez un masque, par exemple :
Chemin correct : D:\Data*
Chemin incorrect : D:\Data\

Dans le champ de texte, vous pouvez également spécifier des règles pour la sélection des fichiers/dossiers à sauvegarder. Pour en savoir plus sur la définition de règles, reportez-vous à la section « Sélection de fichiers/dossiers ». Lorsque vous avez terminé, cliquez sur **Terminé**.

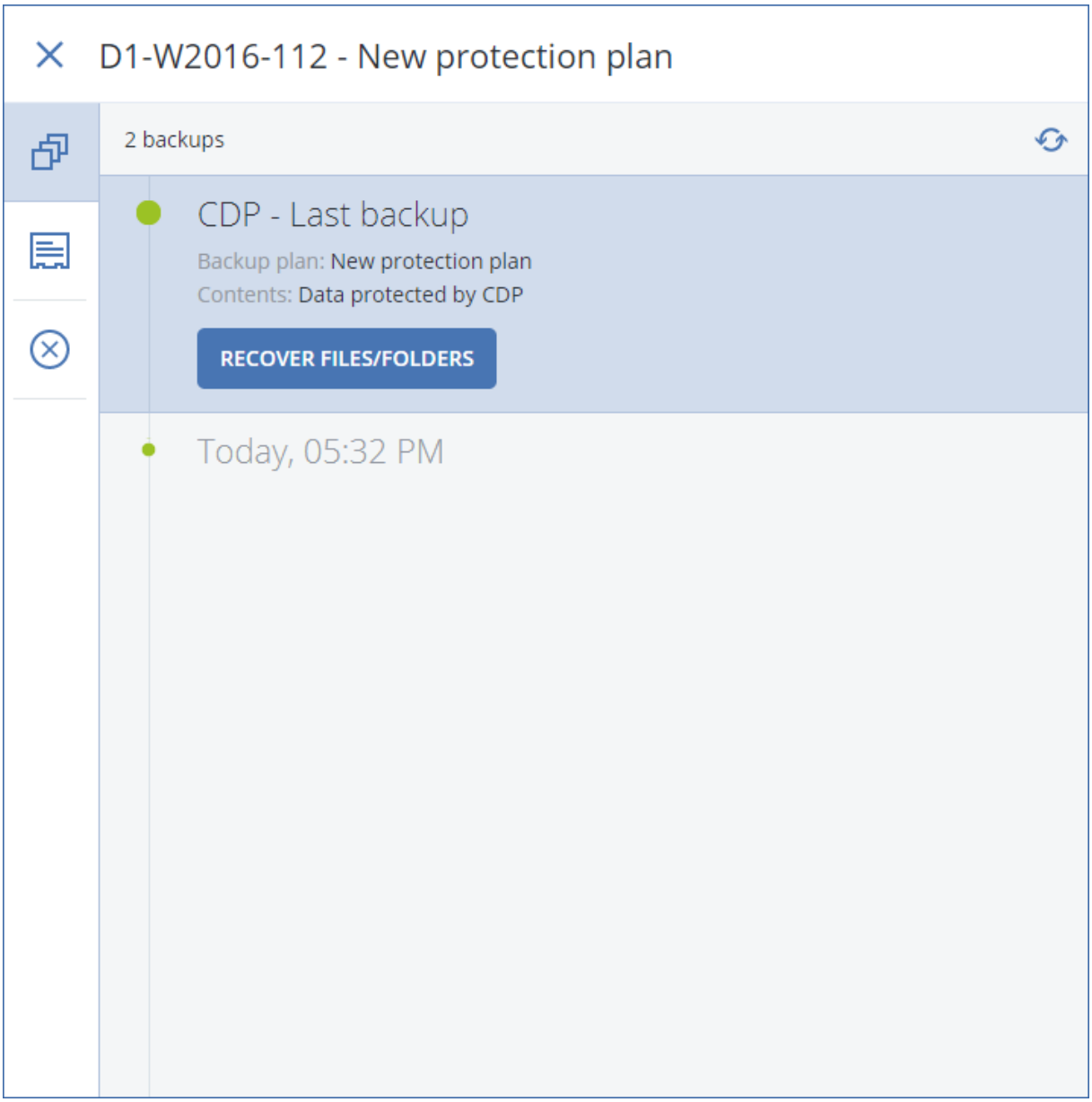
2. Cliquez sur **Créer**.

Le plan de protection avec protection continue des données activée sera alors assigné à la machine sélectionnée. Après la première sauvegarde régulière, les sauvegardes contenant la version la plus à jour des données protégées par CDP seront créées de manière continue. Les données définies via Applications, tout comme celles définies via Fichiers/Dossiers, seront sauvegardées.

Les données sauvegardées de manière continue sont conservées conformément à la règle de rétention définie pour le module Sauvegarde.

Distinguer les sauvegardes protégées de manière continue

Les sauvegardes qui sont sauvegardées de manière continue disposent du préfixe CDP.



Restaurer votre machine à son état le plus récent

Si vous souhaitez pouvoir restaurer votre machine à son état le plus récent, vous pouvez vous servir de l'option **Protection continue des données (CDP)** dans le module Sauvegarde d'un plan de protection.

À partir d'une sauvegarde CDP, vous pouvez restaurer une machine tout entière, ou des fichiers/dossiers spécifiques. Dans le premier cas, vous rétablirez l'état le plus récent d'une machine tout entière. Dans l'autre, vous rétablirez l'état le plus récent de fichiers/dossiers.

Sélection d'une destination

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

Pour sélectionner un emplacement de sauvegarde

1. Cliquez sur **Où sauvegarder**.
2. Effectuez l'une des actions suivantes :
   - Sélectionnez un emplacement de sauvegarde précédemment utilisé ou prédéfini
   - Cliquez sur **Ajouter un emplacement**, puis indiquez un nouvel emplacement de sauvegarde.

Emplacements pris en charge

- **Stockage dans le Cloud**

  Les sauvegardes seront stockées dans le centre de données du Cloud.
- **Dossier local**

  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.

  Naviguez vers le dossier partagé souhaité ou indiquez son chemin au format suivant :
  - Pour les partages SMB/CIFS : `\\<nom d'hôte>\<chemin>\` ou `smb://<nom d'hôte>/<chemin>/`
  - Pour les partages DFS : `\\<nom de domaine DNS complet>\<racine DFS>\<chemin>`

    Par exemple, `\\exemple.entreprise.com\partage\fichiers`

  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.
- **Acronis Cyber Infrastructure**

  Acronis Cyber Infrastructure peut être utilisé comme stockage software-defined storage très fiable avec redondance des données et réparation automatique. Ce stockage peut être configuré comme une passerelle pour stocker des sauvegardes dans Microsoft Azure ou dans l'une des nombreuses solutions de stockage compatibles avec S3 ou Swift. Le stockage peut également utiliser la solution NFS. Pour plus d'informations, consultez la page À propos de Acronis Cyber Infrastructure.

Important
La sauvegarde vers Acronis Cyber Infrastructure n'est pas disponible pour les ordinateurs macOS.

- **Dossier NFS** (disponible uniquement sur les machines sous Linux ou macOS)
  Vérifiez que le package nfs-utils est installé sur la machine Linux sur laquelle l'agent pour Linux est installé.
  Naviguez vers le dossier NFS souhaité ou indiquez son chemin au format suivant :
  `nfs://<nom d'hôte>/<dossier exporté>:/<sous-dossier>`
  Cliquez ensuite sur la flèche.
  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 sur un disque de la machine sauvegardée. Cette partition doit être créée manuellement, avant de configurer une sauvegarde. Pour en savoir plus sur la manière de créer Secure Zone, ses avantages et ses limites, consultez la section À propos de Secure Zone.
- **SFTP**
  Saisissez le nom ou l'adresse du serveur SFTP. Les notations suivantes sont prises en charge :
  `sftp://<serveur>`
  `sftp://<serveur>/<dossier>`
  Après avoir saisi le nom d'utilisateur et le mot de passe, vous pouvez parcourir les dossiers du serveur.
  Dans n'importe quelle notation, vous pouvez également spécifier le port, le nom d'utilisateur et le mot de passe :
  `sftp://<serveur>:<port>/<dossier>`
  `sftp://<nom d'utilisateur>@<serveur>:<port>/<dossier>`
  `sftp://<nom d'utilisateur>:<mot de passe>@<serveur>:<port>/<dossier>`
  Si le numéro de port n'est pas spécifié, le port 22 est utilisé.
  Les utilisateurs, pour lesquels un accès SFTP sans mot de passe est configuré, ne peuvent pas sauvegarder vers SFTP.
  La sauvegarde sur des serveurs FTP n'est pas prise en charge.

Options de stockage avancées

- **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\<nom de l'ordinateur>` :

```
WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject
("WScript.Network").ComputerName);
```

- Le script **JScript** suivant fournit l'emplacement de sauvegarde dans un dossier de l'ordinateur sur lequel le script s'exécute :

```
WScript.Echo("C:\\Backup");
```

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 Web Cyber Protect. Utilisez également la majuscule pour la lettre du lecteur.

- Le script **VBScript** suivant fournit l'emplacement de sauvegarde pour un ordinateur au format `\\bkpsrv\<nom de l'ordinateur>` :

```
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**.

- **Nœud de stockage**

  Un nœud de stockage est un serveur destiné à optimiser l'utilisation de plusieurs ressources (telles que la capacité de stockage pour l'entreprise, la bande passante du réseau et la charge de l'UC des serveurs de production) requises pour la protection de données de l'entreprise. Ce but est atteint grâce à l'organisation et à la gestion des emplacements qui servent d'unités de stockage dédiées des sauvegardes de l'entreprise (emplacements gérés).

  Vous pouvez sélectionner un emplacement préalablement créé ou en créer un nouveau en cliquant sur **Ajouter un emplacement** > **Nœud de stockage**. Pour des informations concernant les paramètres, consultez la section « Ajouter un emplacement géré ».

  Vous pourrez être invité à spécifier le nom d'utilisateur et le mot de passe pour le nœud de stockage. Les membres des groupes Windows suivants de la machine sur laquelle un nœud de stockage est installé ont accès à tous les emplacements gérés du nœud de stockage.

  - **Administrateurs**
  - **Remote Users Acronis ASN**

Ce groupe est créé automatiquement lorsque le nœud de stockage est installé. Par défaut, ce groupe est vide. Vous pouvez ajouter des utilisateurs à ce groupe manuellement.

- **Bande**

  Si un périphérique à bandes est attaché à la machine sauvegardée ou à un nœud de stockage, la liste d'emplacements affiche le pool de bandes par défaut. Ce pool est créé automatiquement.

  Vous pouvez sélectionner le pool par défaut ou en créer un nouveau en cliquant sur **Ajouter un emplacement** > **Bande**. Pour des informations concernant les paramètres du pool, consultez la section « Créer un pool ».

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.

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.

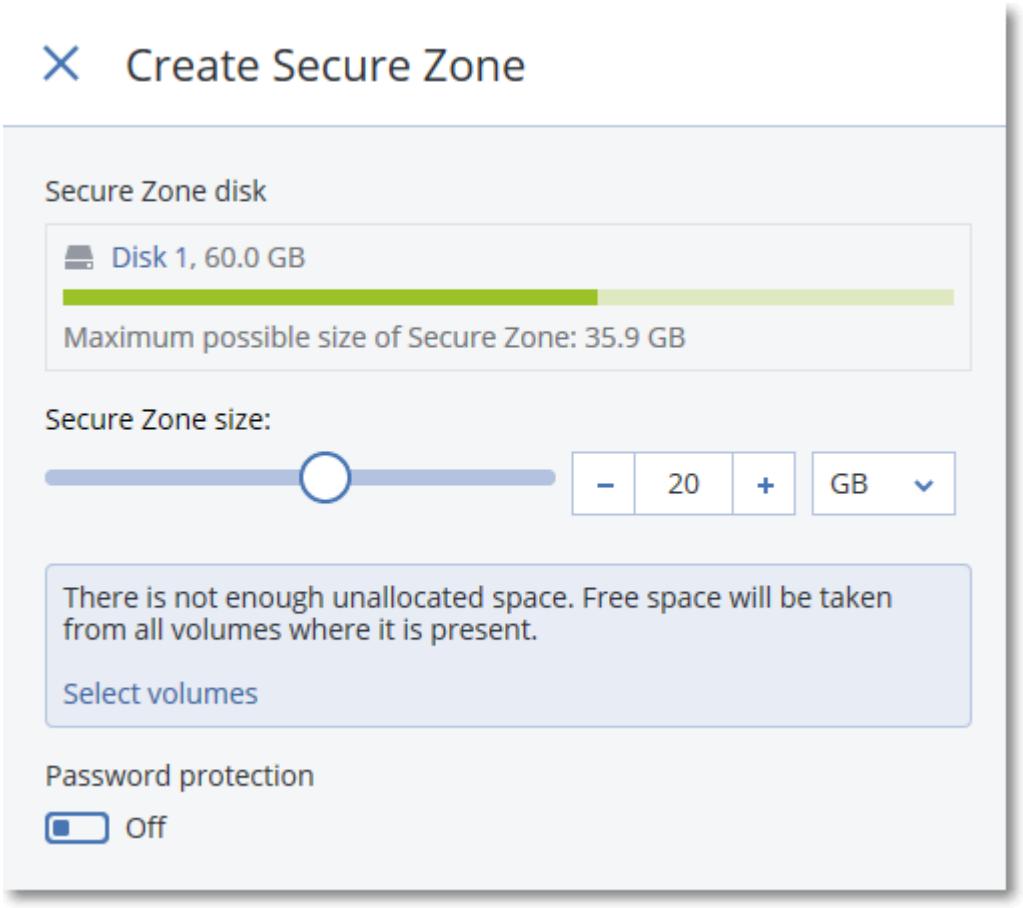
- Lorsque tout l'espace non alloué est collecté mais que ce n'est toujours pas assez, le logiciel prend de l'espace libre dans les volumes que vous sélectionnez, proportionnellement à la taille des volumes.
- Cependant, il doit toujours y avoir de l'espace libre sur un volume, de façon à ce que le système 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.



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.

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.

À propos d'Acronis Cyber Infrastructure

Acronis Cyber Protect 15 prend en charge l'intégration avec Acronis Cyber Infrastructure 3.5 Update 5 ou versions ultérieures.

La sauvegarde vers Acronis Cyber Infrastructure n'est pas disponible pour les ordinateurs macOS.

Déploiement

Pour utiliser Acronis Cyber Infrastructure, déployez-le sur du matériel vierge dans vos locaux. Au moins cinq serveurs physiques sont recommandés pour tirer pleinement parti du produit. Si vous avez uniquement besoin de la fonctionnalité passerelle, vous pouvez utiliser un serveur physique ou virtuel, ou configurer une passerelle cluster avec autant de serveurs que vous le souhaitez.

Assurez-vous que les paramètres de date/heure sont synchronisés entre le serveur de gestion et Acronis Cyber Infrastructure. Les paramètres de date/heure pour Acronis Cyber Infrastructure peuvent être configurés pendant le déploiement. La synchronisation date/heure via Network Time Protocol (NTP) est activé par défaut.

Vous pouvez déployer plusieurs instances d'Acronis Cyber Infrastructure et les enregistrer sur le même serveur de gestion.

Enregistrement

L'inscription est effectuée dans l'interface web Acronis Cyber Infrastructure. Acronis Cyber Infrastructure peut être uniquement enregistré par les administrateurs de l'organisation et uniquement au sein de l'organisation. Une fois enregistré, le stockage est disponible pour toutes les unités de l'organisation. Il peut être ajouté comme emplacement de sauvegarde à n'importe quelle unité ou à l'organisation.

L'opération inverse (désinscription) s'effectue dans l'interface Acronis Cyber Protect. Cliquez sur **Paramètres** > **Nœuds de stockage**, sélectionnez l'Acronis Cyber Infrastructure requis, puis cliquez sur **Supprimer**.

Ajout d'un emplacement de sauvegarde

Seul un emplacement de sauvegarde sur chaque instance d'Acronis Cyber Infrastructure peut être ajouté à une unité ou organisation. Un emplacement ajouté au niveau d'une unité est disponible pour cette unité et les administrateurs de l'organisation. Un emplacement ajouté au niveau d'une organisation est disponible pour les administrateurs de l'organisation uniquement.

Lors de l'ajout d'un emplacement, vous créez et entrez son nom. Si vous avez besoin d'ajouter un emplacement existant à un serveur de gestion nouveau ou différent, cochez la case **Utiliser un emplacement existant...**, cliquez sur **Rechercher**, puis sélectionnez un emplacement dans la liste.

Si plusieurs instances d'Acronis Cyber Infrastructure sont enregistrées sur le serveur de gestion, il est possible de sélectionner une instance d'Cyber Infrastructure lors de l'ajout de l'emplacement.

Modèles de sauvegarde, opérations et limitations

L'accès direct à Acronis Cyber Infrastructure depuis le support de démarrage n'est pas disponible. Pour utiliser Acronis Cyber Infrastructure, enregistrez le support sur le serveur de gestion et gérez-le via la console Web Cyber Protect.

L'accès à Acronis Cyber Infrastructure via l'interface de ligne de commande n'est pas disponible.

Concernant les modèles de sauvegarde disponibles et les opérations avec sauvegardes, Acronis Cyber Infrastructure est similaire au stockage dans le Cloud. La seule différence : les sauvegardes peuvent être répliquées *à partir* d'AcronisCyber Infrastructure pendant l'exécution d'un plan de protection.

Documentation

L'ensemble de la documentation Acronis Cyber Infrastructure est disponible sur le site Internet d'Acronis.

Planification

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

La planification utilise les mêmes paramètres de temps (y compris le fuseau horaire) que le système d'exploitation dans lequel l'agent est installé. Le fuseau horaire de l'agent pour VMware (matériel virtuel) peut être configuré dans l'interface de l'agent.

Par exemple, si un plan de protection est planifié pour s'exécuter à 21h00 et appliqué à plusieurs machines situées dans des fuseaux horaires différents, la sauvegarde commencera sur chaque machine à 21h00, heure locale.

Les paramètres de planification dépendent de la destination de la sauvegarde.

Lorsque vous effectuez une sauvegarde vers le Cloud

Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi. Vous pouvez sélectionner l'heure de démarrage de la sauvegarde.

Si vous souhaitez modifier la fréquence des sauvegardes, faites glisser le curseur, puis indiquez la planification des sauvegardes.

Vous pouvez planifier la sauvegarde pour qu'elle s'exécute en fonction d'événements, plutôt qu'en fonction d'une heure. Pour ce faire, sélectionnez le type d'événement dans le sélecteur de planification. Pour plus d'informations, consultez la section « Planifier par événements ».

Important
La première sauvegarde sera complète, et prendra donc plus de temps. Les sauvegardes suivantes seront incrémentielles et dureront beaucoup moins longtemps.

Lorsque vous effectuez une sauvegarde vers d'autres emplacements

Vous pouvez choisir l'un des modèles de sauvegarde prédéfinis ou créer un modèle personnalisé. Le modèle de sauvegarde fait partie du plan de protection, qui inclut le calendrier et les méthodes de sauvegarde.

Dans **Modèle de sauvegarde**, sélectionnez l'une des options suivantes :

- **Toujours incrémentielle (fichier unique)**
  Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi. Vous pouvez sélectionner l'heure de démarrage de la sauvegarde.
  Si vous souhaitez modifier la fréquence des sauvegardes, faites glisser le curseur, puis indiquez la planification des sauvegardes.
  Les sauvegardes utilisent le nouveau format de sauvegarde sous forme d'un fichier unique[1].
  Ce schéma n'est pas disponible lors de la sauvegarde sur un lecteur de bandes ou un serveur SFTP.
- **Toujours complète**
  Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi. Vous pouvez sélectionner l'heure de démarrage de la sauvegarde.
  Si vous souhaitez modifier la fréquence des sauvegardes, faites glisser le curseur, puis indiquez la planification des sauvegardes.
  Toutes les sauvegardes sont complètes.
- **Complète hebdomadaire, incrémentielle journalière**
  Par défaut, les sauvegardes s'effectuent de manière quotidienne, du lundi au vendredi. Vous pouvez modifier les jours de la semaine et l'heure des sauvegardes.
  Une sauvegarde complète est créée une fois par semaine. Toutes les autres sauvegardes sont incrémentielles. Le jour au cours duquel la sauvegarde complète est créée dépend de l'option

[1] Nouveau format de sauvegarde, pour lequel les sauvegardes complètes et incrémentielles subséquentes sont enregistrées sous forme d'un fichier .tib unique, plutôt que d'une suite de fichiers. 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, par exemple les serveurs SFTP.

Sauvegarde hebdomadaire (cliquez sur l'icône en forme d'engrenage, puis sur **Options de sauvegarde** > **Sauvegarde hebdomadaire**).

- **Complète mensuelle, différentielle hebdomadaire, incrémentielle journalière (GFS)**

  Par défaut, les sauvegardes incrémentielles s'effectuent de manière quotidienne, du lundi au vendredi, les sauvegardes différentielles tous les samedis, et les sauvegardes complètes le premier de chaque mois. Vous pouvez modifier ces planifications et l'heure des sauvegardes.

  Ce modèle de sauvegarde est affiché en tant que sauvegarde **Personnalisée** dans le volet du plan de protection.
- **Personnalisée**

  Spécifiez les planifications pour les sauvegardes complètes, différentielles et incrémentielles.

  Les sauvegardes différentielles ne sont pas disponibles pour les données SQL, Exchange ou d'état du système.

Grâce à un modèle de sauvegarde, vous pouvez planifier la sauvegarde pour qu'elle s'exécute en fonction d'événements, plutôt qu'en fonction d'une heure. Pour ce faire, sélectionnez le type d'événement dans le sélecteur de planification. Pour plus d'informations, consultez l'article « Planifier par événements ».

Options de planification supplémentaires

Vous pouvez procéder comme suit pour toutes les destinations :

- Indiquez les conditions de démarrage de la sauvegarde, afin qu'une sauvegarde planifiée s'exécute uniquement si les conditions sont remplies. Pour plus d'informations, consultez l'article « Conditions de démarrage ».
- 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. Lorsque la planification est désactivée, les règles de rétention ne sont pas appliquées, sauf en cas de lancement manuel d'une sauvegarde.
- Introduire un délai à 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.

  Cliquez sur l'icône en forme d'engrenage, puis sur **Options de sauvegarde** > **Planification**. Sélectionnez **Répartir les heures de démarrage de sauvegarde dans une fenêtre de temps**, puis spécifiez le délai maximal. 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.

  Remarque

  Dans les déploiements dans le Cloud, cette option est activée par défaut, avec un délai maximal de 30 minutes. Par défaut, dans les déploiements sur site, toutes les sauvegardes démarrent à l'heure planifiée.

- Cliquez sur **Afficher plus** pour accéder aux options suivantes :
  - **Si la machine est arrêtée, exécutez les tâches ratées lors du démarrage de la machine** (désactivée par défaut)
  - **Empêcher l'activation du mode veille ou veille prolongée pendant la sauvegarde** (désactivée par défaut)

    Cette option fonctionne uniquement pour les machines sous Windows.
  - **Sortir du mode veille ou veille prolongée pour démarrer une sauvegarde planifiée** (désactivée par défaut)

    Cette option fonctionne uniquement pour les machines sous Windows. Cette option ne fonctionne pas lorsque la machine est éteinte, c'est-à-dire l'option n'utilise pas la fonctionnalité Wake-on-LAN.

Planifier par événement

Lors de la configuration de la planification d'un plan de protection, sélectionnez le type d'événement dans le sélecteur de planification. La sauvegarde sera lancée aussitôt que l'un des événements se produira.

Vous pouvez choisir l'un des événements suivants :

- **Lors du temps écoulé depuis la dernière sauvegarde**

  Il s'agit du temps écoulé depuis la fin de la dernière sauvegarde réussie dans le même plan de protection. Vous pouvez spécifier la durée.

  Remarque
  Comme la planification se base sur un événement de sauvegarde réussi, si une sauvegarde échoue, le planificateur n'exécutera pas le travail tant qu'un opérateur n'aura pas exécuté le plan manuellement et que ce dernier n'aura pas été exécuté avec succès.

- **Lorsqu'un utilisateur se connecte au système**

  Par défaut, la connexion d'un utilisateur lancera une sauvegarde. Vous pouvez remplacer tout utilisateur par un compte d'utilisateur spécifique.
- **Lorsqu'un utilisateur se déconnecte du système**

  Par défaut, se déconnecter de tout utilisateur lancera une sauvegarde. Vous pouvez remplacer tout utilisateur par un compte d'utilisateur spécifique.

  Remarque
  La sauvegarde ne fonctionnera pas à l'arrêt d'un système, car un arrêt est différent d'une déconnexion.

- **Au démarrage du système**
- **À l'arrêt du système**
- **Lors d'un événement du journal des événements Windows**

  Vous devez spécifier les propriétés de l'événement.

Le tableau ci-dessous affiche les événements disponibles pour diverses données sous les systèmes d'exploitation Windows, Linux et macOS.

QUOI SAUVEGARDER	Lors du temps écoulé depuis la dernière sauvegarde	Lorsqu'un utilisateur se connecte au système	Lorsqu'un utilisateur se déconnecte du système	Au démarrage du système	À l'arrêt du système	Lors d'un événement du Journal des événements Windows
Disques/volumes ou fichiers (machines physiques)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disques/volumes (machines virtuelles)	Windows, Linux	–	–	–	–	–
Configuration ESXi	Windows, Linux	–	–	–	–	–
Boîtes aux lettres Microsoft 365	Windows	–	–	–	–	Windows
Bases de données et boîtes aux lettres Exchange	Windows	–	–	–	–	Windows
Bases de données SQL	Windows	–	–	–	–	Windows

Lors d'un événement du Journal des événements Windows

Vous pouvez planifier le démarrage d'une sauvegarde lorsqu'un événement Windows a été enregistré dans l'un des journaux d'événements, comme les journaux des **applications**, de **sécurité** ou **système**.

Par exemple, vous pouvez définir un plan de protection qui exécutera automatiquement une sauvegarde complète d'urgence de vos données aussitôt que Windows découvre que votre disque dur est sur le point de tomber en panne.

Pour parcourir les événements et voir leurs propriétés, utilisez le composant logiciel **Observateur d'événements** disponible sur la console **Gestion d'ordinateur**. Pour ouvrir le journal de **sécurité**, vous devez être membre du groupe **Administrateurs**.

Propriétés des événements

Nom du journal

Spécifie le nom du journal. Sélectionnez le nom d'un journal standard (**Application**, **Sécurité**, ou **Système**) dans la liste, ou saisissez un nom de journal, par exemple : **Microsoft Office Sessions**

Source d'événement

Spécifie l'événement source, lequel est généralement le programme ou le composant système qui a causé l'événement, par exemple : **disque**

Toute source d'événement contenant la chaîne spécifiée déclenchera la sauvegarde planifiée. Cette option n'est pas sensible à la casse. Par conséquent, si vous spécifiez la chaîne **service**, les sources d'événement **gestionnaire de contrôle du Service** et **Time-service** déclencheront tous les deux une sauvegarde.

Type d'événement

Spécifiez le type d'événement : **Erreur**, **Avertissement**, **Information**, **Succès de l'audit** ou **Échec de l'audit**.

Identifiant d'événement

Spécifie le numéro de l'événement, lequel identifie généralement la sorte d'événement particulier parmi les événements de la même source.

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 le 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 encore prêt à l'accès.

Exemple : Sauvegarde d'urgence « Bloc défectueux »

Un ou plusieurs blocs défectueux qui sont soudainement apparus sur le disque dur indiquent habituellement que le lecteur de disque dur est sur le point de tomber en panne. Supposons que vous voulez créer un plan de protection qui sauvegarde les données du disque dur aussitôt qu'une situation de ce genre se produit.

Lorsque Windows détecte un mauvais bloc sur le disque dur, il enregistre un événement avec le **disque** de source d'événement et le numéro d'événement **7** dans le journal de **Système** ; ce type d'événement est **Erreur**.

Lors de la création du plan, saisissez ou sélectionnez les informations suivantes dans la section **Planification** :

- **Nom de journal** : **Système**
- **Source d'événement** : **disque**
- **Type d'événement** : **Erreur**
- **ID d'événement** : **7**

Important
Pour garantir qu'une telle sauvegarde se terminera malgré la présence de mauvais blocs, vous devez indiquer à la sauvegarde de les ignorer. Pour ce faire, dans les **Options de sauvegarde**, allez dans **Traitement d'erreur**, puis sélectionnez la case **Ignorer mauvais secteurs**.

Conditions de démarrage

Ces paramètres ajoutent plus de flexibilité au planificateur, permettant l'exécution d'une sauvegarde selon certaines conditions. En cas de conditions multiples, toutes seront remplies simultanément pour permettre à la sauvegarde de se lancer. Les conditions de démarrage ne sont pas prises en compte lorsqu'une sauvegarde est lancée manuellement.

Pour accéder à ces paramètres, cliquez sur **Afficher plus** lors de la création d'une planification pour un plan de protection.

Le comportement du planificateur, dans le cas où l'événement (ou n'importe laquelle des conditions s'il y en a plusieurs) n'est pas rempli, est défini dans l'option de sauvegarde Conditions de démarrage de sauvegarde. Pour gérer la situation lorsque les conditions ne sont pas remplies pendant trop longtemps et qu'il devient trop risqué de retarder la sauvegarde, vous pouvez définir l'intervalle de temps à l'issue duquel la sauvegarde sera exécutée, quelle que soit la condition.

Le tableau ci-dessous affiche les conditions de démarrage disponibles pour diverses données sous les systèmes d'exploitation Windows, Linux et macOS.

QUOI SAUVEGARDER	Disques/volumes ou fichiers (machines physiques)	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	–	–	–	–	–
L'hôte de l'emplacement de la sauvegarde	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows

est disponible						
Utilisateurs déconnectés	Windows	–	–	–	–	–
Tient dans l'intervalle de temps	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Économiser de la batterie	Windows	–	–	–	–	–
Ne pas démarrer pendant une connexion mesurée	Windows	–	–	–	–	–
Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants	Windows	–	–	–	–	–
Vérifier l'adresse IP du périphérique	Windows	–	–	–	–	–

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

Exécuter la sauvegarde sur la machine tous les jours à 21h00, de préférence lorsque l'utilisateur est inactif. Si l'utilisateur est toujours actif à 23h00, exécutez quand même la sauvegarde.

- Planification : Quotidiennement, exécuter tous les jours. Démarrage à : **21h00**.
- Condition : **L'utilisateur est inactif**.
- Conditions de démarrage de la sauvegarde : **Patienter jusqu'à ce que les conditions soient remplies, Lancer quand même la sauvegarde après 2** heure(s).

En conséquence,

(1) Si l'utilisateur devient inactif avant 21h00, la sauvegarde débutera à 21h00.

(2) Si l'utilisateur devient inactif entre 21h00 et 23h00, la sauvegarde démarrera immédiatement après que l'utilisateur sera devenu inactif.

(3) Si l'utilisateur est toujours actif à 23h00, la sauvegarde débutera à 23h00.

L'hôte de l'emplacement de la sauvegarde est disponible

« L'hôte de l'emplacement de la sauvegarde est disponible » signifie que la machine hébergeant la destination pour le stockage des sauvegardes est disponible sur le réseau.

Cette condition est efficace pour des dossiers de réseau, le stockage sur le Cloud et les 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

Les données sont sauvegardées dans un dossier tous les jours ouvrés à 21h00. Si la machine qui héberge le dossier n'est pas disponible en ce moment, (par exemple à cause d'un travail de maintenance), sautez la sauvegarde et attendez le démarrage planifié du prochain jour ouvré.

- Planification : Tous les jours, exécuter de lundi à vendredi. Démarrage à : **21h00**.
- Condition : **L'hôte de l'emplacement de la sauvegarde est disponible**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

(1) S'il est 21h00 et que l'hôte est disponible, la sauvegarde démarrera immédiatement.

(2) S'il est 21h00 mais que l'hôte est indisponible, la sauvegarde démarrera le jour ouvré suivant si l'hôte est disponible.

(3) Si l'hôte n'est jamais disponible à 21h00, la tâche ne démarre jamais.

Utilisateurs déconnectés

Vous permet de mettre une sauvegarde en attente jusqu'à ce que tous les utilisateurs se déconnectent de Windows.

Exemple

Exécuter la sauvegarde à 20h00 tous les vendredis, de préférence lorsque tous les utilisateurs sont déconnectés. Si l'un des utilisateurs est toujours connecté à 23h00, lancer quand même la sauvegarde.

- Planification : Hebdomadaire, les vendredis. Démarrage à : **20h00**.
- 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** heure(s).

En conséquence :

(1) Si tous les utilisateurs sont déconnectés à 20h00, la sauvegarde débutera à 20h00.

(2) Si le dernier utilisateur se déconnecte entre 20h00 et 23h00, la sauvegarde démarrera automatiquement lorsque l'utilisateur se sera déconnecté.

(3) Si l'un des utilisateurs est toujours connecté à 23h00, la sauvegarde débute à 23h00.

Tient dans l'intervalle de temps

Limite l'heure de début d'une sauvegarde à un intervalle spécifié.

Exemple

Une société utilise différents emplacements sur la même unité de stockage rattachée au réseau pour sauvegarder les données des utilisateurs et des serveurs. Le jour ouvré débute à 08h00 et se termine à 17h00. Les données d'utilisateur doivent être sauvegardées à la déconnexion de l'utilisateur, mais pas avant 16h30. Tous les jours à 23h00, les serveurs de la société sont sauvegardés. Donc, toutes les données des utilisateurs doivent être de préférence sauvegardées avant cette heure afin de libérer la bande passante du réseau. On considère que la sauvegarde des données d'un utilisateur ne prend pas plus d'une heure. L'heure de début de la dernière sauvegarde est 22h00. Si un utilisateur est toujours connecté lors de l'intervalle de temps spécifié ou se déconnecte à n'importe quel moment, ne sauvegardez pas les données de l'utilisateur, c'est-à-dire ignorez l'exécution de la sauvegarde.

- Événement : **Lorsqu'un utilisateur se déconnecte du système**. Spécifiez le compte utilisateur : **Tout utilisateur**.
- Condition : **Tient dans l'intervalle de temps** de **16h30** à **22h00**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

(1) si l'utilisateur se déconnecte entre 16h30 et 22h00, la tâche de sauvegarde démarre automatiquement à la déconnexion.

(2) si l'utilisateur se déconnecte à n'importe quel autre moment, la sauvegarde sera ignorée.

Économiser de la batterie

Empêche une sauvegarde si le périphérique (un ordinateur portable ou une tablette) n'est pas connecté à une source d'alimentation. En fonction de la valeur de l'option de sauvegarde Conditions de démarrage de la sauvegarde, la sauvegarde ignorée démarrera ou non après la connexion du périphérique à une source d'alimentation. Les options suivantes sont disponibles :

- **Ne pas démarrer lors d'une alimentation sur batterie**
  Une sauvegarde démarrera seulement si le périphérique 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 le périphérique est connecté à une source d'alimentation ou si le niveau de la batterie est supérieur à la valeur spécifiée.

Exemple

Les données sont sauvegardées dans un dossier réseau tous les jours ouvrés à 21h00. Si le périphérique est connecté à une source d'alimentation (par exemple : l'utilisateur participe à une réunion tardive), il est préférable d'ignorer la sauvegarde pour économiser de la batterie et d'attendre que l'utilisateur connecte son périphérique à une source d'alimentation.

- Planification : Tous les jours, exécuter de lundi à vendredi. Démarrage à : 21h00.
- 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 :

(1) S'il est 21h00 et que le périphérique est connecté à une source d'alimentation, la sauvegarde démarrera immédiatement.

(2) S'il est 21h00 et que le périphérique fonctionne sur batterie, la sauvegarde démarrera dès que le périphérique sera connecté à une source d'alimentation.

Ne pas démarrer pendant une connexion mesurée

Empêche une sauvegarde (y compris une sauvegarde sur un disque local) si le périphérique 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.

Mesure supplémentaire pour empêcher les sauvegardes via une connexion mobile : lorsque vous activez la condition **Ne pas démarrer pendant une connexion mesurée**, la condition **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants** est activée automatiquement. Les noms de réseaux suivants sont spécifiés par défaut : « Android », « téléphone », « mobile » et « modem ». Vous pouvez supprimer ces noms de la liste en cliquant sur le symbole X.

Exemple

Les données sont sauvegardées dans un dossier réseau tous les jours ouvrés à 21h00. Si l'appareil est connecté à Internet via une connexion mesurée (par exemple : l'utilisateur est voyage d'affaires), il est préférable d'ignorer la sauvegarde pour économiser du trafic réseau et d'attendre le démarrage programmé le prochain jour ouvré.

- Planification : Tous les jours, exécuter de lundi à vendredi. Démarrage à : 21h00.
- Condition : **Ne pas démarrer pendant une connexion mesurée**.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

(1) S'il est 21h00 et que le périphérique n'est pas connecté à Internet via une connexion mesurée, la sauvegarde démarrera immédiatement.

(2) S'il est 21h00 et que le périphérique est connecté à Internet via une connexion mesurée, la sauvegarde démarrera le prochain jour ouvré.

(3) Si le périphérique est toujours connecté à Internet via une connexion mesurée à 21h00, la sauvegarde ne démarre jamais.

Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants

Empêche une sauvegarde (y compris une sauvegarde sur un disque local) si le périphérique est connecté à l'un des réseaux sans fil spécifiés. 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 chaîne dans leur nom, quelle que soit la casse. Par exemple, si utilisez « téléphone » comme nom de réseau, la sauvegarde ne démarrera pas lorsque le périphérique est connecté à l'un des réseaux suivants : « Téléphone de John », « téléphone_wifi » ou « mon_wifi_TÉLÉPHONE ».

Cette condition est pratique pour empêcher les sauvegardes lorsque le périphérique est connecté à Internet via une connexion mobile.

Mesure supplémentaire pour empêcher les sauvegardes via une connexion mobile : la condition **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants** est automatiquement activée 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 ». Vous pouvez supprimer ces noms de la liste en cliquant sur le symbole X.

Exemple

Les données sont sauvegardées dans un dossier réseau tous les jours ouvrés à 21h00. Si le périphérique est connecté à Internet via une connexion mobile (par exemple : un ordinateur portable est connecté en mode affilié), il est préférable d'ignorer la sauvegarde et d'attendre le démarrage programmé le prochain jour ouvré.

- Planification : Tous les jours, exécuter de lundi à vendredi. Démarrage à : 21h00.
- Condition : **Ne pas démarrer pendant une connexion aux réseaux Wi-Fi suivants**, **Nom du réseau** : <SSID du réseau>.
- Conditions de démarrage de la sauvegarde : **Ignorer la sauvegarde planifiée**.

En conséquence :

(1) S'il est 21h00 et que le périphérique n'est pas connecté au réseau spécifié, la sauvegarde démarrera immédiatement.

(2) S'il est 21h00 et que le périphérique est connecté au réseau spécifié, la sauvegarde démarrera le prochain jour ouvré.

(3) Si le périphérique est toujours connecté au réseau spécifié à 21h00, la sauvegarde ne démarre jamais.

Vérifier l'adresse IP du périphérique

Empêche une sauvegarde (y compris une sauvegarde sur un disque local) si l'une des adresses IP du périphérique est située dans 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**

Quelle que soit l'option, vous pouvez spécifier plusieurs plages. Prend en charge uniquement les adresses IPv4.

Cette condition est utile si un utilisateur est à l'étranger, elle permet d'éviter des frais élevés de transit de données. De plus, elle permet également d'éviter les sauvegardes via une connexion VPN (réseau virtuel privé).

Exemple

Les données sont sauvegardées dans un dossier réseau tous les jours ouvrés à 21h00. Si l'appareil est connecté au réseau de l'entreprise via un tunnel VPN (par exemple : l'utilisateur fait du télétravail), il est préférable d'ignorer la sauvegarde et d'attendre que l'utilisateur revienne avec son appareil au bureau.

- Planification : Tous les jours, exécuter de lundi à vendredi. Démarrage à : 21h00.
- Condition : **Vérifier l'adresse IP du périphérique**, **Démarrer si en dehors de la plage d'adresses IP**, **De** : <début de la plage d'adresses IP VPN>, **À** : <fin de la plage d'adresses IP VPN>.
- Conditions de démarrage de la sauvegarde : **Attendre que les conditions soient satisfaites**.

En conséquence :

(1) S'il est 21h00 et que l'adresse IP de la machine se situe en dehors de la plage spécifiée, la sauvegarde démarrera immédiatement.

(2) S'il est 21h00 et que l'adresse IP de la machine se situe dans la plage spécifiée, la sauvegarde démarrera dès que le périphérique obtiendra une adresse IP non VPN.

(3) Si l'adresse de la machine se situe toujours dans la plage spécifiée à 21h00, la sauvegarde ne démarre jamais.

Règles de rétention

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

1. Cliquez sur **Durée de conservation**.
2. Dans **Nettoyage**, sélectionnez l'une des options suivantes :
   - **Par âge des sauvegardes** (par défaut)
     Indiquez la durée de conservation des sauvegardes créées à partir du plan de protection. Par défaut, les règles de rétention sont spécifiées séparément pour chaque jeu de sauvegarde[1]. Si vous souhaitez utiliser une règle unique pour toutes les sauvegardes, cliquez sur **Passer à une règle unique pour tous les ensembles de sauvegarde**.
   - **Par nombre de sauvegardes**
     Indiquez le nombre maximum de sauvegardes devant être conservées.
   - **Par volume total de sauvegardes**
     Indiquez la taille maximale de sauvegardes devant être conservées.
     Ce paramètre n'est pas disponible avec le modèle de sauvegarde **Toujours incrémentielle (fichier unique)** ni lors de la sauvegarde sur un serveur SFTP ou sur un périphérique à bandes.
   - **Conserver les sauvegardes indéfiniment**
3. Sélectionnez quand débuter la tâche de nettoyage :

[1]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 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.

- **Après la sauvegarde** (par défaut)

  Les règles de rétention seront appliquées après la création d'une nouvelle sauvegarde.
- **Avant la sauvegarde**

  Les règles de rétention seront appliquées avant la création d'une nouvelle sauvegarde.

  Ce paramètre n'est pas disponible lors de la sauvegarde de clusters Microsoft SQL Server ou Microsoft Exchange Server.

Autres choses à savoir

- La dernière sauvegarde créée par le plan de protection est conservée dans tous les cas, sauf 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.

  Avertissement !
  Si vous supprimez la seule sauvegarde que vous possédez en appliquant de telles règles de rétention et que la sauvegarde échoue, vous ne disposerez d'aucune sauvegarde à partir de laquelle restaurer les données puisqu'il n'y aura plus aucune sauvegarde disponible.

- Les sauvegardes stockées sur des bandes ne sont pas supprimées tant que la bande n'est pas écrasée.
- Si, en fonction du modèle et du format de sauvegarde, chaque sauvegarde est stockée sous forme de fichier indépendant, ce fichier ne peut pas être supprimé tant que toutes ses sauvegardes (incrémentielle ou différentielle) n'ont pas expiré. Cela implique un espace de stockage supplémentaire pour les sauvegardes dont la suppression est différée. En outre, l'âge, le nombre ou la taille des sauvegardes peuvent être supérieurs aux valeurs que vous avez indiquées.

  Ce comportement peut être modifié à l'aide de l'option de sauvegarde « Consolidation de la sauvegarde ».
- Les règles de rétention font partie d'un plan de protection. Elles ne fonctionnent plus pour les sauvegardes d'une machine dès lors que le plan de protection est retiré de la machine ou supprimé, ou que la machine elle-même est supprimée du serveur de gestion. Si vous n'avez plus besoin des sauvegardes créées par le plan, supprimez-les comme décrit dans « Suppression de sauvegardes ».

Chiffrement

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.

Important
Il est impossible de restaurer les sauvegardes chiffrées si vous perdez ou oubliez le mot de passe.

Chiffrement dans un plan de protection

Pour activer le chiffrement, indiquez les paramètres de chiffrement lors de la création d'un plan de protection. Une fois un plan de protection appliqué, les paramètres de chiffrement ne peuvent pas être modifiés. Pour utiliser des paramètres de chiffrement différents, créez un nouveau plan de protection.

Spécification des paramètres de chiffrement dans un plan de protection

1. Dans le volet du plan de protection, activez le commutateur **Chiffrement**.
2. Indiquez et confirmez le mot de passe de chiffrement.
3. Sélectionnez l'un des algorithmes de chiffrement suivants :
   - **AES 128** – les sauvegardes sont chiffrées à l'aide de l'algorithme du standard de chiffrement avancé (AES) avec une clé de 128 bits.
   - **AES 192** – les sauvegardes sont chiffrées à l'aide de l'algorithme du standard de chiffrement avancé (AES) avec une clé de 192 bits
   - **AES 256** – les sauvegardes sont chiffrées à l'aide de l'algorithme du standard de chiffrement avancé (AES) avec une clé de 256 bits
4. Cliquez sur **OK**.

Chiffrement en tant que propriété de machine

Cette option est pensée pour les administrateurs gérant les sauvegardes de plusieurs machines. Si vous avez besoin d'un mot de passe de chiffrement unique pour chaque machine ou si vous devez activer le chiffrement des sauvegardes indépendamment des paramètres de chiffrement du plan de protection, enregistrez les paramètres de chiffrement individuellement sur chaque machine. Les sauvegardes sont chiffrées à l'aide de l'algorithme AES avec une clé de 256 bits.

L'enregistrement des paramètres de chiffrement sur une machine affecte les plans de protection comme suit :

- **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 qui seront appliqués ultérieurement à la machine.** Les paramètres de chiffrement enregistrés sur une machine ont priorité sur les paramètres de chiffrement d'un plan de protection. Toute sauvegarde sera chiffrée, même si le chiffrement est désactivé dans les paramètres du plan de protection.

Cette option peut être utilisée sur une machine exécutant l'agent pour VMware. Toutefois, soyez prudent si vous avez plus d'un agent pour VMware connecté au même vCenter Server. Il est obligatoire d'utiliser les mêmes paramètres de chiffrement pour l'ensemble des agents, parce qu'ils sont soumis à un type d'équilibrage de charge.

Après leur enregistrement, les paramètres de chiffrement peuvent être modifiés ou réinitialisés comme indiqué ci-dessous.

Important
Si un plan de protection en cours d'exécution sur cette machine a déjà créé des sauvegardes, la modification des paramètres de chiffrement entraînera l'échec de ce plan. Pour continuer à sauvegarder, créez un nouveau plan.

Enregistrement des paramètres de chiffrement sur une machine

1. Connectez-vous en tant qu'administrateur (sous Windows) ou utilisateur racine (sous Linux).
2. Exécutez le script suivant :
   - Sous Windows : `<chemin_installation>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<mot de passe_chiffrement>`
     Dans ce cas, `<chemin_installation>` est le chemin d'installation de l'agent de protection. Par défaut, il s'agit de **%ProgramFiles%\BackupClient** pour les déploiements dans le Cloud et de **%ProgramFiles%\Acronis** pour les déploiements sur site.
   - Sous Linux : **/usr/sbin/acropsh -m manage_creds --set-password** `<mot de passe_chiffrement>`

Réinitialisation des paramètres de chiffrement sur une machine

1. Connectez-vous en tant qu'administrateur (sous Windows) ou utilisateur racine (sous Linux).
2. Exécutez le script suivant :
   - Sous Windows : `<chemin_installation>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**
     Dans ce cas, `<chemin_installation>` est le chemin d'installation de l'agent de protection. Par défaut, il s'agit de **%ProgramFiles%\BackupClient** pour les déploiements dans le Cloud et de **%ProgramFiles%\Acronis** pour les déploiements sur site.
   - Sous Linux : **/usr/sbin/acropsh -m manage_creds --reset**

Pour modifier les paramètres de chiffrement à l'aide du composant Cyber Protect Monitor

1. Connectez-vous en tant qu'administrateur sous Windows ou macOS.
2. Cliquez sur l'icône **Cyber Protect Monitor** dans la zone de notification (sous Windows) ou dans la barre de menus (sous macOS).
3. Cliquez sur l'icône en forme d'engrenage.
4. Cliquez sur **Chiffrement**.
5. Effectuez l'une des actions suivantes :
   - Sélectionnez **Définir un mot de passe spécifique pour cette machine**. Indiquez et confirmez le mot de passe de chiffrement.
   - Sélectionnez **Utiliser les paramètres de chiffrement spécifiés dans le plan de protection**.
6. Cliquez sur **OK**.

Fonctionnement du chiffrement

L'algorithme de chiffrement AES fonctionne en mode Enchaînement des blocs (CBC) et utilise une clé générée de manière aléatoire avec une taille définie par l'utilisateur de 128, 192 ou 256 bits. Plus la taille de la clé est importante, plus le programme mettra de temps à chiffrer les sauvegardes et plus vos données seront sécurisées.

La clé de chiffrement est ensuite chiffrée avec AES-256 en utilisant un hachage SHA-256 du mot de passe en tant que clé. Le mot de passe lui-même n'est stocké nulle part sur le disque ou dans les sauvegardes ; le hachage du mot de passe est utilisé à des fins de vérification. Avec cette sécurité à deux niveaux, les données de sauvegarde sont protégées de tout accès non autorisé, mais il n'est pas possible de restaurer un mot de passe perdu.

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
- Si la destination de sauvegarde est un emplacement géré avec déduplication ou chiffrement activé(e)

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.

Conversion en une machine virtuelle

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

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.

Méthodes de conversion

- **Conversion régulière**
  Il existe deux façons de configurer une conversion régulière.
  - **Faire de la conversion une partie d'un plan de protection**
    La conversion sera effectuée après chaque sauvegarde (si elle est configurée pour l'emplacement principal) ou après chaque réplication (si elle est configurée pour le deuxième emplacement et d'autres emplacements).
  - **Créer un plan de conversion distinct**
    Cette méthode vous permet de spécifier une planification de la conversion distincte.
- **Récupération vers une nouvelle machine virtuelle**
  Cette méthode permet de choisir les disques à restaurer et d'ajuster les paramètres pour chaque disque virtuel. Utilisez cette méthode pour effectuer la conversion une fois ou occasionnellement, par exemple, pour réaliser une migration physique à virtuelle.

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 HC3 de Scale Computing, 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 HC3 de Scale Computing) 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 ci-dessous résume les types de machine virtuelle qui peuvent être exécutés par les agents :

Type de MV	Agent pour VMware	Agent pour Hyper-V	Agent pour Windows	Agent pour Linux	Agent pour Mac	Agent pour HC3 de Scale Computing
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware Workstation	+	+	+	+	–	–
Fichiers VHDX	+	+	+	+	–	–
HC3 de Scale Computing	–	–	–	–	–	+

Limites

- L'agent pour Windows, l'agent pour VMware (Windows) et l'agent pour Hyper-V ne peuvent pas convertir des sauvegardes stockées sur NFS.
- Les sauvegardes stockées sur NFS ou un serveur SFTP ne peuvent pas être converties en un plan de conversion séparé.
- Les sauvegardes stockées dans Secure Zone ne peuvent être converties que par l'agent exécuté sur le même ordinateur.
- Les sauvegardes ne peuvent être converties en machine virtuelle HC3 de Scale Computing que dans un plan de conversion séparé.
- 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 HC3 de Scale Computing, 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 vers ESXi et Hyper-V, par rapport à l'exécution d'une machine virtuelle à partir d'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 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.

Dans le second cas, les ressources sont utilisées uniquement lorsque 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 communique avec l'agent qui lit les données de la sauvegarde. De plus, la machine virtuelle est temporaire.

Conversion en machine virtuelle dans un plan de protection

Vous pouvez configurer la conversion en machine virtuelle à partir de n'importe quel emplacement de sauvegarde ou de réplication présent dans un plan de protection. La conversion sera effectuée après chaque sauvegarde ou réplication.

Pour des informations sur les prérequis et les limites, veuillez vous référer à « Ce que vous devez savoir à propos de la conversion ».

Configurer une conversion en machine virtuelle dans un plan de protection

1. Choisissez à partir de quel emplacement de sauvegarde vous voulez effectuer la conversion.
2. Dans le volet du plan de protection, cliquez sur **Convertir en MV** sous cet emplacement.
3. Activez le commutateur **Conversion**.
4. Dans **Convertir en**, sélectionnez le type de machine virtuelle cible. Vous pouvez sélectionner l'une des options suivantes :
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **Fichiers VHDX**
5. Effectuez l'une des actions suivantes :
   - Pour VMware ESXi et Hyper-V : 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. [Facultatif] Cliquez sur **Agent qui effectuera la conversion**, puis sélectionnez un agent.

   Il peut s'agir de l'agent qui effectue la sauvegarde (par défaut) ou d'un agent installé sur une autre machine. S'il s'agit du deuxième cas, la sauvegarde doit être stockée dans un emplacement partagé, tel qu'un dossier réseau, de façon à ce que l'autre machine puisse y accéder.
7. [Facultatif] Pour VMware ESXi et Hyper-V, vous pouvez également procéder comme suit :
   - 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.
   - Modifiez le mode d'allocation du disque. Le paramètre par défaut est **Dynamique** pour VMware ESXi et **En expansion dynamique** pour Hyper-V.
   - Cliquez sur **Paramètres de MV** pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.
8. Cliquez sur **Valider**.

Comment la conversion régulière vers une MV fonctionne

La façon dont les conversions régulières fonctionnent 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 au lieu de la créer de nouveau. 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 rien, 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 nouveau à partir de rien.

Instantanés intermédiaires

Pour être en mesure de mettre à jour la machine virtuelle, le logiciel stocke quelques instantanés intermédiaires de celle-ci. Ils sont nommés **Sauvegarde...** et **Réplica...** et doivent être conservés. Les instantanés qui ne sont plus nécessaires sont automatiquement supprimés.

Le dernier 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.

Les autres instantanés sont pour usage interne par le logiciel.

Réplication

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

Cette section décrit la réplication de sauvegarde dans le cadre d'un plan de protection. Pour plus d'informations sur la création d'un plan de réplication distinct, consultez la section « Traitement des données hors hôte ».

Si vous activez la réplication de sauvegardes, chaque sauvegarde est copiée vers un autre emplacement immédiatement après sa création. Si les sauvegardes antérieures n'étaient pas reproduites (par exemple, si la connexion réseau a été perdue), le logiciel reproduit également toutes les sauvegardes qui sont apparues après la dernière réplication réussie.

Les sauvegardes répliquées ne dépendent pas des sauvegardes de l'emplacement d'origine et vice versa. Vous pouvez restaurer des données à partir de n'importe quelle sauvegarde sans avoir accès à d'autres emplacements.

Exemples d'utilisation

- **Reprise d'activité après sinistre sûre**

  Stocker vos sauvegardes sur site (pour restauration immédiate) et hors site (pour sécuriser les sauvegardes en cas de défaillance du stockage local ou d'un désastre naturel).
- **Utilisation du stockage sur le 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**

  Supprimez les anciennes sauvegardes du stockage rapide conformément aux règles de rétention afin de ne pas abuser de l'espace de stockage dispendieux.

Emplacements pris en charge

Vous pouvez répliquer une sauvegarde *à partir* de n'importe lequel de ces emplacements :

- Un dossier local
- Un dossier réseau
- Secure Zone
- Un serveur SFTP
- Des emplacements gérés par un nœud de stockage

Vous pouvez répliquer une sauvegarde *vers* n'importe lequel de ces emplacements :

- Un dossier local
- Un dossier réseau
- Le stockage sur le Cloud
- Un serveur SFTP
- Des emplacements gérés par un nœud de stockage
- Un périphérique à bandes

Pour activer la réplication des sauvegardes

1. Dans le volet du plan de protection, cliquez sur **Ajouter un emplacement**.

   La commande **Ajouter un emplacement** s'affiche uniquement si la réplication est prise en charge *depuis* le dernier emplacement de sauvegarde ou de réplication sélectionné.
2. Spécifiez l'emplacement où les sauvegardes seront répliquées.
3. [Facultatif] Dans **Durée de conservation**, modifiez les règles de rétention de l'emplacement sélectionné, comme décrit dans la section « Règles de rétention ».
4. [Facultatif] Dans **Convertir en MV**, indiquez les paramètres pour la conversion en une machine virtuelle, comme expliqué dans la section « Conversion en une machine virtuelle ».

5. [Facultatif] Cliquez sur l'icône en forme d'engrenage > **Performance et créneau de sauvegarde**, puis définissez le créneau de sauvegarde pour l'emplacement choisi, comme décrit dans « Performance et créneau de sauvegarde ». Ces paramètres définiront la performance de réplication.
6. [Facultatif] Répétez les étapes 1 à 5 pour tous les emplacements où vous souhaitez répliquer les sauvegardes. Jusqu'à cinq emplacements sont pris en charge, y compris le principal.

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 en savoir plus sur ce plan en particulier, reportez-vous à "Réplication de sauvegarde" (p. 361).

Remarques pour les utilisateurs disposant de la licence Advanced

Conseil

Vous pouvez régler la réplication des sauvegardes *depuis* le stockage sur le Cloud en créant un plan de réplication séparé. Pour plus d'informations, consultez la section « Traitement des données hors hôte ».

Restrictions

- La réplication des sauvegardes *depuis* un emplacement géré par un nœud de stockage vers un dossier local n'est pas pris en charge. Un dossier local signifie un dossier sur la machine avec l'agent qui a créé la sauvegarde.
- La réplication des sauvegardes *vers* un emplacement géré avec déduplication activée n'est pas prise en charge pour les sauvegardes au format de sauvegarde **Version 12**.

Quelle Machine exécute l'opération ?

La réplication d'une sauvegarde *depuis* n'importe quel emplacement est initiée par l'agent ayant créé la sauvegarde et est effectuée :

- par cet agent si l'emplacement *n'est pas* géré par un nœud de stockage ;
- par le nœud de stockage correspondant si l'emplacement est géré. Toutefois, la réplication d'une sauvegarde depuis l'emplacement géré vers le stockage dans le Cloud est effectuée par l'agent qui a créé la sauvegarde.

Comme il ressort de la description ci-dessus, l'opération sera exécutée que si la machine avec l'agent est sous tension.

Réplication de sauvegardes entre emplacements gérés

La réplication d'une sauvegarde depuis un emplacement géré vers un autre est effectuée par le nœud de stockage.

Si la déduplication est activée pour l'emplacement cible (possiblement sur un autre nœud de stockage), le nœud de stockage source envoie seulement les blocs de données qui ne sont pas présents dans l'emplacement de stockage cible. En d'autres termes, comme un agent, le nœud de stockage effectue la déduplication à la source. Cela réduit le trafic sur le réseau lorsque vous répliquez des données entre des nœuds de stockage séparés géographiquement.

Démarrage manuel d'une sauvegarde

1. Sélectionnez une machine sur laquelle au moins un plan de protection est appliqué.
2. Cliquez sur **Sauvegarder**.
3. Si plus d'un plan de protection est appliqué, sélectionnez le plan de protection souhaité.
4. Effectuez l'une des actions suivantes :
   - Cliquez sur **Exécuter maintenant**. Une sauvegarde incrémentielle sera créée.
   - Si le modèle de sauvegarde comprend plusieurs méthodes de sauvegarde, vous pouvez choisir la méthode à utiliser. Cliquez sur la flèche du bouton **Exécuter maintenant**, puis sélectionnez **Complète, Incrémentielle** ou **Différentielle**.

La première sauvegarde créée par un plan de protection est toujours complète.

La progression de la sauvegarde s'affiche dans la colonne **Statut** de la machine.

Options de sauvegarde

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

Pour modifier les options de sauvegarde, cliquez sur l'icône en forme d'engrenage située à côté du nom du plan de protection, puis cliquez sur **Options de sauvegarde**.

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.

	Sauvegarde au niveau disque			Sauvegarde au niveau fichier			Machines virtuelles			SQL et Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Scale Computing	Windows
Alertes	+	+	+	+	+	+	+	+	+	+
Consolidation de sauvegarde	+	+	+	+	+	+	+	+	+	-
Nom du fichier de sauvegarde	+	+	+	+	+	+	+	+	+	+
Format de la sauvegarde	+	+	+	+	+	+	+	+	+	+
Validation de la sauvegarde	+	+	+	+	+	+	+	+	+	+
Changed Block Tracking (CBT)	+	-	-	-	-	-	+	+	+	+
Mode de sauvegarde de cluster	-	-	-	-	-	-	-	-	-	+
Niveau de compression	+	+	+	+	+	+	+	+	+	+
Notifications par messagerie électronique	+	+	+	+	+	+	+	+	+	+
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	+	+	+	-	-	-	-	-	-	-
Filtres de fichiers	+	+	+	+	+	+	+	+	+	-
Instantané de sauvegarde de niveau fichier	-	-	-	+	+	+	-	-	-	-
Troncation de journal	-	-	-	-	-	-	+	+	-	SQL uniquement
Prise d'instantanés LWM	-	+	-	-	-	-	-	-	-	-
Points de montage	-	-	-	+	-	-	-	-	-	-
Snapshot Multi-volume	+	+	-	+	+	-	-	-	-	-
Performance et créneau de sauvegarde	+	+	+	+	+	+	+	+	+	+
Envoi de données physiques	+	+	+	+	+	+	+	+	+	-
Commandes Pré/Post	+	+	+	+	+	+	+	+	+	+

Commandes de capture de données Pré/Post	+	+	+	+	+	+	+	-	-	+
Instantanés matériels SAN	-	-	-	-	-	-	+	-	-	-
Planification										
Répartir les heures de démarrage dans une fenêtre de temps	+	+	+	+	+	+	+	+	+	+
Limiter le nombre de sauvegardes simultanées	-	-	-	-	-	-	+	+	+	-
Sauvegarde secteur par secteur	+	+	-	-	-	-	+	+	+	-
Fractionnement	+	+	+	+	+	+	+	+	+	+
Gestion des bandes	+	+	+	+	+	+	+	+	+	+
Traitement de l'échec de tâche	+	+	+	+	+	+	+	+	+	+
Conditions de démarrage de tâche	+	+	-	+	+	-	+	+	+	+
Service de cliché instantané des volumes	+	-	-	+	-	-	-	+	-	+
Service de cliché instantané des	-	-	-	-	-	-	+	+	+	-

volumes (VSS) pour les machines virtuelles										
Sauvegarde hebdomadaire	+	+	+	+	+	+	+	+	+	+
Journal des événements Windows	+	-	-	+	-	-	+	+	+	+

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.

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 :

- La destination de la sauvegarde est un périphérique à bandes ou 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 des bandes ne peuvent pas être consolidées. 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. Les sauvegardes stockées sur une bande disparaissent de l'interface graphique uniquement lorsque la bande est réécrite ou effacée.

Nom de fichier de sauvegarde

Cette option définit le nom des fichiers de sauvegarde créés par le plan de protection.

Ces noms s'affichent dans le 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 traditionnel)
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)	

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.

Remarque
La date et l'heure sont ajoutées au nom de fichier de la sauvegarde uniquement dans la version 11 du format de sauvegarde.

Après avoir changé le nom d'un fichier de sauvegarde, la sauvegarde suivante sera une sauvegarde complète, sauf si vous spécifiez le nom d'une sauvegarde existante de la même machine. Dans ce cas, une sauvegarde complète, incrémentielle ou différentielle sera créée selon la planification des plans de protection.

Notez qu'il est possible de définir des noms de fichier de sauvegarde pour des emplacements qui ne peuvent être parcourus par un gestionnaire de fichiers (tel que le stockage sur le Cloud ou un périphérique à bandes). Cela est utile si vous souhaitez que les noms personnalisés s'affichent dans l'onglet **Stockage de sauvegarde**.

Où puis-je voir les noms des fichiers de sauvegarde ?

Sélectionnez l'onglet **Stockage de sauvegarde**, puis sélectionnez le groupe 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**.

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**).

Nom de fichier de sauvegarde par défaut

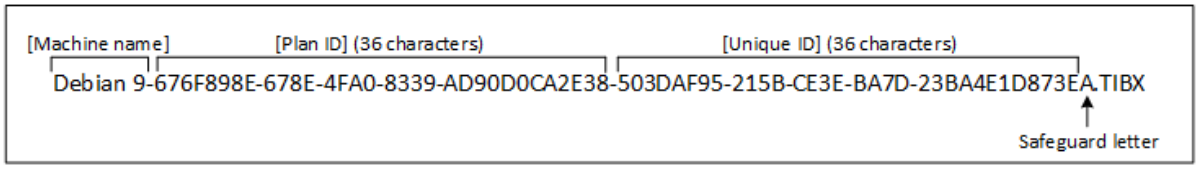
Le nom de fichier de sauvegarde par défaut est `[Nom de l'ordinateur]-[Identifiant du plan]-[Identifiant unique]A`.

Le nom de fichier de sauvegarde par défaut pour la sauvegarde de boîtes aux lettres est `[ID de la boîte aux lettres]_mailbox_[ID du plan]A`.

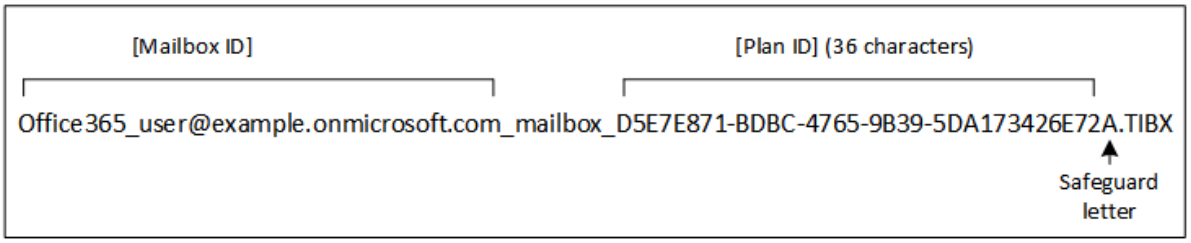
Le nom est constitué des variables suivantes :

- `[Nom de la machine]` Cette variable est remplacée par le nom de la machine (celui qui est affiché dans la console Web Cyber Protect) pour tous les types de données sauvegardées, à l'exception des boîtes aux lettres Microsoft 365. Pour les boîtes aux lettres Microsoft 365, elle est remplacée par le nom principal de l'utilisateur (UPN) de la boîte.
- `[Identifiant du plan]` Cette variable est remplacée par l'identificateur unique d'un plan de protection. Cette valeur ne change pas si le plan est renommé.
- `[Identifiant unique]` Cette variable est remplacée par l'identificateur unique de l'ordinateur ou de la boîte aux lettres sélectionnées. Cette valeur ne change pas si la machine est renommée ou si l'UPN de la boîte aux lettres change.
- `[Identifiant de la boîte aux lettres]` Cette variable est remplacée par l'UPN de la boîte aux lettres.
- « `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.



Le diagramme ci-dessous affiche le nom de fichier de sauvegarde par défaut pour les boîtes aux lettres.



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
...
```

Pour le format version 11 avec le modèle de sauvegarde **« Toujours incrémentielle (fichier unique) »** :

```
MyBackup.xml
MyBackup.tib
```

Pour le format version 11 avec d'autres modèles de sauvegarde :

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Utilisation de variables

Outre les variables utilisées par défaut, vous pouvez utiliser la variable `[Nom du plan]` qui est remplacée par le nom du plan de protection.

Si plusieurs ordinateurs ou boîtes aux lettres sont sélectionnés pour la sauvegarde, le nom du fichier de sauvegarde doit contenir la variable `[Nom de la machine]`, `[Identifiant de la boîte aux lettres]` ou `[Identifiant unique]`.

Nom de fichier de sauvegarde ou affectation simplifiée des noms des fichiers

En utilisant du texte brut ou des variables, vous pouvez créer les mêmes noms de fichier que dans les versions antérieures de Acronis Cyber Protect. Cependant, les noms de fichier simplifiés ne peuvent pas être reconstruits : dans la version 12, les noms de fichiers sont dotés d'un horodatage, sauf si un format sous forme d'un fichier unique est utilisé.

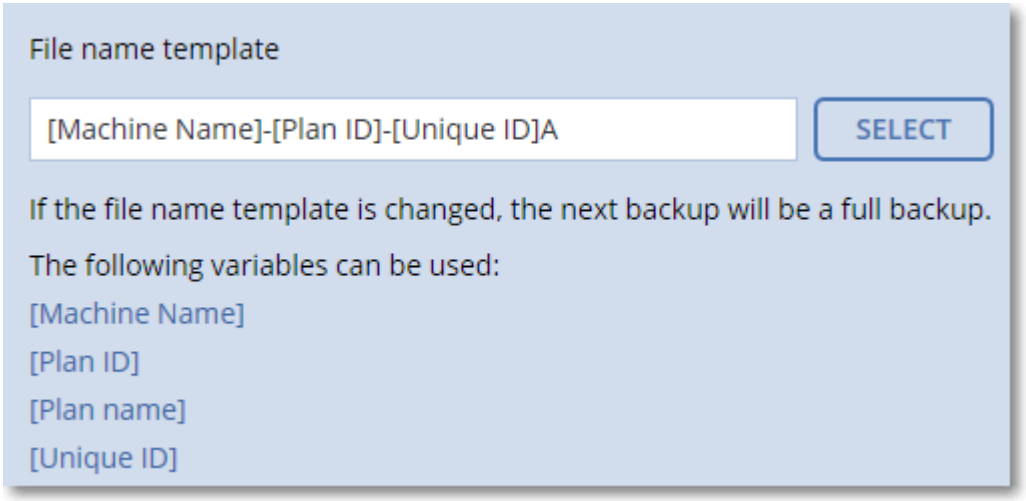
Exemples d'utilisation

- **Afficher des noms de fichier conviviaux**
  Vous voulez distinguer facilement les sauvegardes en parcourant l'emplacement de sauvegarde avec un gestionnaire de fichiers.

- **Continuer une série de sauvegardes existante**

  Supposons qu'un plan de protection soit appliqué à un seul ordinateur et que vous deviez supprimer ce dernier de la console Web Cyber Protect ou désinstaller l'agent avec ses paramètres de configuration. Lorsque la machine a été rajoutée ou que l'agent a été réinstallé, vous pouvez forcer le plan de protection à continuer les sauvegardes vers la même sauvegarde ou série de sauvegardes. Pour cela, dans les options de sauvegarde de votre plan de protection, cliquez sur **Nom de fichier de la sauvegarde**, puis sur **Sélectionner** pour sélectionner la sauvegarde souhaitée.

  Le bouton **Parcourir** affiche les sauvegardes à l'emplacement sélectionné dans la section **Où sauvegarder** du volet du plan de protection. Il ne peut rien parcourir en dehors de cet emplacement.



- **Mise à niveau à partir d'une version précédente du produit**

  Si, au cours de la mise à niveau, un plan de protection n'a pas migré automatiquement, recréez-le et faites-le pointer vers l'ancien fichier de sauvegarde. Si une seule machine est sélectionnée pour la sauvegarde, cliquez sur **Parcourir**, puis sélectionnez la sauvegarde requise. Si plusieurs machines sont sélectionnées pour la sauvegarde, recréez l'ancien nom de fichier de sauvegarde en utilisant des variables.

Remarque
Le bouton **Sélectionner** n'est disponible que pour les plans de protection créés pour et appliqués à un seul appareil.

Format de sauvegarde

Cette option définit le format des sauvegardes créées par le plan de protection. Elle est uniquement disponible pour les plans de protection qui utilisent le format de sauvegarde hérité version 11. Dans ce cas, vous pouvez le modifier et sélectionner le nouveau format version 12. Une fois cette modification effectuée, l'option devient inaccessible.

Cette option *n'est pas* effective pour les sauvegardes de boîte aux lettres. Les sauvegardes de boîte aux lettres sont toujours au nouveau format.

Le préréglage est le suivant : **Sélection automatique**.

Vous pouvez sélectionner l'une des options suivantes :

- **Sélection automatique**

  Le format Version 12 sera utilisé, sauf si le plan de protection ajoute des sauvegardes à celles créées par des versions antérieures du produit.
- **Version 12**

  Un nouveau format recommandé dans la plupart des cas pour la sauvegarde et la restauration. Chaque chaîne de sauvegarde (une sauvegarde complète ou différentielle et toutes les sauvegardes incrémentielles qui en dépendent) est enregistrée dans un fichier TIBX unique.

  Avec ce format, la règle de rétention **Par volume total de sauvegardes** n'est pas effective.
- **Version 11**

  Format hérité conservé pour une compatibilité descendante. Il vous permet d'ajouter des sauvegardes à celles créées par des versions antérieures du produit.

  Utilisez également ce format (avec n'importe quel modèle de sauvegarde, sauf **Toujours incrémentielle (fichier unique)**) si vous souhaitez que les sauvegardes complètes, incrémentielles et différentielles soient des fichiers séparés.

  Ce format est sélectionné automatiquement si la destination de la sauvegarde (ou de la réplication) est un emplacement géré avec déduplication activée ou un emplacement géré avec chiffrement activé. Si vous changez le format à la **Version 12**, les sauvegardes échoueront.

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.

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. Vous pouvez définir les noms de fichier en utilisant l'option Nom de fichier de la sauvegarde. 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 traditionnel)
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)	

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.
- Si la destination de la sauvegarde (ou de la réplication) est un emplacement géré avec déduplication activée, les sauvegardes échoueront.

Déduplication dans l'archive

Le format version 12 est compatible avec la déduplication dans l'archive.

La déduplication dans l'archive utilise la déduplication côté client et apporte 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.

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 validée immédiatement après sa création. Cette opération est effectuée par l'agent de protection.

Le préréglage est le suivant : **Désactivé**.

La validation calcule une somme de contrôle pour chaque bloc de données restauré depuis la sauvegarde. La seule exception est la validation des sauvegardes de niveau fichier se trouvant dans le stockage sur le Cloud. Ces sauvegardes sont validées en vérifiant la cohérence des métadonnées enregistrées dans la sauvegarde.

La validation est un processus très long, même pour les petites sauvegardes incrémentielles ou différentielles. Cette opération valide en effet les données physiques de la sauvegarde ainsi que toutes les données récupérables par la sélection de cette sauvegarde. Cela nécessite un accès aux sauvegardes précédemment créées.

Même si une validation réussie signifie une forte probabilité de restauration réussie, elle ne vérifie pas tous les facteurs ayant une incidence sur le processus de restauration. Si vous sauvegardez le système d'exploitation, nous vous recommandons d'effectuer une restauration d'essai avec le support de démarrage vers un disque dur de secours ou d'exécuter une machine virtuelle depuis la sauvegarde dans l'environnement ESXi ou Hyper-V.

Changed Block Tracking (CBT)

Cette option est effective pour les sauvegardes de niveau disque pour les machines virtuelles et physiques sous Windows. Cette option est également effective pour les sauvegardes de bases de données de Microsoft SQL Server et de 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 AlwaysOn (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 AlwaysOn (AAG) de Microsoft SQL Server. Pour que cette option prenne effet, l'agent pour SQL doit être installé sur tous

les nœuds AAG. Pour plus d'informations sur la sauvegarde des groupes de disponibilité AlwaysOn, consultez la section « Protection des groupes de disponibilité AlwaysOn (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.
- **Secondaire réplica**
  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

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

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.

Notifications par courrier électronique

Cette option vous permet de configurer des notifications par messagerie électronique au sujet d'événements qui se produisent au cours de la sauvegarde.

Cette option est disponible uniquement pour les déploiements sur site. Déploiement Cloud : les paramètres par défaut sont configurés par compte lorsqu'un compte est créé.

Le préréglage est le suivant : **Utiliser les paramètres système.**

Vous pouvez utiliser les paramètres système, ou les remplacer par des valeurs personnalisées qui seront spécifiques à ce plan. Les paramètres système sont configurés comme décrit dans la section « Notifications par messagerie électronique ».

Important
Lorsque les paramètres système sont modifiés, tous les plans de protection qui utilisent ces paramètres sont affectés.

Avant d'activer cette option, assurez-vous que les paramètres du **Serveur de messagerie** sont configurés.

Personnaliser les notifications par e-mail pour un plan de protection

1. Sélectionnez **Personnaliser les paramètres pour ce plan de protection**.
2. Dans le champ **Adresses électroniques des destinataires**, indiquez l'adresse électronique de destination. Vous pouvez saisir plusieurs adresses séparées par des points-virgules.
3. [Facultatif] Dans le champ **Objet**, modifiez l'objet de la notification par messagerie électronique. Vous pouvez utiliser les variables suivantes :
   - `[Alerte]` - résumé des alertes.
   - `[Terminal]` - nom du terminal.
   - `[Plan]` - nom du plan ayant généré l'alerte.
   - `[Serveur de gestion]` - nom d'hôte de l'ordinateur sur lequel le serveur de gestion est installé.
   - `[Unité]` - nom de l'unité à laquelle l'ordinateur appartient.

   L'objet par défaut est `[Alerte]` **Terminal :** `[Terminal]` **Plan :** `[Plan]`
4. Sélectionnez les cases à cocher correspondant aux événements pour lesquels vous souhaitez recevoir des notifications. Vous pouvez choisir dans la liste de toutes les alertes se produisant au cours d'une sauvegarde, regroupées par niveau de gravité.

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.

Par exemple, si la destination de sauvegarde sur le réseau devient inaccessible ou inatteignable, le programme essayera d'atteindre la destination toutes les 30 secondes, mais pas plus de 30 fois. Les tentatives s'arrêteront dès que la connexion sera rétablie OU que le nombre de tentatives sera atteint, suivant lequel de ces deux cas de figure se produit en premier.

Stockage dans le Cloud

Si le stockage sur le Cloud est sélectionné en tant qu'emplacement de sauvegarde, la valeur de l'option est automatiquement définie sur **Activé**. **Nombre de tentatives : 300**. **Intervalle entre les tentatives : 30 secondes.**

Dans ce cas, le nombre de tentatives est illimité, mais le délai avant l'échec de la sauvegarde est calculé comme suit : (300 secondes + **Intervalle entre les tentatives**) * (**Nombre de tentatives** + 1).

Exemples :

- Avec les valeurs par défaut, la sauvegarde échouera après (300 secondes + 30 secondes) * (300 + 1) = 99 330 secondes, soit environ 27,6 heures.
- Si vous définissez **Nombre de tentatives** à 1 et **Intervalle entre les tentative**s à 1 seconde, la sauvegarde échouera après (300 secondes + 1 seconde) * (1 + 1) = 602 secondes, soit environ 10 minutes.

Si le délai calculé dépasse 30 minutes et que le transfert des données n'a pas encore commencé, le délai réel est défini à 30 minutes.

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.

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

En utilisant les filtres de fichiers, vous pouvez inclure certains fichiers et dossiers dans une sauvegarde, ou en exclure d'une sauvegarde.

Sauf indication contraire, les filtres de fichiers sont disponibles à la fois pour une sauvegarde de niveau disque et de niveau fichier.

Les filtres de fichiers ne sont pas efficaces lorsqu'ils sont appliqués aux disques dynamiques (volumes LVM ou LDM) d'une machine virtuelle sauvegardée par Agent pour VMware, Agent pour Hyper-V ou Agent pour Scale Computing en mode sans agent.

Pour activer 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**.
4. Choisissez les options parmi celles décrites ci-dessous.

Inclure ou exclure des fichiers correspondant à des critères spécifiques

Il existe deux options qui fonctionnent de manière inversée.

- **Ne sauvegardez que les fichiers répondant aux critères suivants**
  Exemple : Si vous choisissez de sauvegarder l'ensemble de la machine en indiquant **C:\File.exe** dans les critères de filtre, seul ce fichier sera sauvegardé.

  Remarque
  Ce filtre ne fonctionne pas pour les sauvegardes de niveau fichier si **la version 11** est sélectionnée dans **Format de la sauvegarde** et si la destination de sauvegarde n'est pas le stockage dans le Cloud.

- **Ne sauvegardez pas les fichiers répondant aux critères suivants**

  Exemple : Si vous choisissez de sauvegarder l'ensemble de la machine en indiquant **C:\File.exe** dans les critères de filtre, seul ce fichier sera ignoré.

Vous avez la possibilité de choisir ces deux options à la fois. La dernière option prime sur la première, c'est-à-dire que si vous indiquez **C:\File.exe** dans les deux champs, ce fichier sera ignoré lors de la sauvegarde.

Critères :

- **Chemin complet**

  Spécifiez le chemin d'accès complet au fichier ou dossier, en commençant par la lettre du lecteur (lors de la sauvegarde de Windows) ou le répertoire racine (lors de la sauvegarde de Linux ou macOS).

  Sous Windows et Linux/macOS, vous pouvez utiliser une barre oblique dans le chemin du dossier ou du fichier (comme dans **C:/Temp/fichier.tmp**). Sous Windows, vous pouvez également utiliser la barre oblique inverse traditionnelle (comme dans **C:\Temp\fichier.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'affichera. En présence d'un filtre d'inclusion, la sauvegarde échouera.

  Un filtre de chemin d'accès complet inclut la lettre du lecteur (sous Windows) ou le répertoire racine (sous Linux ou macOS). Par exemple, un chemin d'accès de fichier complet peut être **C:\Temp\File.tmp**. Un filtre qui inclut la lettre du lecteur ou le répertoire racine (par exemple **C:\Temp\File.tmp** ou **C:\Temp***) entraînera un avertissement ou une erreur.

  Un filtre qui n'inclut pas 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'entraînera pas d'avertissement ni d'erreur. Toutefois, si le système d'exploitation de l'ordinateur sauvegardé n'est pas détecté correctement, ces filtres ne fonctionneront pas.

- **Nom**

  Spécifiez le nom du fichier ou du dossier, comme **Document.txt**. Tous les fichiers et dossiers portant ce nom seront sélectionnés.

Les critères *ne sont pas* sensibles à la casse. Par exemple, lorsque vous spécifiez **C:\Temp**, cela revient à sélectionner également **C:\TEMP**, **C:\temp**, , etc.

Vous pouvez utiliser un ou plusieurs caractères génériques (*, ** et ?) dans le critère. Ces caractères peuvent être utilisés à la fois dans le chemin d'accès complet et le nom du fichier ou du dossier.

L'astérisque (*) remplace zéro ou plusieurs caractères dans un nom de fichier. Par exemple, le critère **Doc*.txt** englobe les fichiers tels que **Doc.txt** et **Document.txt**.

[Uniquement pour le format **Version 12**] Le double astérisque (**) remplace zéro ou plusieurs caractères dans un nom de fichier et de chemin d'accès, 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**.

Le point d'interrogation (?) remplace exactement un seul caractère dans un nom de fichier. Par exemple, le critère **Doc?.txt** englobe les fichiers tels que **Doc1.txt** et **Docs.txt**, mais pas les fichiers **Doc.txt** ou **Doc11.txt**.

Exclure fichiers et dossiers masqués

Cochez cette case pour ignorer les fichiers et les dossiers qui ont l'attribut **Caché** (pour les systèmes de fichiers qui sont pris en charge par Windows) ou qui commencent par un point (.) (pour les systèmes de fichiers de Linux tels que Ext2 et Ext3). Si un dossier est caché, tout son contenu (y compris les fichiers qui ne sont pas cachés) sera exclu.

Exclure tous fich. et doss. système

Cette option est effective uniquement pour les systèmes de fichiers qui sont pris en charge par Windows. Sélectionnez cette case à cocher pour ignorer les fichiers et dossiers possédant l'attribut **Système**. Si un dossier a l'attribut **Système**, tout son contenu (y compris les fichiers qui n'ont pas l'attribut **Système**) sera exclu.

Remarque
Vous pouvez afficher les attributs de fichier ou dossier dans les propriétés du fichier/dossier ou en utilisant la commande attrib. Pour plus d'informations, consultez le Centre d'aide et de support dans Windows.

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.

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

Des activités malveillantes peuvent être menées sur une machine par des virus, des malware et des ransomware. Un autre cas nécessitant des investigations est le vol ou la modification de données sur une machine au moyen de divers programmes. Il se peut que de telles activités doivent être examinées, mais cela est possible uniquement si vous conservez une preuve numérique sur la machine que vous examinez. Malheureusement, il se peut que les preuves (fichiers, traces, etc.) soient supprimées ou qu'une machine devienne indisponible.

L'option de sauvegarde intitulée **Données d'investigation** vous permet de recueillir des preuves pouvant être utilisées dans les enquêtes d'investigation. Les éléments suivants peuvent servir de preuve numérique : un instantané d'un espace disque inutilisé, des vidages mémoire et un instantané de processus en cours d'exécution. La fonctionnalité **Données d'investigation** est disponible pour la sauvegarde d'une machine entière.

Actuellement, l'option **Données d'investigation** est disponible uniquement pour les machines Windows exécutant les versions de système d'exploitation suivantes :

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Remarque
• Une fois un plan de protection appliqué à un ordinateur avec un module de sauvegarde, les paramètres des données d'investigation ne peuvent pas être modifiés. Pour utiliser des paramètres de données d'investigation différents, créez un nouveau plan de protection.
• Les sauvegardes contenant un recueil de données d'investigation ne sont pas prises en charge pour les ordinateurs connectés à votre réseau via VPN et n'ont pas d'accès direct à Internet.

Les emplacements pris en charge pour les sauvegardes avec données d'investigation sont les suivants :

- Stockage dans le Cloud
- Dossier local

  Remarque
  1. Le dossier local est pris en charge uniquement sur un disque dur externe connecté via USB.
  2. Les disques dynamiques locaux ne sont pas pris en charge en tant qu'emplacement pour les sauvegardes d'investigation.

- Dossier réseau

Les sauvegardes avec données d'investigation sont automatiquement notarisées. Les sauvegardes d'investigation permettent aux enquêteurs d'analyser les zones de disque qui ne sont généralement pas incluses dans une sauvegarde de disque habituelle.

Processus de sauvegarde d'investigation

Le système effectue les opérations suivantes lors d'un processus de sauvegarde d'investigation :

1. Collecte le vidage mémoire brut et la liste des processus en cours d'exécution.
2. Redémarre automatiquement une machine dans le support de démarrage.
3. Crée la sauvegarde qui inclut aussi bien l'espace occupé que l'espace non alloué.
4. Notarise les disques sauvegardés.
5. Redémarre dans le système d'exploitation en ligne et poursuit l'exécution du plan (par exemple, réplication, rétention, validation et autre).

Pour configurer un recueil de données d'investigation

1. Dans la console Web Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**. Le plan de protection peut également être créé depuis l'onglet **Plans**.
2. Sélectionnez le périphérique et cliquez sur **Protéger**.
3. Dans le plan de protection, activez le module **Sauvegarde**.
4. Dans **Quoi sauvegarder**, sélectionnez **Toute la machine**.
5. Dans **Options de sauvegarde**, cliquez sur **Modifier**.
6. Trouvez l'option **Données d'investigation**.
7. Activez **Collecter des données d'investigation**. Le système recueillera automatiquement un vidage de mémoire et créera un instantané des processus en cours d'exécution.

   Remarque
   Il se peut que le vidage mémoire complet contienne des données sensibles telles que des mots de passe.

8. Précisez l'emplacement.

9. Cliquez sur **Exécuter maintenant** pour exécuter immédiatement une sauvegarde avec données d'investigation, ou attendez que la sauvegarde ait été créée selon la planification.
10. Accédez à **Tableau de bord** > **Activités**, vérifiez que la sauvegarde avec données d'investigation a bien été créée.

Par conséquent, les sauvegardes incluront les données d'investigation que vous pourrez récupérer et analyser. Les sauvegardes avec données d'investigation sont identifiées et peuvent être filtrées parmi d'autres sauvegardes dans **Stockage de sauvegarde** > **Emplacements** à l'aide de l'option **Uniquement avec les données d'investigation**.

Comment récupérer des données d'investigation à partir d'une sauvegarde ?

1. Dans la console Web Cyber Protect, accédez à **Stockage de sauvegarde** et sélectionnez l'emplacement avec les sauvegardes contenant des données d'investigation.
2. Sélectionnez la sauvegarde avec données d'investigation et cliquez sur **Afficher les sauvegardes**.
3. Cliquez sur **Restaurer** pour la sauvegarde avec données d'investigation.
   - Pour obtenir uniquement les données d'investigation, cliquez sur **Données d'investigation**. Le système affichera un dossier avec données d'investigation. Sélectionnez un fichier de vidage mémoire ou tout autre fichier d'investigation, et cliquez sur **Télécharger**.
   - Pour restaurer une sauvegarde d'investigation, cliquez sur **Machine complète**. Le système restaurera la sauvegarde sans mode de démarrage. Il sera donc possible de vérifier que le disque n'a pas été modifié.

Vous pouvez utiliser le vidage mémoire fourni avec plusieurs logiciels d'investigation tiers ; utilisez par exemple Volatility Framework sur https://www.volatilityfoundation.org/ pour une analyse plus complète de la mémoire.

Notarisation des sauvegardes avec les données d'investigation

Pour garantir qu'une sauvegarde avec données d'investigation correspond parfaitement à l'image qui a été prise et qu'elle n'a pas été compromise, le module 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.

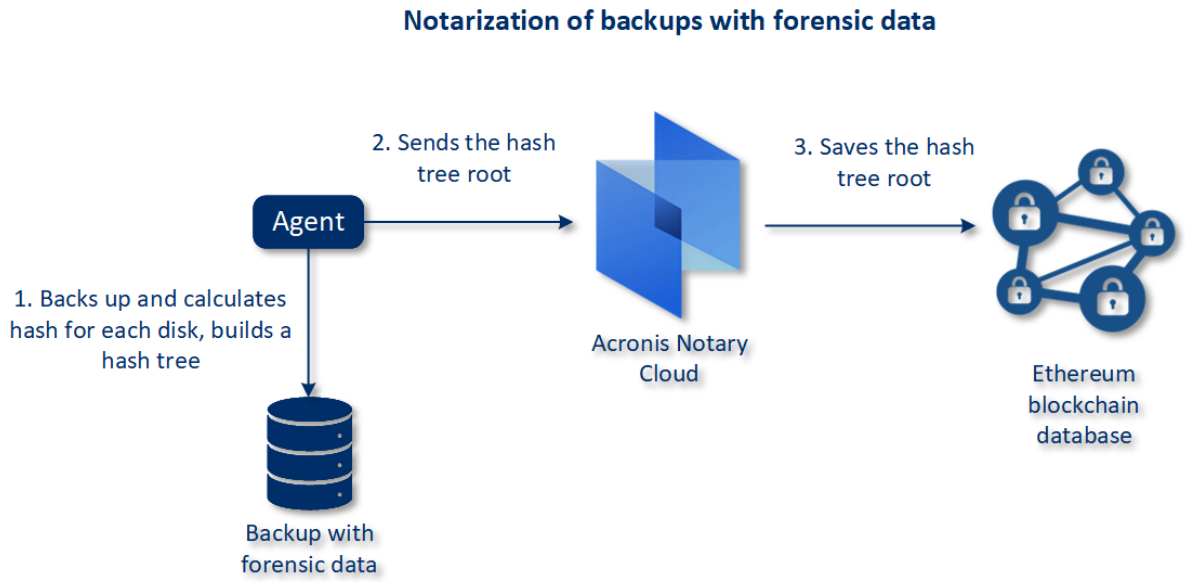
Lors d'une sauvegarde, l'agent calcule les codes de hachage des disques sauvegardés, crée un arbre de hachage, enregistre l'arbre dans la sauvegarde, puis envoie la racine de l'arbre de hachage au service Notary. Le service Notary enregistre la racine de l'arbre de hachage dans la base de données Blockchain 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.

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 Protect 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. Il se trouve dans le répertoire : `C:\Program Files\Acronis\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 :
  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
- obtenir le contenu
- calculer le hachage

list backups

Répertorie les points de récupérations dans une sauvegarde.

SYNOPSIS :

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Options

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> : le GUID de la sauvegarde.

<date> : la date de création de la sauvegarde. Son format est le suivant : 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 :

```
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>
```

<numéro> – identificateur du disque.

<taille> – taille in octets.

<statut_de_notarisation> – 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 récupération sur la sortie standard (stdout).

SYNOPSIS :

```
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 récupération à l'aide de l'algorithme SHA-256 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 Web. 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 »)

--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 Cloud. Par exemple, sous Windows, ce certificat est situé dans `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<nomd'utilisateur>.crt` où <nomd'utilisateur> – est le nom de compte nécessaire pour accéder à Cyber 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=MOT_DE_PASSE	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 :
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

Troncation de journal

Cette option est effective pour la sauvegarde des bases de données backup Microsoft SQL Server et la sauvegarde de niveau disque avec la sauvegarde de l'application Microsoft SQL Server activée.

Cette option définit si les journaux de transaction SQL Server sont tronqués après la réussite d'une 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 ce logiciel. Désactivez cette option si vous sauvegardez les journaux de transaction en utilisant le moteur de sauvegarde natif de Microsoft SQL Server. Vous pourrez appliquer les journaux de transaction après une restauration et ainsi restaurer une base de données à n'importe quel point dans le temps.

Prise d'instantanés LWM

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 volume n'est pas requis. Aussi, il est recommandé 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.

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.

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 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**.
- Si aucun ordinateur n'est sélectionné (c'est le cas lorsque vous commencez à créer un plan de protection depuis la page **Plans** > **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

La restauration en un seul clic permet aux utilisateurs de restaurer automatiquement la dernière sauvegarde de disque de leur machine. Il peut s'agir d'une sauvegarde de toute la machine, ou de

disques ou volumes spécifiques de cette machine.

Cette fonctionnalité est accessible sur la machine d'un utilisateur après activation par un administrateur, en association avec Startup Recovery Manager. L'administrateur peut réaliser cette opération uniquement via l'interface de ligne de commande. Pour en savoir plus sur la manière d'activer Startup Recovery Manager et la restauration en un seul clic, reportez-vous à la référence de la ligne de commande.

La restauration en un seul clic prend en charge les stockages de sauvegarde suivants :

1. Secure Zone
2. Stockage en réseau
3. Stockage dans le Cloud

Si un type de stockage spécifique n'est pas disponible ou s'il ne comporte aucune sauvegarde de disque, l'utilisateur est invité à utiliser le type de stockage suivant.

Si plus d'un jeu de sauvegardes (aussi appelé *archive*) contenant des sauvegardes de disque est disponible dans le stockage, la restauration en un seul clic sélectionne le jeu de sauvegardes mis à jour en dernier. L'utilisateur ne peut pas sélectionner un autre jeu de sauvegardes.

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 (aussi appelée *point de reprise*) au sein du jeu de sauvegardes sélectionné automatiquement

Restauration d'une machine à l'aide de la restauration en un seul clic

Prérequis

- Un administrateur a activé la restauration en un seul clic sur la machine sélectionnée.
- Il existe au moins une sauvegarde de disque de la machine sélectionnée.

Pour restaurer une machine

1. Redémarrez la machine que vous voulez restaurer.
2. Lors du redémarrage, appuyez sur F11 pour entrer dans Startup Recovery Manager.
3. Sélectionnez l'option de restauration en un seul clic souhaitée :
   - Pour restaurer automatiquement la dernière sauvegarde en date, appuyez sur 1 sur le clavier.
   - Pour restaurer une autre sauvegarde parmi le dernier jeu de sauvegardes mis à jour, appuyez sur 2 sur le clavier.
     - Pour sélectionner la sauvegarde souhaitée (aussi appelée *point de reprise*), appuyez sur le numéro correspondant sur le clavier.

L'interface graphique utilisateur démarre, puis disparaît. La procédure de restauration se poursuit sans cette interface.Une fois la restauration terminée, votre machine redémarre.

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 reprise du Cloud.

Vous pouvez configurer cette option séparément pour chaque emplacement spécifié dans le plan de protection. Afin de configurer cette option pour un emplacement de réplication, cliquez sur l'icône en forme d'engrenage située à côté du nom de l'emplacement, puis cliquez sur **Performance et créneau de sauvegarde**.

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 (validation, conversion vers une machine virtuelle) 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 de CPU : **Basse** (sous Windows, correspond à **Inférieure à la normale**).
- Vitesse de sortie : **Illimitée.**

Quand cette option est activée, les sauvegardes prévues sont autorisées ou bloquées en fonction des paramètres de performance précisés pour l'heure en cours. Au début d'une heure où les sauvegardes sont bloquées, un processus de sauvegarde s'arrête automatiquement et une alerte est générée.

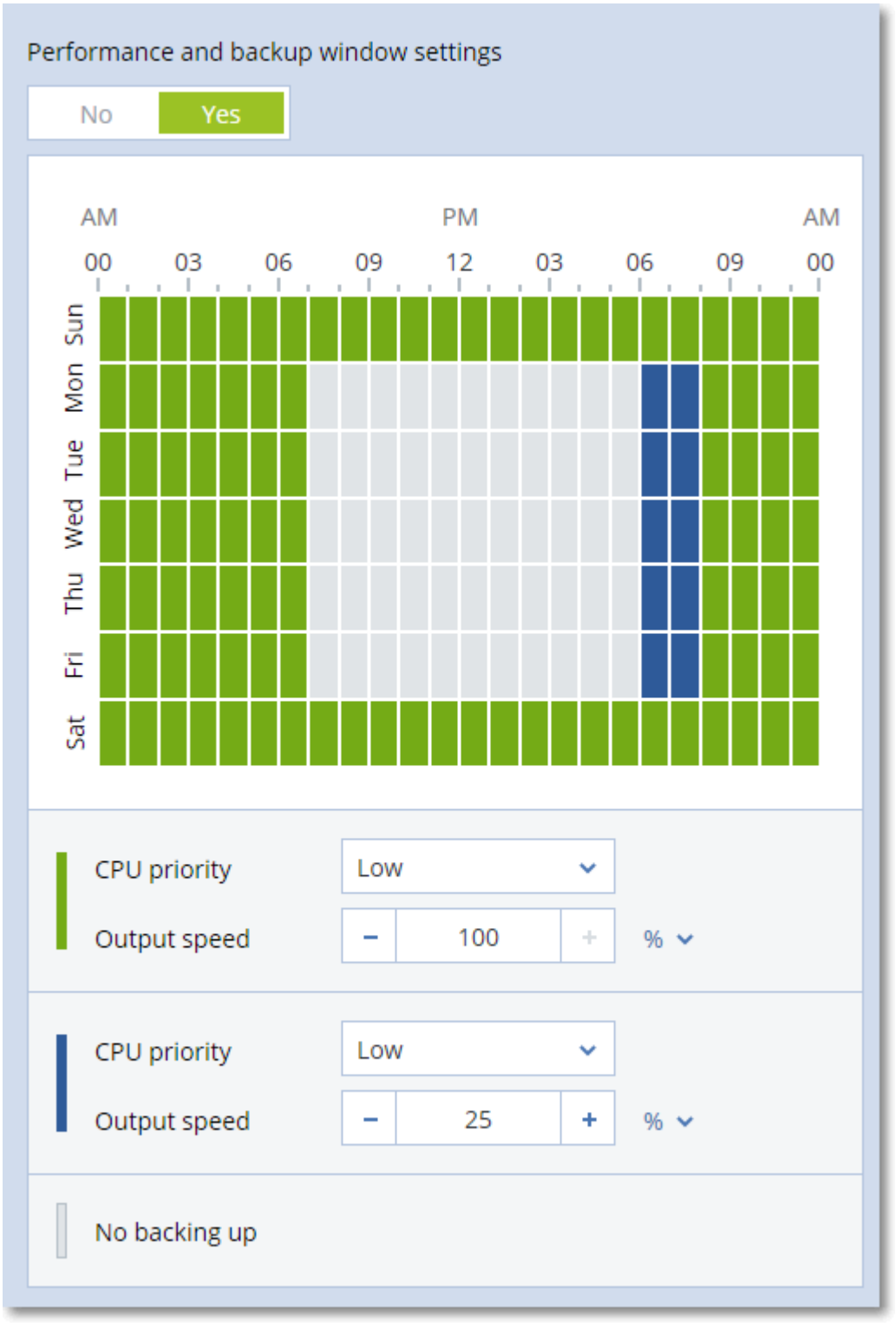
Même si les sauvegardes planifiées sont bloquées, une sauvegarde peut être démarrée manuellement. Cela utilisera les paramètres de performance de l'heure la plus récente où les sauvegardes sont autorisées.

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.



Priorité de CPU

Ce paramètre définit la priorité du processus de sauvegarde dans le système d'exploitation.

Les paramètres disponibles sont les suivants :

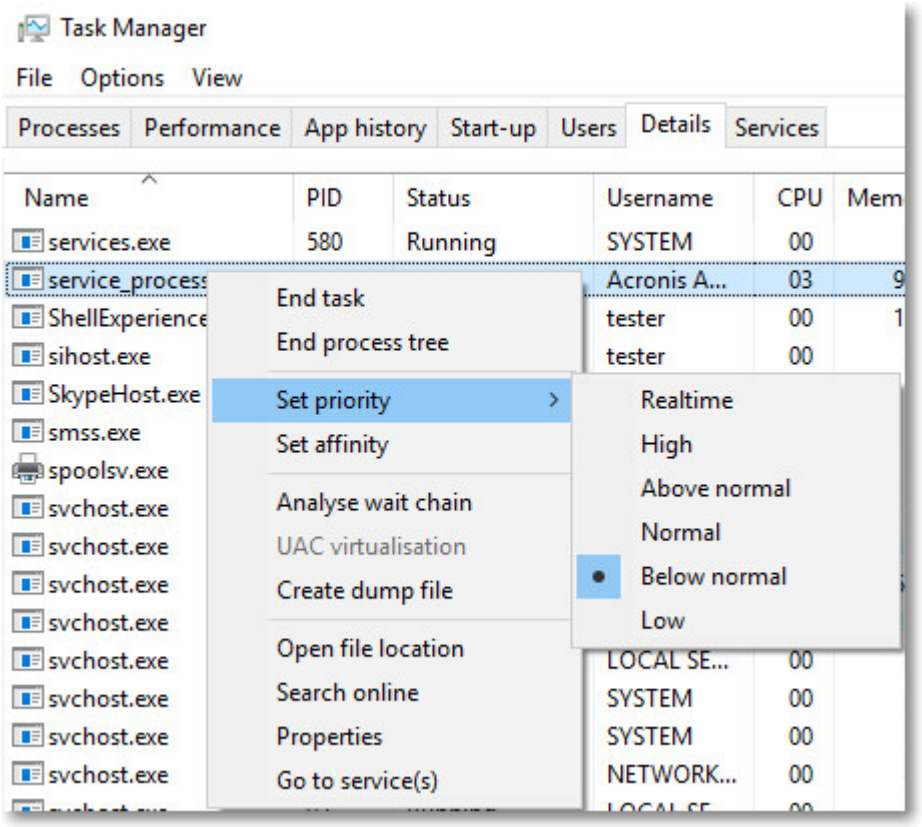
Basse - Sous Windows, correspond à **Inférieure à la normale**).

Normale - Sous Windows, correspond à **Normale**).

Élevée - Sous Windows, correspond à **Élevée**.

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 OS X.



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 effective si la destination de sauvegarde est le stockage sur 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 et l'agent pour Hyper-V. Les sauvegardes créées sous Bootable Media Builder ne sont pas prises en charge.

Cette option détermine si la première sauvegarde complète créée par le plan de protection sera envoyée 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 peuvent être effectuées via le réseau.

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 de l'organisation lors des déploiements sur site et pour les administrateurs lors des déploiements dans le Cloud.

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.

Présentation du processus d'envoi de données physiques

1. Créez un nouveau plan de protection. Dans ce plan, activez l'option de sauvegarde **d'envoi de données physiques**.

   Vous pouvez sauvegarder directement vers le lecteur ou sauvegarder vers un dossier local ou réseau, puis copier/déplacer la (les) sauvegarde(s) vers le lecteur.

   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.

2. 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, effectuez l'une des actions suivantes :

   - Lors des déploiements sur site : connectez-vous à votre compte Acronis, puis cliquez sur **Rendez-vous sur la Console de suivi** sous **Envoi de données physiques**.
   - Lors des déploiements Cloud : connectez-vous au portail de gestion, cliquez sur **Vue d'ensemble** > **Utilisation**, puis cliquez sur **Gérer le service** sous **Envoi de données physiques**.
3. Emballez les lecteurs et envoyez-les au centre de données.

   Important
   Assurez-vous de suivre les instructions d'emballage fournies dans le Guide de l'administrateur sur le service d'envoi de données physiques.

4. 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.

Le programme 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 / un fichier de traitement par lots à exécuter avant le démarrage du processus de sauvegarde

1. Activez le commutateur **Exécuter une commande avant la sauvegarde**.
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 **Valider**.

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.

Commande après la sauvegarde

Pour spécifier une commande / un fichier exécutable à exécuter une fois la sauvegarde terminée

1. Activez le commutateur **Exécuter une commande après la sauvegarde**.
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 sauvegarde 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 sauvegarde 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 sauvegarde. Vous pouvez retrouver le résultat de l'exécution de la commande en explorant l'onglet **Activités**.
6. Cliquez sur **Valider**.

Commandes de capture de données Pré/Post

L'option vous permet de définir les commandes à exécuter automatiquement avant et après la saisie des données (ce qui veut dire la prise d'instantané des données). La capture des données est exécutée au début de la procédure de sauvegarde.

Le modèle suivant illustre quand les commandes de capture de données avant/après sont exécutées.

<table>
<tr><td></td><td colspan="4"><---------- Sauvegarde ----------></td><td></td></tr>
<tr><td>Commandes avant la sauvegarde</td><td>Commande avant la capture de données</td><td>Capture des données</td><td>Commande après la capture de données</td><td></td><td>Commande après la sauvegarde</td></tr>
</table>

Si l'option Volume Shadow Copy Service est activée, l'exécution des commandes et les actions Microsoft VSS seront séquencées de la manière suivante :

Commandes « Avant la capture des données » -> Suspendre VSS -> Capture des données -> Reprendre VSS -> Commandes « Après la 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 / un fichier de traitement par lots à exécuter avant la capture des données

1. Activez le commutateur **Exécuter une commande avant la capture des données**.
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 **Valider**.

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	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

	échouer la sauvegarde si l'exécution de la commande échoue.			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 capture de données

Pour spécifier une commande / un fichier de traitement par lots à exécuter après la capture des données

1. Activez le commutateur **Exécuter une commande après la capture des données**.
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 **Valider**.

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	Effectuer la sauvegarde après l'exécution de la	Sans Objet	Continuer la sauvegarde en même temps que

	sauvegarde uniquement si la commande a été exécutée avec succès.	commande a été exécutée, indépendamment de l'échec ou du succès de l'exécution.		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.

Instantanés matériels SAN

Cette option est appliquée aux sauvegardes des machines virtuelles VMware ESXi.

Le préréglage est le suivant : **Désactivé**.

Cette option détermine l'utilisation des instantanés SAN lors de l'exécution d'une sauvegarde.

Si cette option est désactivée, le contenu du disque virtuel sera lu depuis un instantané VMware. L'instantané sera conservé pendant toute la durée de la sauvegarde.

Si cette option est activée, le contenu du disque virtuel sera lu depuis un instantané SAN. Un instantané VMware sera créé et conservé brièvement pour que l'état des disques virtuels soit cohérent. Si la lecture d'un instantané SAN n'est pas possible, la sauvegarde échouera.

Avant d'activer cette option, suivez les consignes répertoriées dans « Utilisation d'instantanés matériels SAN ».

Planification

Cette option définit si les sauvegardes commencent tel que planifié ou en différé, et combien de machines sont sauvegardées simultanément.

Le préréglage est le suivant :

- Déploiement sur site : **Démarrer toutes les sauvegardes exactement comme planifié.**
- Déploiement Cloud : **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**

  Cette option est uniquement disponible si un plan de protection est appliqué à plusieurs machines virtuelles. Cette option définit combien de machines virtuelles un agent peut sauvegarder simultanément lors de l'exécution d'un plan de protection donné.

  Si, selon le plan de protection, l'agent doit commencer à sauvegarder plusieurs machines à la fois, il choisira deux machines. (Pour optimiser la performances de sauvegarde, l'agent essaie de faire correspondre les machines stockées sur différents stockages.) Dès que l'une des deux sauvegardes est terminée, l'agent choisit la troisième machine et ainsi de suite.

  Vous pouvez modifier le nombre de machines virtuelles que l'agent doit sauvegarder simultanément. La valeur maximale est 10. Toutefois, si l'agent exécute plusieurs plans de protection qui se chevauchent dans le temps, les nombres spécifiés dans leurs options sont additionnés. Vous pouvez limiter le nombre total de machines virtuelles qu'un agent peut sauvegarder simultanément, quel que soit le nombre de plans de protection en cours d'exécution.

  Les sauvegardes des machines virtuelles commenceront exactement comme planifié.

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**.

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

Cette option est efficace pour les modèles de sauvegarde **Toujours complète** ; **Complète hebdomadaire, Incrémentielle quotidienne** ; **Complète mensuelle, Différentielle hebdomadaire, Incrémentielle quotidienne (GFS)** et **Personnalisée**.

Cette option vous permet de sélectionner la méthode de fractionnement des sauvegardes volumineuses en fichiers plus petits

Le préréglage est le suivant : **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**
  Entrez la taille de fichier souhaitée ou sélectionnez-la à partir de la liste déroulante.

Gestion des bandes

Ces options sont effectives lorsque la destination de la sauvegarde est un périphérique à bandes.

Activez la restauration de fichiers à partir des sauvegardes de disques enregistrées sur bandes

Le préréglage est le suivant : **Désactivé**.

Si cette case est cochée, le logiciel crée, à chaque sauvegarde, des fichiers supplémentaires sur un disque dur de la machine à laquelle le périphérique à bandes est attaché. La restauration des fichiers à partir de sauvegardes de disques est possible tant que ces fichiers supplémentaires sont intacts. Les fichiers sont supprimés automatiquement lorsque la bande stockant les sauvegardes correspondantes est effacées, retirée ou écrasée.

L'emplacement des fichiers supplémentaires est le suivant :

- Sous Windows XP et Server 2003 : **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- Sous Windows 7 et les versions ultérieures de Windows : **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- Sous Linux : **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

L'espace occupé par ces fichiers supplémentaires dépend du nombre de fichiers dans la sauvegarde correspondante. Pour une sauvegarde complète d'un disque contenant environ 20 000 fichiers (sauvegarde de disque d'une station de travail type), les fichiers supplémentaires occupent environ 150 Mo. La sauvegarde complète d'un serveur contenant 250 000 fichiers peut produire environ 700 Mo de fichiers supplémentaires. Donc, si vous êtes certain de ne pas avoir besoin de restaurer des fichiers individuels, vous pouvez laisser la case désactivée pour économiser de l'espace disque.

Si les fichiers supplémentaires n'ont pas été créés lors de la sauvegarde ou qu'ils ont été supprimés, vous pouvez toujours les créer en effectuant une nouvelle analyse des bandes sur lesquelles est stockée la sauvegarde.

Déplacer une bande vers le logement après chaque sauvegarde réussie de chaque machine

Le préréglage est le suivant : **Activé**.

Si vous désactivez cette option, une bande restera dans le lecteur après qu'une opération utilisant la bande est terminée. Autrement, le logiciel déplacera la bande vers la prise de connecteur dans laquelle elle se trouvait avant l'opération. Si, conformément au plan de protection, d'autres opérations suivent la sauvegarde (validation de la sauvegarde ou réplication sur un autre emplacement, par exemple), la bande sera replacée dans son logement à la fin de ces opérations.

Si cette option et l'option **Éjecter les bandes une fois les sauvegardes de chaque machine réussies** sont activées, la bande sera éjectée.

Éjecter les bandes après chaque sauvegarde réussie de chaque machine

Le préréglage est le suivant : **Désactivé**.

Lorsque cette case est cochée, le logiciel éjecte les bandes après toute sauvegarde correctement effectuée de chaque machine. Si, conformément au plan de protection, d'autres opérations suivent la sauvegarde (validation de la sauvegarde ou réplication sur un autre emplacement, par exemple), les bandes seront éjectées à la fin de ces opérations.

Écraser une bande dans le lecteur autonome lors de la création d'une sauvegarde complète

Le préréglage est le suivant : **Désactivé**.

L'option s'applique uniquement aux lecteurs de bandes autonomes. Lorsque cette option est activée, une bande insérée dans un lecteur est écrasée chaque fois qu'une sauvegarde complète est créée.

Utilisez les périphériques à bandes et les lecteurs suivants

Cette option vous permet de spécifier les lecteurs de bandes que doit utiliser le plan de protection.

Un pool de bandes contient des bandes provenant de tous les lecteurs de bandes attachés à un ordinateur, qu'il s'agisse d'un nœud de stockage ou d'un ordinateur sur lequel l'agent de protection est installé, ou les deux. Lors que vous sélectionnez un pool de bandes en tant qu'emplacement de sauvegarde, vous sélectionnez indirectement la machine à laquelle le(s) périphérique(s) à bandes est (sont) connecté(s). Par défaut, les sauvegardes peuvent être écrites sur les bandes via n'importe quel lecteur de bandes ou périphérique à bandes attaché à cette machine. Si certains lecteurs manquent ou ne sont pas opérationnels, le plan de protection utilisera ceux qui sont disponibles.

Vous pouvez cliquez sur **Uniquement périphériques et disques sélectionnés**, puis choisir les périphériques à bandes et les lecteurs de la liste. En sélectionnant un périphérique complet, vous sélectionnez tous ses lecteurs. Cela signifie que n'importe lequel de ces lecteurs peut être utilisé par

le plan de protection. Si le périphérique ou lecteur sélectionné manque ou n'est pas opérationnel, ou qu'aucun autre périphérique n'est sélectionné, la sauvegarde échouera.

En utilisant cette option, vous pouvez contrôler les sauvegardes exécutées par plusieurs agents vers une grosse bibliothèque de bandes contenant plusieurs lecteurs. Par exemple, la sauvegarde d'un gros serveur de fichier ou partage de fichiers peut ne pas démarrer si plusieurs agents sauvegardent leurs machines dans le même créneau de sauvegarde, car les agents occupent tous les lecteurs. Si vous autorisez les agents à utiliser, par exemple, les lecteurs 2 et 3, le lecteur 1 devient réservé à l'agent qui sauvegarde le partage.

Traitement en multi-flux

Le préréglage est le suivant : **Désactivé**.

Le traitement en multiflux vous permet de diviser les données d'un agent en plusieurs flux, puis d'écrire simultanément ces flux sur différentes bandes. Les sauvegardes sont plus rapides, ce qui est particulièrement utile lorsque le débit de l'agent est supérieur à celui du lecteur de bandes.

La case à cocher **Traitement en multiflux** est disponible uniquement lorsque vous sélectionnez plusieurs lecteurs de bandes dans l'option **Uniquement les terminaux et lecteurs sélectionnés**. Le nombre de lecteurs sélectionnés est égal au nombre de flux simultanés d'un agent. Si un lecteur sélectionné n'est pas disponible au démarrage d'une sauvegarde, cette dernière échoue.

Pour restaurer une sauvegarde multiflux ou une sauvegarde multiflux et multiplexée, vous avez besoin du même nombre de lecteurs que le nombre de lecteurs utilisés pour créer cette sauvegarde.

Vous ne pouvez pas modifier les paramètres de traitement en multiflux d'un plan de protection existant. Pour utiliser différents paramètres ou modifier les lecteurs de bandes sélectionnés, créez un nouveau plan de protection.

Le traitement en multiflux est disponible pour les lecteurs de bandes joints localement ou associés à un nœud de stockage.

Multiplexage

Le préréglage est le suivant : **Désactivé**.

Le traitement en multiflux vous permet d'écrire sur une seule bande des flux de données issus de plusieurs agents. Cela améliore l'utilisation des lecteurs de bandes rapides. Par défaut, le facteur de multiplexage, c'est-à-dire le nombre d'agents qui envoient des données à une seule bande, est défini sur deux. Vous pouvez augmenter cette valeur jusqu'à dix.

Le multiplexage est utile pour les environnements de grande taille comportant de nombreuses opérations de sauvegarde. Il n'améliore pas les performances d'une sauvegarde unique.

Pour obtenir la sauvegarde la plus rapide dans un environnement de grande envergure, vous devez analyser le débit des agents, du réseau et des lecteurs de bandes. Ensuite, définissez le facteur de multiplexage en conséquence, sans surmultiplexer. Par exemple, si les agents fournissent des

données à 70 Mbits/s, que la vitesse d'écriture du lecteur de bandes est de 250 Mbits/s et que le réseau ne comporte aucun goulot d'étranglement, définissez le facteur de multiplexage sur 3. Un facteur de multiplexage de 4 provoquera un sur-multiplexage et un affaiblissement des performances de sauvegarde. En général, le facteur de multiplexage est compris entre 2 et 5.

En raison de leur structure, les sauvegardes multiplexées sont plus lentes à récupérer. Plus le facteur de multiplexage est élevé, plus la récupération est lente. La récupération simultanée de plusieurs sauvegardes écrites sur une seule bande multiplexée n'est pas prise en charge.

Vous pouvez sélectionner un ou plusieurs lecteurs de bandes pour le multiplexage, ou utiliser l'option de multiplexage avec n'importe quel lecteur de bandes. Le multiplexage n'est pas disponible pour les lecteurs de bandes associés localement.

Vous ne pouvez pas modifier les paramètres de multiplexage d'un plan de protection existant. Pour utiliser des paramètres différents, créez un nouveau plan de protection.

Dans un plan de protection, les combinaisons suivantes de traitement en multiflux et de multiplexage sont possibles :

- **Les deux options de traitement en multiflux et de multiplexage sont désélectionnées.**
  Chaque agent envoie les données à un seul lecteur de bandes.
- **Seule l'option de traitement en multiflux est sélectionnée.**
  Chaque agent envoie les données à au moins deux lecteurs de bandes simultanément.
- **Seule l'option de multiplexage est sélectionnée.**
  Chaque agent envoie les données à un lecteur de bandes qui accepte les flux simultanés de plusieurs agents. Le nombre maximal de flux que peut accepter un lecteur de bandes est défini dans le plan de protection et ne peut pas être modifié à la volée.
- **Les deux options de traitement en multiflux et de multiplexage sont sélectionnées.**
  Chaque agent envoie les données à au moins deux lecteurs de bandes qui acceptent les flux simultanés de plusieurs agents.

Un lecteur de bandes ne peut écrire qu'un seul type de sauvegarde à la fois (multiplexée ou non multiplexée) selon le plan de protection démarré en premier.

Utiliser des ensembles de bandes au sein du même pool de bandes sélectionné pour la sauvegarde

Le préréglage est le suivant : **Désactivé**.

Les bandes à l'intérieur d'un pool peuvent être regroupées dans des **ensembles de bandes**.

Si cette option reste désactivée, les données sont sauvegardées sur toutes les bandes d'un pool. Si cette option est activée, vous pouvez séparer les sauvegardes selon les règles prédéfinies ou personnalisées.

- **Utiliser un ensemble de bandes distinct pour chacune** (choisissez une règle : **Type de sauvegarde**, **Type de périphérique**, **Nom du périphérique**, **Jour du mois**, **Jour de la semaine**, **Mois de l'année**, **Année**, **Date**)

  Si cette variante est sélectionnée, vous pouvez organiser les ensembles de bandes selon une règle prédéfinie. Par exemple, vous pouvez avoir des ensembles de bandes séparés pour chaque jour de la semaine ou stocker des sauvegardes de chaque machine sur un ensemble de bandes séparé.
- **Spécifier une règle personnalisée pour les ensembles de bandes**

  Si cette variante est sélectionnée, spécifiez votre propre règle pour organiser les ensembles de bandes. Cette règle peut contenir les variables suivantes :

Syntaxe des variables	Description des variables	Valeurs disponibles
`[Resource Name]`	Les sauvegardes de chaque machine seront stockées sur un ensemble de bandes séparé.	Nom des machines enregistrées sur le serveur de gestion.
`[Backup Type]`	Les sauvegardes complètes, incrémentielles et différentielles seront stockées sur des ensembles de bandes séparés.	`full`, `inc`, `diff`
`[Resource Type]`	Les sauvegardes des machines de chaque type sont stockées sur un ensemble de bandes séparé.	`Server essentials`, `Server`, `Workstation`, `Physical machine`, `VMware Virtual Machine`, `Virtual-PC Virtual Machine`, `Virtual Server Virtual Machine`, `Hyper-V Virtual Machine`, `Parallels Virtual Machine`, `XEN Virtual Machine`, `KVM Virtual Machine`, `RHEV Virtual Machine`, `Parallels Cloud Virtual Machine`
`[Day]`	Les sauvegardes créées chaque jour du mois seront stockées sur un ensemble de bandes séparé.	`01`, `02`, `03`... `31`
`[Weekday]`	Les sauvegardes créées chaque jour de la semaine seront stockées sur un ensemble de bandes séparé.	`Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`
`[Month]`	Les sauvegardes créées chaque mois de l'année seront stockées sur un ensemble de bandes séparé.	`January`, `February`, `March`, `April`, `May`, `June`, `July`, `August`, `September`, `October`, `November`, `December`
`[Year]`	Les sauvegardes créées chaque	`2017`, `2018`...

	année seront stockées sur un ensemble de bandes séparé.	

- Par exemple, si vous spécifiez la règle en tant que `[Resource Name]-[Backup Type]`, vous aurez un ensemble de bandes distinct pour chaque sauvegarde complète, incrémentielle et différentielle de chaque ordinateur auquel le plan de protection est appliqué.

Vous pouvez également spécifier les ensembles de bandes pour les bandes individuelles. Dans ce cas, le logiciel inscrira d'abord les sauvegardes sur les bandes dont la valeur de l'ensemble coïncide avec la valeur de l'expression spécifiée dans le plan de protection. Puis, si nécessaire, d'autres bandes du même pool seront prises. Après cela, si le pool peut être réapprovisionné, les bandes provenant du pool **Bandes libres** seront utilisées.

Par exemple, si vous spécifiez l'ensemble de bandes `Monday` pour la bande 1, `Tuesday` pour la bande 2, etc. et spécifiez `[Weekday]` dans les options de sauvegarde, la bande correspondante sera utilisée le jour respectif de la semaine.

Traitement de l'échec de tâche

Cette option détermine le comportement du programme lorsqu'un plan de protection programmé échoue. Cette option ne fonctionne pas lorsqu'un plan de protection est démarré manuellement.

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 arrête d'essayer dès qu'une tentative se termine avec succès OU que le nombre spécifié de tentatives est atteint, en fonction du suivant lequel de ces deux cas de figure qui se produit en premier.

Le préréglage est le suivant : **Désactivé**.

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 ».

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.

Service de cliché instantané des volumes

Cette option est valide uniquement pour les systèmes d'exploitation Windows.

L'option définit si un fournisseur de service de cliché instantané des volumes (VSS) doit notifier les applications compatibles avec VSS que la sauvegarde est sur le point de démarrer. Cela 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.

Le préréglage est le suivant : **Activé**. **Sélection automatique du fournisseur d'instantanés**.

Vous pouvez sélectionner l'une des options suivantes :

- **Sélection automatique du fournisseur d'instantanés**
  Sélection automatique parmi les fournisseurs d'instantanés matériels, logiciels et Microsoft Software Shadow Copy.
- **Utilisation du fournisseur de cliché instantané des logiciels Microsoft**
  Nous vous recommandons de choisir cette option lors de la sauvegarde de serveurs d'applications (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint ou Active Directory).

Désactivez cette option si votre base de données est incompatible avec VSS. Les instantanés sont plus rapides mais la cohérence des données des applications pour lesquelles les transactions ne sont pas complétées au moment de la prise de l'instantané ne peut pas être garantie. Vous pouvez utiliser les commandes de capture de données Pré/Post 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 élimineront tous les caches pour garantir que toutes les transactions sont terminées, et spécifiez des commandes après la capture de-données, qui remettront en service la base de données une fois que l'image statique est prise.

Remarque
Si cette option 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** 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.

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 niveau 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 » 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.

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 définit si les instantanés suspendus des machines virtuelles sont pris. Pour prendre un instantané de veille, le logiciel de sauvegarde applique VSS au sein d'une machine virtuelle en utilisant VMware Tools ou les services d'intégration Hyper-V.

Le préréglage est le suivant : **Activé**.

Si cette option est activée, les transactions de toutes les applications compatibles VSS s'exécutant sur une machine virtuelle sont effectuées avant la prise de l'instantané. Si un instantané suspendu échoue après le nombre de tentatives spécifié dans l'option « Gestion des erreurs », et si la sauvegarde de l'application est désactivée, un instantané non suspendu est pris. Si la sauvegarde d'application est activée, la sauvegarde échoue.

Si cette option est désactivée, un instantané non suspendu est pris. La machine virtuelle sera sauvegardée dans un état de panne. Nous vous recommandons de laisser cette option activée à tout moment, même pour les machines virtuelles qui n'exécutent pas d'applications compatibles VSS. Dans le cas contraire, même la cohérence de système de fichier ne peut être garantie au sein de la sauvegarde capturée.

Remarque
Cette option n'affecte pas les machines virtuelles HC3 de Scale Computing. 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.

Quoi restaurer	Méthode de restauration
Machine physique (Windows ou Linux)	Utilisation de l'interface Web Utilisation d'un support de démarrage
Machine physique (Mac)	Utilisation d'un support de démarrage
Machine virtuelle (VMware, Hyper-V ou HC3 de Scale Computing)	Utilisation de l'interface Web Utilisation d'un support de démarrage
Configuration ESXi	Utilisation d'un support de démarrage
Fichiers/Dossiers	Utilisation de l'interface Web 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 l'interface Web
Bases de données SQL	Utilisation de l'interface Web
Bases de données Exchange	Utilisation de l'interface Web
Boîtes aux lettres Exchange	Utilisation de l'interface Web
Boîtes aux lettres Microsoft 365	Utilisation de l'interface Web
Base de données Oracle	Utilisation de l'outil Oracle Explorer

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 emplacement différent, celle-ci n'est pas synchronisée avec iCloud et le fichier d'origine est indisponible.

Restauration sûre

Il est possible qu'une image sauvegardée d'un système d'exploitation soit infectée par un malware et puisse réinfecter la machine sur laquelle elle est restaurée.

La restauration sûre vous permet d'éviter la récurrence de telles infections grâce à une analyse anti-malwares intégrée et à la suppression des malwares lors du processus de restauration.

Limites :

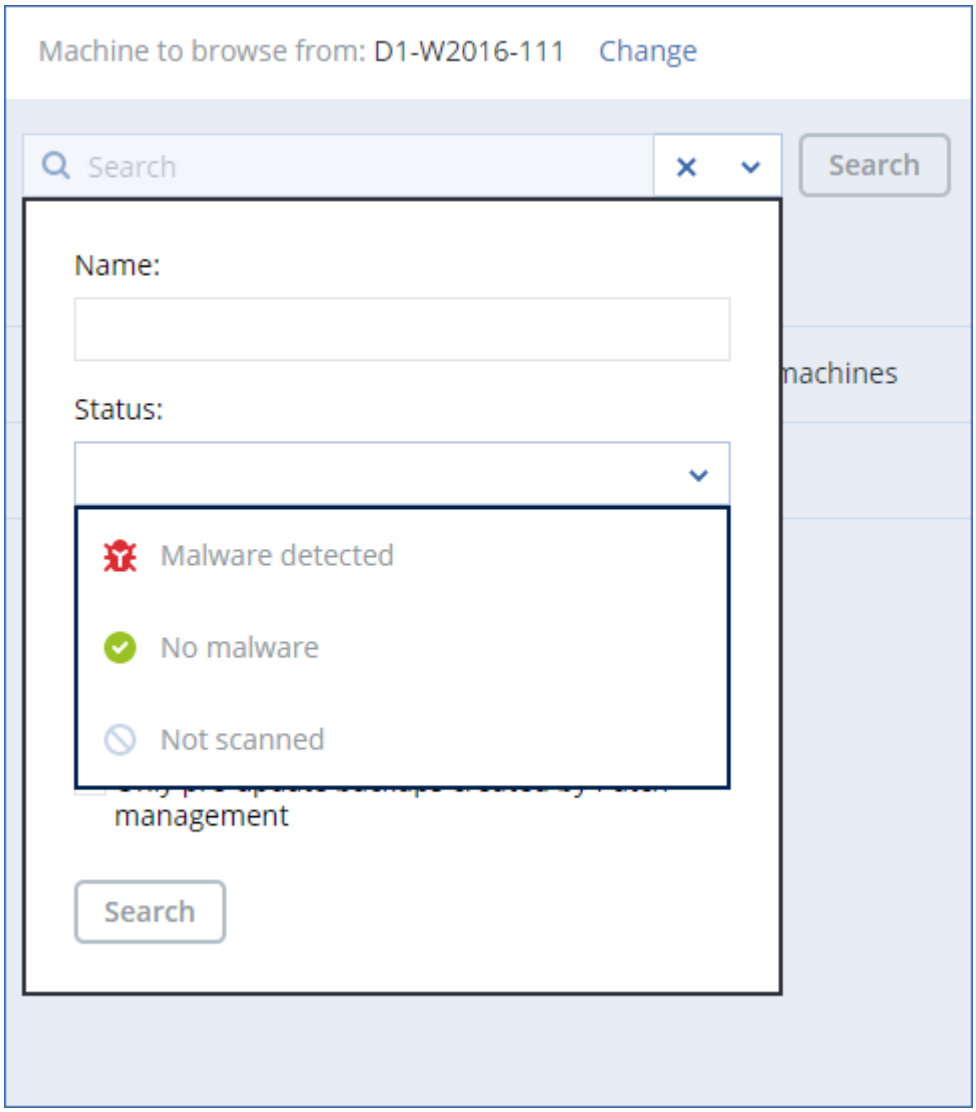
- La restauration sûre n'est prise en charge que pour les machines physiques et virtuelles Windows sur lesquelles l'agent pour Windows est installé.
- Seules les sauvegardes de type **Toute la machine** ou **Disques/volumes** sont prises en charge.
- Seuls les volumes dont le système de fichiers est NTFS sont pris en charge. Les partitions non-NTFS seront restaurées sans faire l'objet de l'analyse anti-malwares.
- La restauration sûre n'est pas prise en charge pour les sauvegardes CDP (Protection continue des données). Une machine sera restaurée en fonction de la dernière sauvegarde normale, sans les données de la sauvegarde CDP. Pour restaurer les données CDP, exécutez une restauration de **Fichiers/dossiers**.

Fonctionnement

Si vous activez l'option de restauration sûre lors du processus de restauration, le système effectuera les tâches suivantes :

1. Scanner la sauvegarde d'image à la recherche de malwares et marquer les fichiers infectés L'un des états suivants est attribué à la sauvegarde :
   - **Aucun malware :** aucun malware n'a été détecté dans la sauvegarde lors de l'analyse.
   - **Malware détecté :** un malware a été détecté dans la sauvegarde lors de l'analyse.
   - **Non analysé :** la sauvegarde n'a pas été analysée à la recherche de malwares.
2. Restaurer la sauvegarde de la machine sélectionnée
3. Supprimer le malware détecté

Vous pouvez filtrer les sauvegardes à l'aide du paramètre **État**.



Création d'un support de démarrage

Un support de démarrage correspond à un CD, un DVD, un lecteur flash USB ou tout autre support amovible qui permet d'exécuter l'agent, sans faire appel à un système d'exploitation. La fonction première d'un support de démarrage est de restaurer les systèmes d'exploitation qui ne démarrent pas.

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 sous Windows ou Linux

1. Télécharger le fichier ISO du support de démarrage. Pour télécharger le fichier, cliquez sur l'icône de compte dans le coin supérieur droit > **Téléchargements** > **Support de démarrage**.

2. Effectuez l'une des actions suivantes :
   - Gravez un CD/DVD avec le fichier ISO.
   - 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.
   - Connectez le fichier ISO à la machine virtuelle que vous souhaitez restaurer, comme s'il s'agissait d'un CD/DVD.

Vous pouvez également créer des supports de démarrage en utilisant Bootable Media Builder.

Pour créer un support de démarrage sur 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.

Restauration d'une machine

Restauration d'une machine physique

Cette section décrit la restauration d'une machine physique à l'aide de la console Web Cyber Protect.

Utilisez le support de démarrage plutôt que la console Web Cyber Protect si vous devez restaurer l'un des éléments suivants :

- Un système d'exploitation macOS
- Tout système d'exploitation de manière complète ou sur une machine hors ligne
- La structure des volumes logiques (volumes créés par Logical Volume Manager sous Linux). Le support vous permet de recréer automatiquement la structure des volumes logique.

La reprise d'un système d'exploitation et de volumes chiffrés avec BitLocker ou CheckPoint nécessite un redémarrage. Pour obtenir plus d'informations, consultez l'article "Restauration avec redémarrage" (p. 328).

Pour restaurer une machine physique

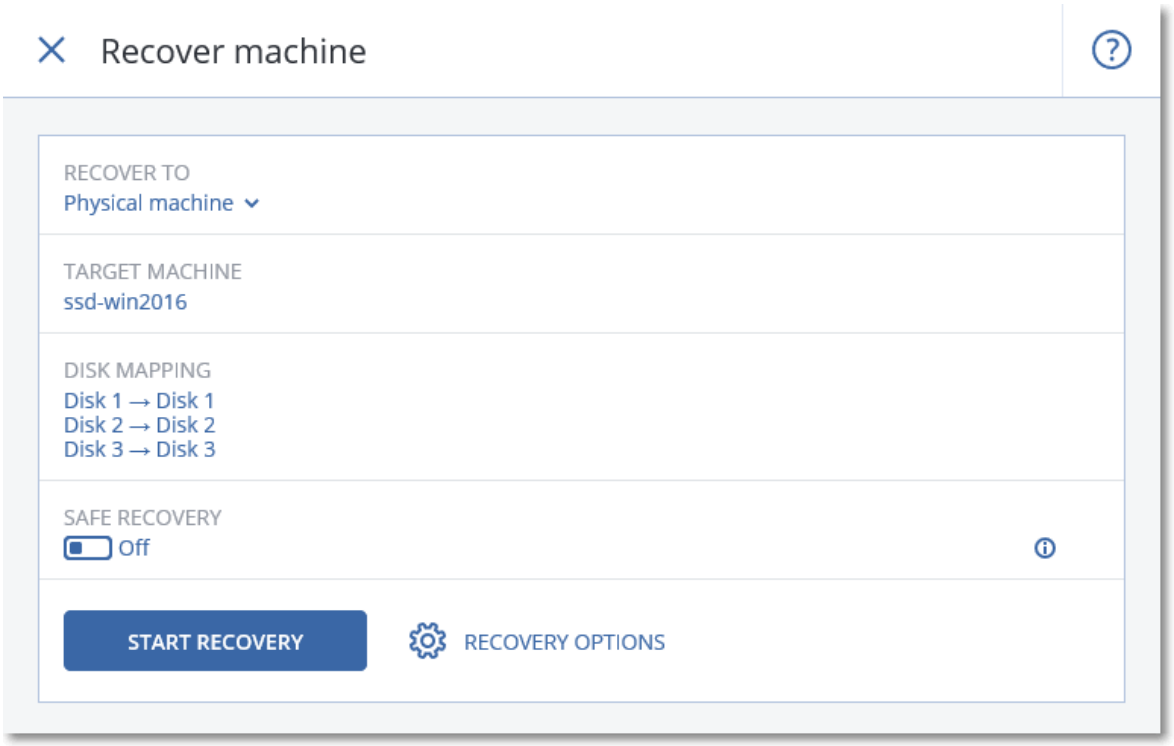
1. Sélectionnez la machine sauvegardée.
2. Cliquez sur **Restauration**.
3. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   Si la 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 une machine**, sélectionnez une machine cible qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
   - Restaurez la machine comme décrit dans « Restauration de disques avec un support de démarrage ».
4. Cliquez sur **Restaurer** > **Machine complète**.

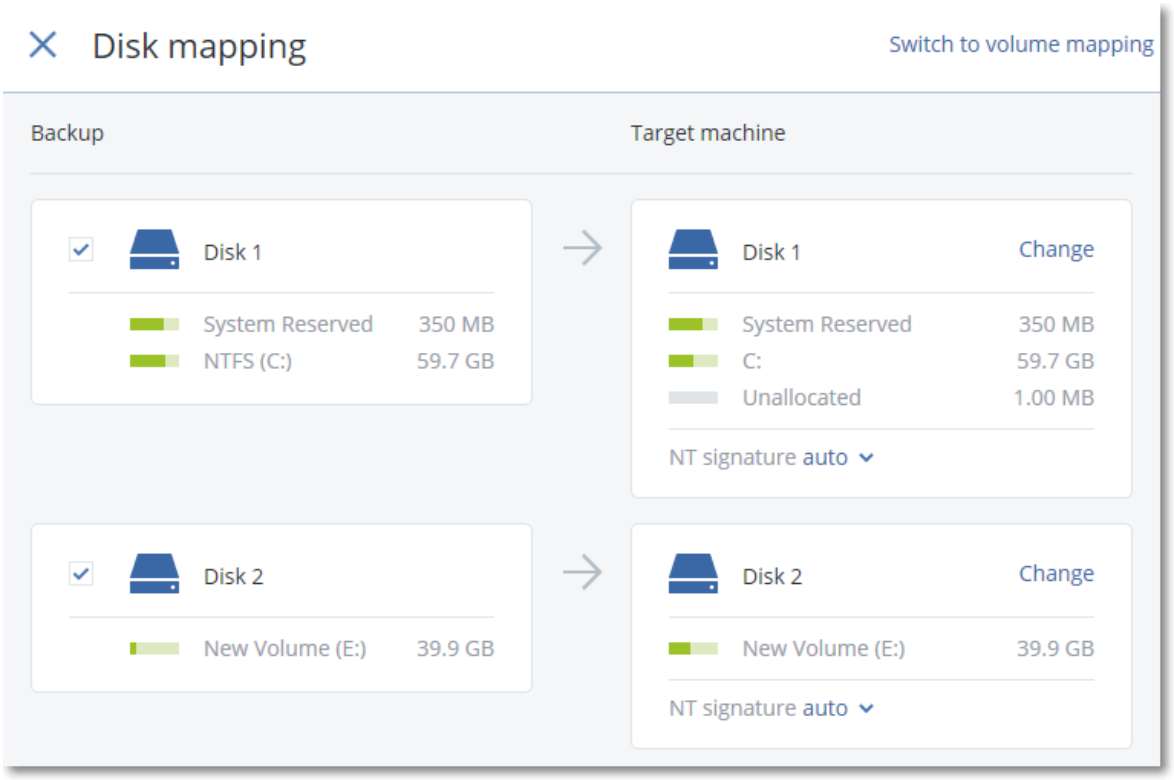
   Le logiciel mappe automatiquement les disques depuis la sauvegarde vers les disques de la machine cible.

   Pour effectuer une restauration sur une autre machine physique, cliquez sur **Machine cible**, puis sélectionnez une machine cible en ligne.



5. Si vous n'êtes pas satisfait du résultat du mappage ou si le mappage du disque échoue, cliquez sur **Mappage de disque** pour re-mapper les disques manuellement.

   Par ailleurs, dans la section Mappage, vous pouvez choisir les différents disques ou volumes à restaurer. Vous pouvez passer d'un disque ou d'un volume à l'autre à l'aide du lien **Basculer vers...** en haut à droite.



6. [Facultatif] Activez le commutateur **Restauration sûre** pour analyser la sauvegarde à la recherche de malwares. Si un malware est détecté, il sera identifié dans la sauvegarde et supprimé dès la fin du processus de restauration.
7. Cliquez sur **Démarrer la restauration**.
8. Confirmez que vous souhaitez écraser les données du disque avec leurs versions sauvegardées. Choisissez si vous souhaitez redémarrer automatiquement la machine.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Restauration d'une machine physique sur une machine virtuelle

Vous pouvez restaurer sauvegarde d'une machine physique sur une machine virtuelle.

La restauration vers une machine virtuelle est possible si au moins un agent pour l'hyperviseur cible pertinent est installé dans votre environnement et enregistré dans le serveur de gestion. Par exemple, une reprise vers VMware ESXi nécessite qu'un Agent pour VMware soit installé dans l'environnement et enregistré dans le serveur de gestion.

Certaines options ne sont disponibles qu'avec le déploiement dans le cloud.

Pour plus d'informations sur les chemins pris en charge pour la migration d'une machine physique vers une machine virtuelle (P2V), voir "Migration de machine" (p. 521).

Remarque
Vous ne pouvez pas restaurer des sauvegardes de machines physiques macOS en tant que machines virtuelles.

Restauration d'une machine physique en tant que machine virtuelle

1. Sélectionnez la machine 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 machine est hors-ligne, les points de restauration ne s'affichent pas. Effectuez l'une des actions suivantes :

   - Si la sauvegarde se trouve dans le cloud ou dans un stockage partagé (accessible par d'autres agents), cliquez sur **Sélectionner l'ordinateur**, sélectionnez un ordinateur en ligne, puis choisissez un point de reprise.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
   - Restaurez l'ordinateur en suivant les indications de "Restaurer des disques et des volumes via un support de démarrage" (p. 329).
4. Cliquez sur **Restaurer** > **Machine complète**.
5. Dans **Restaurer vers**, sélectionnez **Machine virtuelle**.
6. Cliquez sur **Machine cible**.
   a. Sélectionnez l'hyperviseur.

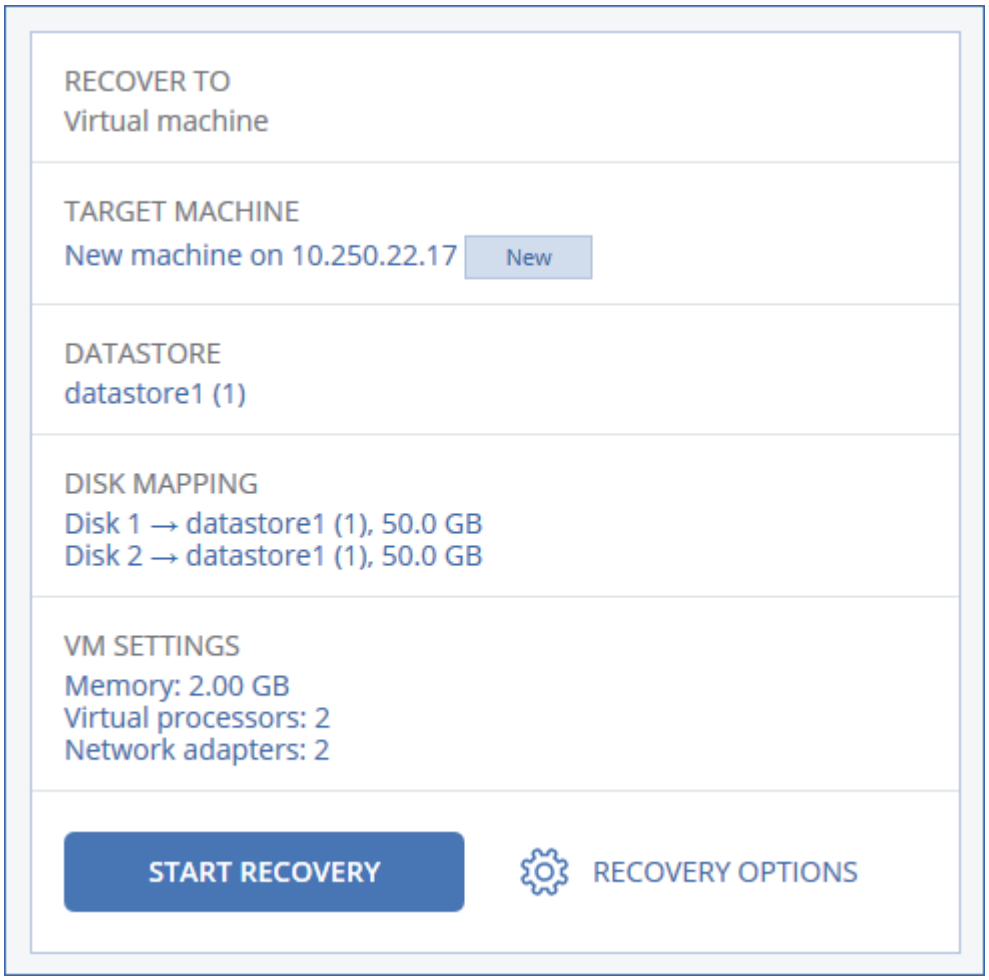
   Remarque
   Au moins un agent pour cet hyperviseur doit être installé dans votre environnement et enregistré dans le serveur de gestion.

   b. Sélectionnez si vous souhaitez restaurer sur une machine nouvelle ou existante. L'option de nouvel ordinateur est préférable, car elle ne nécessite pas de correspondance exacte entre la configuration de disque de la machine cible et celle de la sauvegarde.
   c. Sélectionnez l'hôte et spécifiez le nouveau nom de machine ou sélectionnez une machine cible existante.
   d. Cliquez sur **OK**.
7. [Pour Virtuozzo Hybrid Infrastructure] Cliquez sur **Paramètres de machine virtuelle**, puis sélectionnez **Variété**. Vous avez la possibilité de modifier la taille de la mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.
8. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options de reprise supplémentaires dont vous avez besoin :
   - [Non disponible pour Virtuozzo Hybrid Infrastructure et Scale Computing HC3] Pour sélectionner le magasin de données pour la machine virtuelle, cliquez sur **Magasin de données** pour ESXi, **Chemin d'accès** pour Hyper-V et Virtuozzo, ou **Domaine de stockage** pour Red Hat Virtualization (oVirt), puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.
   - Pour sélectionner le magasin de données (stockage), l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disque**. Dans la section

Mappage, vous pouvez choisir les différents disques à restaurer.

Remarque
Vous ne pouvez pas modifier ces paramètres si vous restaurez un conteneur Virtuozzo ou une machine virtuelle Virtuozzo Hybrid Infrastructure. Pour Virtuozzo Hybrid Infrastructure, vous pouvez uniquement sélectionner la stratégie de stockage pour les disques de destination. Pour cela, sélectionnez le disque de destination souhaité, puis cliquez sur **Modifier**. Dans la lame qui s'ouvre, cliquez sur l'icône en forme d'engrenage, sélectionnez la stratégie de stockage, puis cliquez sur **Terminé**.

- [Disponible pour VMware ESXi, Hyper-V, Virtuozzo et Red Hat Virtualization/oVirt] Pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle, cliquez sur **Paramètres de MV**.



9. Cliquez sur **Démarrer la restauration**.
10. [Lors de la restauration sur une machine virtuelle existante] Confirmez que vous souhaitez écraser les disques.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Restauration d'une machine virtuelle

Vous pouvez restaurer une sauvegarde de machine virtuelle sur une machine physique ou sur une autre machine virtuelle.

La restauration vers une machine virtuelle est possible si au moins un agent pour l'hyperviseur cible pertinent est installé dans votre environnement et enregistré dans le serveur de gestion. Par exemple, une reprise vers VMware ESXi nécessite qu'un Agent pour VMware soit installé dans l'environnement et enregistré dans le serveur de gestion.

Certaines options ne sont disponibles qu'avec le déploiement dans le cloud.

Pour plus d'informations sur les chemins pris en charge pour la migration d'une machine virtuelle vers une machine physique (V2P) ou d'une machine virtuelle vers une machine virtuelle (V2V), voir "Migration de machine" (p. 521).

Remarque
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.

Important
Pour restaurer une machine sur une machine virtuelle, vous devez arrêter cette machine virtuelle. Par défaut, le logiciel stoppe la machine sans invite. Une fois la reprise terminée, vous devrez redémarrer l'ordinateur manuellement. Vous pouvez modifier ce comportement par défaut à l'aide de l'option de restauration de gestion de l'alimentation de MV (cliquez sur **Options de récupération** > **Gestion de l'alimentation de MV**).

Pour restaurer une machine virtuelle

1. Effectuez l'une des actions suivantes :
   - Sélectionnez une machine sauvegardée, cliquez sur **Restauration**, puis sélectionnez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
2. Cliquez sur **Restaurer** > **Machine complète**.
3. [Lors de la restauration sur une machine physique] Dans **Restaurer vers**, sélectionnez **Machine physique**.
   La reprise vers une machine physique est uniquement possible si la configuration de disque de la machine cible correspond exactement à celle de la sauvegarde. Dans ce cas, passez à l'étape 4 dans "Restauration d'une machine physique" (p. 321). Sinon, nous vous recommandons d'effectuer une migration V2P (de machine virtuelle vers une machine physique) à l'aide d'un support de démarrage.
4. [Facultatif] Par défaut, l'ordinateur d'origine est sélectionné comme machine cible. Pour effectuer la restauration vers une autre machine virtuelle, cliquez sur **Machine cible**, puis

procédez comme suit :

a. Sélectionnez l'hyperviseur.

> **Remarque**
> Au moins un agent pour cet hyperviseur doit être installé dans votre environnement et enregistré dans le serveur de gestion.

b. Sélectionnez si vous souhaitez restaurer sur une machine nouvelle ou existante.

c. Sélectionnez l'hôte, puis spécifiez le nom de la nouvelle machine ou sélectionnez une machine cible existante.

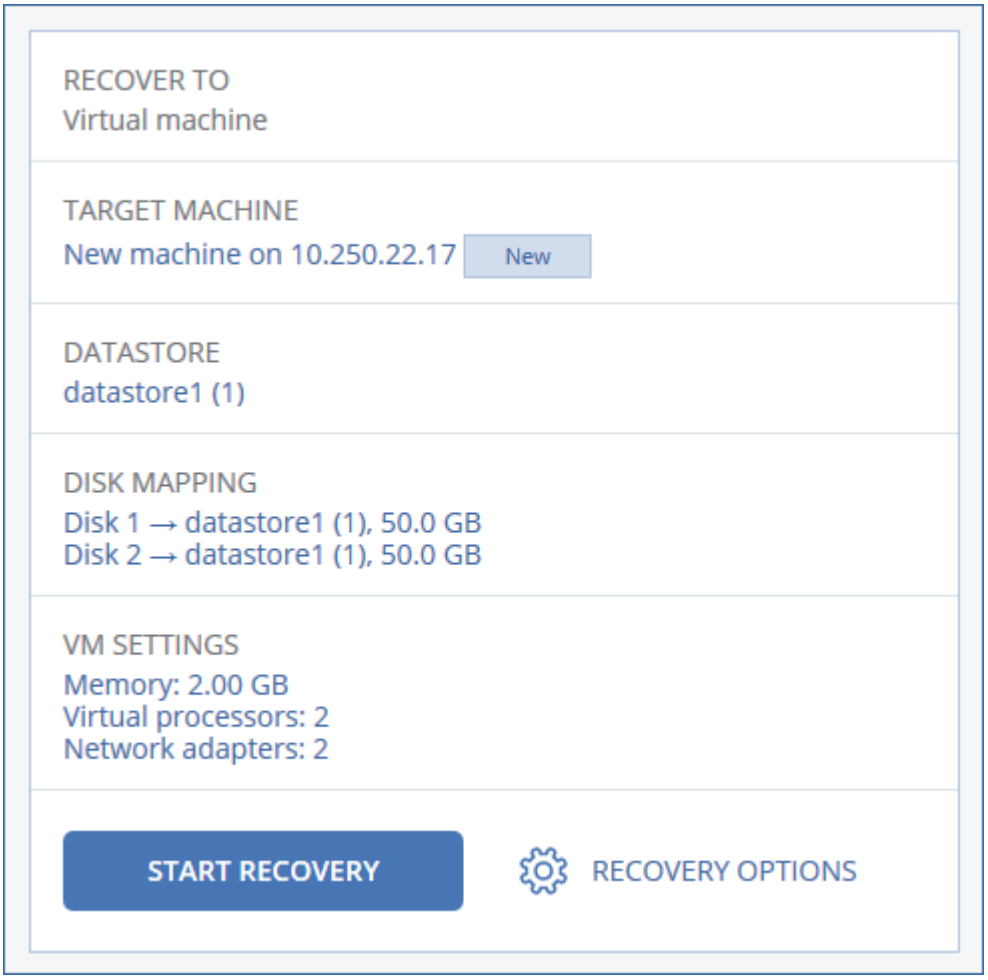
d. Cliquez sur **OK**.

5. [Pour Virtuozzo Hybrid Infrastructure] Cliquez sur **Paramètres de machine virtuelle**, puis sélectionnez **Variété**. Vous avez la possibilité de modifier la taille de la mémoire, le nombre de processeurs et les connexions réseau de la machine virtuelle.
6. [Facultatif] [Lors de la restauration sur un nouvel ordinateur] Configurez les options de reprise supplémentaires dont vous avez besoin :
   - [Non disponible pour Virtuozzo Hybrid Infrastructure et Scale Computing HC3] Pour sélectionner le magasin de données pour la machine virtuelle, cliquez sur **Magasin de données** pour ESXi, **Chemin d'accès** pour Hyper-V et Virtuozzo, ou **Domaine de stockage** pour Red Hat Virtualization (oVirt), puis sélectionnez le magasin de données (stockage) pour la machine virtuelle.
   - Pour sélectionner le magasin de données (stockage), l'interface et le mode de provisionnement de chaque disque virtuel, cliquez sur **Mappage de disque**. Dans la section Mappage, vous pouvez choisir les différents disques à restaurer.

     > **Remarque**
     > Vous ne pouvez pas modifier ces paramètres si vous restaurez un conteneur Virtuozzo ou une machine virtuelle Virtuozzo Hybrid Infrastructure. Pour Virtuozzo Hybrid Infrastructure, vous pouvez uniquement sélectionner la stratégie de stockage pour les disques de destination. Pour cela, sélectionnez le disque de destination souhaité, puis cliquez sur **Modifier**. Dans la lame qui s'ouvre, cliquez sur l'icône en forme d'engrenage, sélectionnez la stratégie de stockage, puis cliquez sur **Terminé**.

   - [Disponible pour VMware ESXi, Hyper-V, Virtuozzo et Red Hat Virtualization/oVirt] Pour modifier la taille de mémoire, le nombre de processeurs et les connexions réseau de la

machine virtuelle, cliquez sur **Paramètres de MV**.



7. Cliquez sur **Démarrer la restauration**.
8. [Lors de la restauration sur une machine virtuelle existante] Confirmez que vous souhaitez écraser les disques.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Restauration avec redémarrage

Un redémarrage est nécessaire lorsque vous restaurez les éléments suivants :

- Un système d'exploitation
- Des volumes chiffrés par BitLocker ou CheckPoint

Important
Les volumes chiffrés et sauvegardés sont restaurés comme volumes non chiffrés.

Configuration requise

- La reprise des volumes chiffrés nécessite la présence sur le même ordinateur d'un volume non chiffré disposant d'au moins 1 Go d'espace libre. Sinon, la reprise échouera.

- La reprise d'un volume système chiffré ne requiert aucune action supplémentaire. Pour restaurer un volume non-système chiffré, vous devez d'abord le verrouiller, par exemple en ouvrant un fichier qui y réside. Dans le cas contraire, la reprise se poursuit sans redémarrage et le volume récupéré risque de ne pas être reconnu par Windows.

Dépannage

Si la reprise échoue et que votre ordinateur redémarre avec l'erreur `Impossible d'obtenir le fichier de la partition`, désactivez le démarrage sécurisé. Pour en savoir plus sur la façon de procéder, consultez la section Désactivation du démarrage sécurisé dans la documentation Microsoft.

Restaurer des disques et des volumes via un support de démarrage

Pour en savoir plus sur la manière de créer un support de démarrage, consultez la section "Création d'un support de démarrage" (p. 320).

Pour restaurer des disques ou des volumes via un support de démarrage

1. Démarrez la machine cible par le biais d'un support de démarrage.
2. [Pour macOS uniquement] Si vous restaurez des volumes formatés APFS vers un ordinateur non d'origine ou vierge, recréez la configuration du disque d'origine manuellement :
   a. Cliquez sur **Utilitaire de disque**.
   b. Recréez la configuration du disque d'origine. Pour obtenir des instructions, consultez l'article https://support.apple.com/guide/disk-utility/welcome.
   c. Cliquez sur **Utilitaire de disque** > **Quitter l'utilitaire de disque**.

   Remarque
   À partir de macOS 11 Big Sur, le volume système ne peut pas être sauvegardé et restauré. Pour restaurer un système macOS amorçable, vous devez restaurer le volume de données, puis y installer macOS.
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 le nom d'hôte/l'adresse IP et le port de serveur proxy. Sinon, ignorez cette étape.
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 sur le Cloud**. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.

- Pour effectuer une restauration depuis un dossier local ou réseau, rendez-vous dans **Dossiers locaux** ou **Dossiers réseau**.

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.
9. Dans **Contenu des sauvegardes**, sélectionnez **Disques** ou **Volumes**, puis les éléments que vous souhaitez restaurer. Cliquez sur **OK** pour confirmer votre sélection.

   Important
   Si la machine sauvegardée dispose de disques dynamiques ou de volumes logiques (LWM), sélectionnez **Volumes**.

10. 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.

11. [Pour macOS uniquement] Pour restaurer un volume de données au format APFS en tant que système macOS amorçable, dans la **section Installation de macOS**, veillez à ce que la case **Installer macOS sur le volume de données macOS restauré** reste cochée.

    Après la récupération, le système redémarre et l'installation de macOS démarre automatiquement. Vous avez besoin d'une connexion Internet pour que le programme d'installation télécharge les fichiers nécessaires.

    Si vous n'avez pas besoin de restaurer le volume de données au format APFS en tant que système amorçable, désélectionnez la case **Installer macOS sur le volume de données macOS restauré**. Vous pourrez toujours rendre ce volume amorçable ultérieurement en y installant macOS manuellement.
12. [Pour Linux uniquement] Si la machine sauvegardée possède des volumes logiques (LWM) 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.
    c. Confirmez votre choix :
13. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
14. Cliquez sur **OK** pour démarrer la restauration.

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 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 périphérique 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 périphérique contenant les pilotes quand vous travaillez en utilisant un support de démarrage. Utilisez un support basé sur WinPE si le périphérique 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 :

- 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 l'adaptateur 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 périphérique 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.

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.

Restauration des fichiers

Restauration de fichiers via l'interface Web

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 récupération.
   - Sélectionnez un point de récupération 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. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers et des dossiers requis.

   Vous pouvez utiliser un ou plusieurs caractères génériques (* et ?). Pour plus de détails sur l'utilisation de caractères génériques, consultez la section « Filtres de fichiers »

   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.
8. Cliquez sur **Restaurer**.

   Dans **Restaurer vers**, vous voyez l'une des options suivantes :

   - La machine sur laquelle les fichiers que vous souhaitez restaurer étaient initialement présents (si un agent est installé sur cette machine).
   - L'ordinateur où est installé l'agent pour VMware, Hyper-V ou Scale Computing HC3 (si les fichiers proviennent d'une machine virtuelle ESXi, Hyper-V ou Scale Computing HC3).

   Il s'agit de la machine cible pour la restauration. Vous pouvez sélectionner une autre machine, le cas échéant.

9. Dans **Chemin d'accès**, sélectionnez la destination de la restauration. Vous pouvez sélectionner l'une des options suivantes :
   - l'emplacement d'origine (lors d'une restauration vers la machine d'origine)
   - un dossier local sur la machine cible

     Remarque
     Les liens symboliques ne sont pas pris en charge.

   - un dossier réseau accessible depuis la machine cible
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**

La progression de la restauration sont affichées dans l'onglet **Activités**.

Téléchargement de fichiers depuis le Cloud

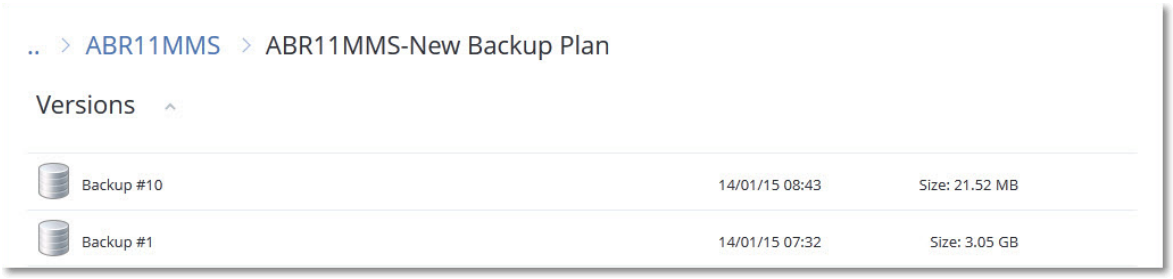
Vous pouvez explorer le stockage Cloud, consulter les contenus des sauvegardes et télécharger les fichiers dont vous avez besoin.

Limites

- les sauvegardes des états du système, de SQL, des bases de données et des bases de données Exchange ne sont pas consultables.
- Pour une meilleure expérience de téléchargement, ne téléchargez pas plus de 100 Mo à la fois. Pour récupérer rapidement de plus grandes quantités de données depuis le Cloud, utilisez la procédure de récupération de fichiers.

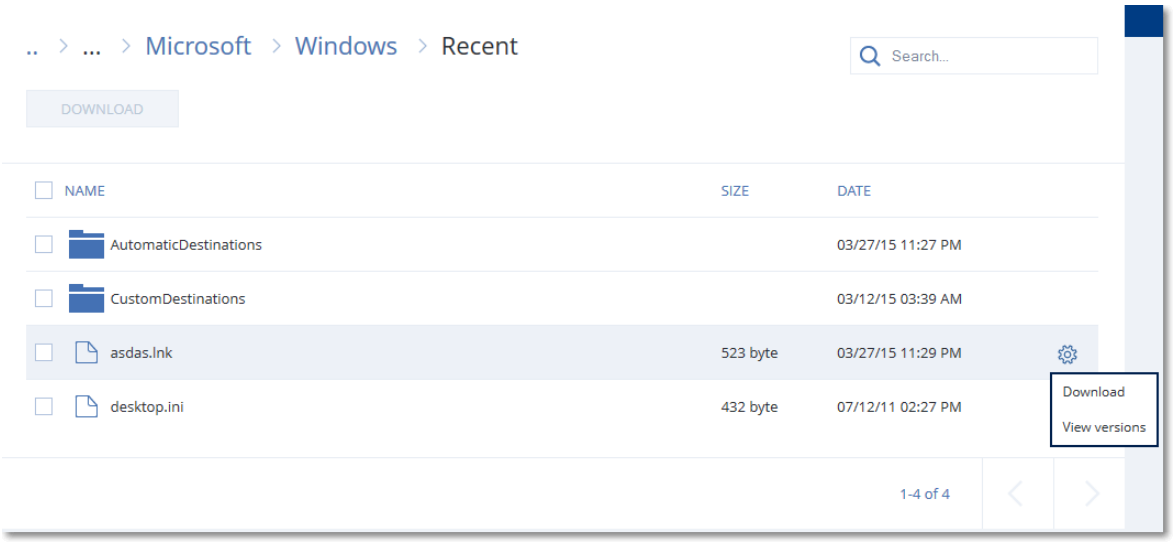
Pour télécharger des fichiers à partir du stockage sur le Cloud

1. Sélectionnez une machine qui a été sauvegardée.
2. Cliquez sur **Restaurer** > **Autres méthodes de restauration...** > **Téléchargement des fichiers**.
3. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.
4. [Lorsque vous parcourez les sauvegardes de lecteur] Sous **Versions**, cliquez sur la sauvegarde à partir de laquelle vous souhaitez récupérer les fichiers.



[Lorsque vous parcourez les sauvegardes de niveau disque] Vous pouvez sélectionner la date et l'heure de sauvegarde à la prochaine étape, via l'icône en forme d'engrenage située à droite du fichier sélectionné. Par défaut, les fichiers sont restaurés à partir de la dernière sauvegarde.

5. Recherchez le dossier requis ou utilisez la fonction de recherche pour obtenir la liste des fichiers requis.



6. Activez les cases à cocher pour les éléments que vous devez restaurer, puis cliquez sur **Télécharger**.

   Si vous sélectionnez un seul fichier, il sera téléchargé en l'état. Autrement, les données sélectionnées seront archivées sous forme d'un fichier .zip.
7. Sélectionnez l'emplacement où enregistrer les données, puis cliquez sur **Enregistrer**.

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
- 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 ».
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.

Restauration de fichiers via un support de démarrage

Pour en savoir plus sur la manière de créer un support de démarrage, consultez la section « Création d'un support de démarrage ».

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 le nom d'hôte/l'adresse IP et le port de serveur proxy. Sinon, ignorez cette étape.
4. Sur l'écran d'accueil, cliquez sur **Restaurer**.
5. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
6. Indiquez l'emplacement de la sauvegarde :
   - Pour restaurer des informations depuis le Cloud, sélectionnez **Stockage sur le Cloud**. Saisissez les informations d'identification du compte auquel la machine sauvegardée a été associée.
   - Pour effectuer une restauration depuis un dossier local ou réseau, rendez-vous dans **Dossiers locaux** ou **Dossiers réseau**.

   Cliquez sur **OK** pour confirmer votre sélection.

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. Dans **Contenu des sauvegardes**, sélectionnez **Dossiers/fichiers**.
9. Sélectionnez les données que vous voulez restaurer. Cliquez sur **OK** pour confirmer votre sélection.
10. 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.
11. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
12. Cliquez sur **OK** pour démarrer la restauration.

Remarque
L'emplacement de bande prend beaucoup de place et ne passera peut-être pas dans la RAM lorsque vous réanalysez et restaurez dans un support de démarrage Linux et WinPE. Pour Linux, vous devez monter un autre emplacement pour enregistrer les données sur un disque ou un partage. Voir Acronis Cyber Backup Advanced : Modification du dossier TapeLocation (KB 27445). Pour Windows PE, aucune solution de contournement n'existe pour le moment.

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.
- Un agent de protection doit être installé sur la machine utilisée pour explorer la sauvegarde.
- Le système du fichier sauvegardé doit être l'un des suivants : FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS ou HFS+.
- 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 :
   `<nom de machine> - <GUID du plan de protection>`
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.

Restauration de l'état du système

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.

La progression de la restauration sont affichées dans l'onglet **Activités**.

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 ».

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.
12. [Facultatif] Cliquez sur **Options de restauration**, pour spécifier des paramètres supplémentaires.
13. Cliquez sur **OK** pour démarrer la restauration.

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 :

- 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 HC3	Windows
Validation de la sauvegarde	+	+	+	+	+	+	+	+	+

Mode de démarrage	+	-	-	-	-	-	-	+	-
Date et heure des fichiers	-	-	-	+	+	+	+	-	-
Gestion erreurs	+	+	+	+	+	+	+	+	+
Exclusions de fichiers	-	-	-	+	+	+	+	-	-
Flashback	+	+	+	-	-	-	-	+	-
Restauration de chemin d'accès complet	-	-	-	+	+	+	+	-	-
Points de montage	-	-	-	+	-	-	-	-	-
Performance	+	+	-	+	+	+	-	+	+
Commandes Pré/Post	+	+	-	+	+	+	-	+	+
Modification de SID	+	-	-	-	-	-	-	-	-
Gestion de l'alimentation des MV	-	-	-	-	-	-	-	+	-

"Gestion des bandes" (p. 350) > Utiliser cache disque pour accélérer restauration	-	-	-	+	+	+	-	-	-
Journal des événements Windows	+	-	-	+	-	-	-	Hyper-V uniquement	+
Mettre sous tension après la récupération	-	-	-	-	-	-	+	-	-

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**.

calculant une somme de contrôle pour chaque bloc de données enregistré dans la sauvegarde. La seule exception est la validation des sauvegardes de niveau fichier se trouvant dans le stockage sur le Cloud. Ces sauvegardes sont validées en vérifiant la cohérence des méta-informations enregistrées dans la sauvegarde.

La validation est un processus très long, même pour les petites sauvegardes incrémentielles ou différentielles. Cette opération valide en effet les données physiques de la sauvegarde ainsi que toutes les données récupérables par la sélection de cette sauvegarde. Cela nécessite un accès aux sauvegardes précédemment créées.

Remarque
La validation est disponible pour le stockage dans le Cloud situé dans un centre de données Acronis et fourni par des partenaires d'Acronis.

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).
- 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
- Le transfert entre UEFI et BIOS n'est pas pris en charge si la sauvegarde est stockée sur un périphérique à bandes.

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 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.

Enregistrer des informations système au cas où 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.

Si l'option est activée, seules les différences entre les données de la sauvegarde et le disque de destination sont restaurées. Ceci accélère la récupération de données vers le même disque que celui qui a été sauvegardé, en particulier si la structure de volume du disque n'a pas changé. Les données sont comparées au niveau des blocs.

Pour les machines physiques, comparer les données au niveau des blocs est une opération chronophage. Si la connexion au stockage de sauvegarde est rapide, il vous faudra moins de temps pour restaurer le disque entier que de calculer les différences de données. Par conséquent, nous vous recommandons d'activer cette option seulement si la connexion au stockage de sauvegarde est lente (par exemple, si la sauvegarde est stockée dans le stockage dans le Cloud ou dans un fichier réseau à distance).

Lors de la restauration d'une machine physique, le préréglage dépend de l'emplacement de la sauvegarde :

- Si l'emplacement de la sauvegarde est dans le stockage dans le Cloud, le préréglage est le suivant : **Activé**.
- Pour d'autres emplacements de sauvegarde, le préréglage est le suivant : **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**, **Haute**.

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.

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-récupération ne sera pas exécutée si la récupération 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 **Valider**.

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 n'est pas achevée	Sélectionné	Sélectionné	Effacé	Effacé
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 sauvegarde 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 **Valider**.

Remarque
Une commande post-récupération ne sera pas exécutée si la récupération exécute un redémarrage.

Gestion des bandes

Vous pouvez utiliser les options de restauration de gestion de bandes suivantes.

Utilisez un cache de disque pour accélérer la récupération.

Le préréglage est le suivant : **Désactivé**.

Nous vous recommandons fortement d'utiliser l'option **Utiliser cache disque pour accélérer restauration** lorsque vous restaurez des fichiers depuis une archive d'image. Sinon, l'opération de restauration peut prendre beaucoup de temps. Avec cette option, la lecture de bande se fait de manière séquentielle, sans interruption ni rembobinage.

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 ou l'agent pour HC3 de Scale Computing.

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, Hyper-V ou Scale Computing HC3.

Éteindre les machines virtuelles cibles lors du démarrage de la récupération

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 récupération 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**.

Mettre sous tension après la récupération

Cette option est effective en cas de fonctionnement avec le support de démarrage.

Le préréglage est le suivant : **Désactivé**.

Cette option permet de démarrer la machine dans le système d'exploitation restauré sans intervention de l'utilisateur.

Reprise d'activité après sinistre

Cette fonctionnalité est disponible uniquement dans les déploiements dans le Cloud de Acronis Cyber Protect. Pour une description détaillée de cette fonctionnalité, veuillez consulter le site https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html.

Opérations avec des sauvegardes

L'onglet Stockage de sauvegarde

L'onglet **Stockage de sauvegarde** affiche les sauvegardes de l'ensemble des ordinateurs enregistrés sur le serveur de gestion. Cela comprend les machines hors ligne et les machines qui ne sont plus enregistrées.

Les sauvegardes stockées à un emplacement partagé (tel que partage SMB ou NFS) sont visibles de tous les utilisateurs bénéficiant d'un accès en lecture à l'emplacement en question.

Dans Windows, les fichiers de sauvegarde héritent des permissions d'accès de leur dossier parent. Par conséquent, nous vous recommandons de restreindre les permissions de lecture pour ce dossier.

Concernant le stockage dans le Cloud, les utilisateurs ont uniquement accès à leurs propres sauvegardes. Dans un déploiement dans le Cloud, un administrateur peut afficher les sauvegardes pour tout compte appartenant au même groupe ou à ses groupes enfants. Ce compte est choisi de façon indirecte dans **Machine à explorer**. L'onglet **Stockage de sauvegarde** affiche les sauvegardes de l'ensemble des machines enregistrées dans le même compte que cette machine.

Les emplacements de sauvegarde utilisés dans les plans de protection sont automatiquement ajoutés à l'onglet **Stockage de sauvegarde**. Pour ajouter un dossier personnalisé (par exemple, un périphérique USB amovible) à la liste des emplacements de sauvegarde, cliquez sur **Parcourir** et indiquez le chemin d'accès au dossier.

Avertissement !
Ne tentez pas de modifier manuellement les fichiers de sauvegarde, car cela pourrait altérer les fichiers et rendre les sauvegardes inutilisables. Nous vous recommandons également d'exporter les sauvegardes ou d'utiliser la réplication de sauvegarde plutôt que de déplacer manuellement des fichiers de sauvegarde.

Sélectionner un point de récupération à l'aide de l'onglet Stockage de sauvegarde

1. Dans l'onglet **Stockage de sauvegarde**, sélectionnez l'emplacement de stockage des sauvegardes.

   Le logiciel présente toutes les sauvegardes que votre compte est autorisé à afficher dans l'emplacement sélectionné. Les sauvegardes sont placées dans des groupes. Les noms des groupes reposent sur l'exemple suivant :

   `<nom de machine> - <nom de plan de protection>`
2. Sélectionnez le groupe à partir duquel vous voulez restaurer les données.
3. [Facultatif] Cliquez sur **Modifier** en regard de **Machine à explorer**, puis sélectionnez une autre machine. Certaines sauvegardes ne peuvent être explorées que par des agents spécifiques. Par exemple, vous devez sélectionner une machine exécutant l'agent pour SQL afin de parcourir les sauvegardes de bases de données Microsoft SQL Server.

Important
Notez que **Machine à explorer** est une destination par défaut pour la restauration depuis une sauvegarde de machine physique. Après avoir sélectionné un point de récupération et cliqué sur **Restaurer**, vérifiez le paramètre **Machine cible** afin de vous assurer qu'il s'agit bien de la machine vers laquelle vous souhaitez effectuer une restauration. Pour modifier la destination de restauration, spécifiez une autre machine dans **Machine à explorer**.

4. Cliquez sur **Afficher les sauvegardes**.
5. Sélectionnez le 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 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. Par défaut, les noms des fichiers suivent le modèle suivant :

   `<nom de machine> - <GUID du plan de protection>`
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. Double-cliquez sur un volume pour le monter, puis cliquez sur une des options suivantes :
   - **Monter**

     Remarque
     Seule la dernière sauvegarde de l'archive (chaîne de sauvegarde) peut être montée en mode lecture/écriture.
   - **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.
2. Effectuez un clic droit sur le volume monté.
3. Cliquez sur **Démonter**.

4. 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

La validation est une opération qui vérifie la possibilité de restauration de données à partir d'une sauvegarde. Pour en savoir plus sur cette opération, reportez-vous à "Validation" (p. 362).

Pour valider une sauvegarde

1. Sélectionnez la charge de travail 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 charge de travail est hors ligne, les points de récupération 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 charge de travail cible qui est en ligne, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde. Pour en savoir plus sur ce type de sauvegarde, reportez-vous à "L'onglet Stockage de sauvegarde" (p. 353).
4. Cliquez sur l'icône en forme d'engrenage, puis sur **Valider**.
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 que vous spécifiez. La sauvegarde originale demeure intacte. L'exportation 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.

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 récupération, utilisez un plan de réplication de sauvegarde.

Le nom du fichier de sauvegarde de la sauvegarde exportée dépend de la valeur de l'option du format de sauvegarde :

- Pour le format **Version 12** avec tout modèle de sauvegarde, le nom du fichier de sauvegarde 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.
- Pour le format **Version 11** avec le modèle de sauvegarde **« Toujours incrémentielle (fichier unique) »**, le nom de fichier de sauvegarde correspond exactement à celui de la sauvegarde d'origine. Si de multiples sauvegardes issues de la même chaîne de sauvegarde sont exportées vers le même emplacement, chaque opération d'exportation remplace la sauvegarde précédemment exportée.
- Pour le format **Version 11** avec d'autres modèles de sauvegarde, le nom du fichier de sauvegarde est identique à celui de la sauvegarde d'origine, à l'exception de l'estampille. Les estampilles des sauvegardes exportées correspondent à l'heure où l'exportation a été réalisée.

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 machine 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 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 une machine**, sélectionnez une machine cible qui est en ligne, puis choisissez un point de restauration.
   - Sélectionnez un point de récupération dans l'onglet Stockage de sauvegarde.
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

Avertissement !
Lorsqu'une sauvegarde est supprimée, toutes ses données le sont également, et ce de façon permanente. Les données supprimées ne peuvent pas être récupérées.

Suppression des sauvegardes d'un ordinateur en ligne et présente dans la console Web Cyber Protect

1. Dans l'onglet **Tous les périphériques**, sélectionnez la machine dont vous souhaitez supprimer les sauvegardes.
2. Cliquez sur **Restauration**.
3. Sélectionnez l'endroit duquel vous souhaitez supprimer les sauvegardes.
4. Effectuez l'une des actions suivantes :
   - Pour supprimer une seule sauvegarde, sélectionnez-la, puis cliquez sur l'icône en forme d'engrenage et sur **Supprimer**.
   - Pour supprimer l'ensemble des sauvegardes d'un emplacement sélectionné, cliquez sur **Tout supprimer**.
5. Confirmez votre choix.

Suppression des sauvegardes d'une machine

1. Dans l'onglet **Stockage de sauvegarde**, sélectionnez l'emplacement dans lequel vous souhaitez supprimer les sauvegardes.
   Le logiciel présente toutes les sauvegardes que votre compte est autorisé à afficher dans l'emplacement sélectionné. Les sauvegardes sont placées dans des groupes. Les noms des groupes reposent sur l'exemple suivant :
   `<nom de machine> - <nom de plan de protection>`
2. Sélectionnez un groupe.
3. Effectuez l'une des actions suivantes :
   - Pour supprimer une seule sauvegarde, cliquez sur **Afficher les sauvegardes**, sélectionnez la sauvegarde à supprimer, puis cliquez sur l'icône en forme d'engrenage et sur **Supprimer**.
   - Pour supprimer le groupe sélectionné, cliquez sur **Supprimer**.
4. Confirmez votre choix.

Pour supprimer des sauvegardes directement du stockage Cloud

1. Connectez-vous au stockage Cloud, comme décrit dans « Téléchargement de fichiers depuis le Cloud ».
2. Cliquez sur le nom de la machine contenant les sauvegardes que vous souhaitez supprimer.
   Le logiciel affiche un ou plusieurs groupes de sauvegardes.
3. Cliquez sur l'icône en forme d'engrenage en regard du groupe de sauvegardes que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.
5. Confirmez l'opération.

L'onglet Plans

Avec une licence Advanced, vous pouvez gérer les plans de protection et d'autres plans à l'aide de l'onglet **Plans**.

Chaque section de l'onglet **Plans** contient tous les plans d'un type spécifique. Les sections suivantes sont disponibles :

- **Protection**
- **Analyse de sauvegarde**
- **Réplication de sauvegarde**
- **Validation**
- **Nettoyage**
- **Conversion en MV**
- **Réplication de MV**
- **Support de démarrage**. Cette section affiche les plans de protection créés pour des ordinateurs démarrés depuis un support de démarrage et qui ne peuvent être appliqués qu'à ces ordinateurs.

Dans chaque section, vous pouvez créer, modifier, désactiver, activer, supprimer et inspecter l'exécution d'un plan.

Le clonage et l'arrêt sont disponibles uniquement dans les plans de protection. Contrairement à l'arrêt d'une sauvegarde depuis l'onglet **Terminaux**, l'arrêt d'un plan de protection concerne les sauvegardes sur tous les terminaux sur lesquels le plan est en cours d'exécution. Si les heures de démarrage de la sauvegarde pour plusieurs terminaux sont distribuées dans une fenêtre de temps, l'arrêt d'un plan de protection arrête l'exécution des sauvegardes ou empêche leur démarrage.

Vous pouvez également exporter un plan vers un fichier et importer un plan précédemment exporté.

Traitement des données hors hôte

La plupart des actions qui font partie d'un plan de protection, comme la réplication, la validation et l'application des règles de rétention, sont effectuées par l'agent chargé de la sauvegarde. Cela ajoute une charge de travail à la machine sur laquelle s'exécute l'agent, même une fois le processus de sauvegarde terminé.

En séparant les plans d'analyse antimalware, de réplication, de validation, de nettoyage et de conversion des plans de protection, vous aurez la flexibilité de :

- choisir un autre agent pour effectuer ces opérations ;
- planifier ces opérations durant les heures creuses afin de réduire au minimum la consommation de bande passante ;

- déplacer des opérations en dehors des heures de bureau, si la configuration d'un agent dédié ne fait pas partie de vos plans.

Si vous utilisez un nœud de stockage, il peut être judicieux d'installer un agent dédié sur la même machine.

Contrairement aux plans de sauvegarde et de réplication, qui utilisent les paramètres de temps des machines qui exécutent les agents, les plans de traitement de données hors hôte s'exécutent selon les paramètres de temps de la machine du serveur de gestion.

Plan d'analyse de la sauvegarde

Emplacements pris en charge

Vous pouvez analyser les sauvegardes à la recherche de malware dans les emplacements suivants : **Stockage dans le Cloud**, **dossier local** et **dossier réseau**. Seul un agent installé sur l'ordinateur analysé peut accéder à l'emplacement **Dossier local**.

Pour plus d'informations sur l'analyse de sauvegarde et ses limites, reportez-vous à l'article Analyse antimalware des sauvegardes.

Créer un plan d'analyse de sauvegarde

1. Dans la console Web Cyber Protect, cliquez sur **Plans** > **Analyse de sauvegarde**.
2. Cliquez sur **Création d'un plan**.
3. [Facultatif] Pour modifier le nom du plan, cliquez sur l'icône représentant un crayon située à côté du nom par défaut.
4. Sélectionnez l'agent d'analyse.
5. Sélectionnez l'emplacement de sauvegarde ou des sauvegardes à analyser.
   Vous pouvez sélectionner plusieurs emplacements de sauvegarde simultanément. Pour inclure plusieurs sauvegardes dans un plan, vous devez les ajouter une par une.
6. [Si **Stockage dans le Cloud** ou **Dossier réseau** sont sélectionnées] Le cas échéant, spécifiez les identifiants donnant accès au stockage de sauvegarde.
7. [Si une sauvegarde chiffrée est sélectionnée] Saisissez le mot de passe pour accéder à la sauvegarde. Si un emplacement de stockage ou plusieurs sauvegardes chiffrées sont sélectionnés, vous pouvez spécifier un seul mot de passe. Si le mot de passe est incorrect pour une sauvegarde donnée, une alerte s'affiche. Seules sont analysées les sauvegardes pour lesquelles un mot de passe correct est fourni.
8. Configurez la planification de l'analyse.
9. Lorsque vous avez terminé, cliquez sur **Créer**.

Le plan d'analyse de sauvegarde est alors créé.

Réplication de sauvegarde

Emplacements pris en charge

Le tableau suivant récapitule les emplacements de sauvegarde pris en charge par les plans de réplication de sauvegarde.

Emplacement de sauvegarde	Pris en charge comme source	Pris en charge comme cible
Stockage dans le Cloud	+	+
Dossier local	+	+
Dossier réseau	+	+
Dossier NFS	–	–
Secure Zone	–	–
Serveur SFTP	–	–
Emplacement géré*	+	+
Lecteur de bandes	–	+

* Vérifiez les restrictions décrites dans la rubrique "Remarques pour les utilisateurs disposant de la licence Advanced" (p. 265).

Pour créer un plan de réplication de sauvegarde

1. Cliquez sur **Plans** > **Réplication de sauvegarde**.
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. Cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera la réplication.
   Vous pouvez sélectionner n'importe quel agent ayant accès aux emplacements de sauvegarde source et cible.
5. Cliquez sur **Éléments à répliquer**, puis sélectionnez les sauvegardes que ce plan répliquera.
   Vous pouvez passer d'une sélection des sauvegardes ou d'une sélection d'emplacements entiers à l'autre à l'aide de l'option **Emplacements** / **Sauvegardes** en haut à droite.
   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.
6. Cliquez sur **Destination** et spécifiez l'emplacement cible.

7. [Facultatif] Dans **Comment répliquer**, sélectionnez les sauvegardes à répliquer. Vous pouvez sélectionner l'une des options suivantes :
   - **Tous les plans de sauvegarde** (par défaut)
   - **Sauvegardes complètes uniquement**
   - **Seulement la dernière sauvegarde**
8. [Facultatif] Cliquez sur **Planification**, puis modifiez la planification.
9. [Facultatif] Cliquez sur **Règles de rétention**, puis indiquez les règles de rétention pour l'emplacement cible, comme décrit dans « Règles de rétention ».
10. Si les sauvegardes sélectionnées dans **Éléments à répliquer** sont chiffrées, activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement. Sinon, ignorez cette étape.
11. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
12. Cliquez sur **Créer**.

Validation

La validation est une opération qui vérifie la possibilité de restauration de données à partir d'une sauvegarde.

La validation d'un emplacement de sauvegarde valide toutes les sauvegardes stockées dans cet emplacement.

Fonctionnement

Un plan de validation offre deux méthodes de validation. Si vous sélectionnez les deux méthodes, les opérations seront exécutées consécutivement.

- **Calculer une somme de contrôle pour chaque bloc de données enregistré dans la sauvegarde**

  Pour plus d'informations sur la validation par le calcul d'une somme de contrôle, consultez la section « Validation de la sauvegarde ».
- **Exécution d'une machine virtuelle à partir d'une sauvegarde**

  Cette méthode fonctionne uniquement pour les sauvegardes de niveau disque contenant un système d'exploitation. Pour utiliser cette méthode, vous avez besoin d'un hôte ESXi ou Hyper-V et d'un agent de protection (agent pour VMware ou agent pour Hyper-V) qui gère cet hôte.

  L'agent exécute une machine virtuelle à partir d'une sauvegarde, puis la connecte à des outils VMware ou à un service de pouls d'Hyper-V, 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 et exécute la suivante.

Si la validation échoue, vous pouvez vérifier les détails dans la section **Activités** de l'onglet **Présentation**.

Emplacements pris en charge

Le tableau suivant récapitule les emplacements de sauvegarde pris en charge par les plans de validation.

Emplacement de sauvegarde	Calculer une somme de contrôle	Exécuter une MV
Stockage dans le Cloud	+	+
Dossier local	+	+
Dossier réseau	+	+
Dossier NFS	–	–
Secure Zone	–	–
Serveur SFTP	–	–
Emplacement géré	+	+
Lecteur de bandes	+	–

Pour créer un nouveau plan de validation

1. Cliquez sur **Plans** > **Validation**.
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. Cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera la validation.
   Si vous souhaitez effectuer une validation en exécutant une machine virtuelle depuis une sauvegarde, vous devez sélectionner l'agent pour VMware ou l'agent pour Hyper-V. Sinon, sélectionnez n'importe quel agent enregistré sur le serveur de gestion et ayant accès à l'emplacement de sauvegarde.
5. Cliquez sur **Éléments à valider**, puis sélectionnez les sauvegardes que ce plan validera.
   Vous pouvez passer d'une sélection des sauvegardes ou d'une sélection d'emplacements entiers à l'autre à l'aide de l'option **Emplacements** / **Sauvegardes** en haut à droite.
   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.
6. [Facultatif] Dans **Quoi valider**, sélectionnez les sauvegardes à valider. Vous pouvez sélectionner l'une des options suivantes :

- **Toutes les sauvegardes**
- **Seulement la dernière sauvegarde**

7. [Facultatif] Cliquez sur **Comment valider**, puis choisissez l'une des méthodes suivantes :
   - **Vérification de la somme de contrôle**
     Le logiciel calculera une somme de contrôle pour chaque bloc de données enregistré dans la sauvegarde.
   - **Exécuter en tant que machine virtuelle**
     Le logiciel exécutera une machine virtuelle à partir de chaque sauvegarde.
8. Si vous choisissez **Exécuter en tant que machine virtuelle** :
   a. Cliquez sur **Machine cible**, puis sélectionnez le type de machine virtuelle (ESXi ou Hyper-V), l'hôte et le modèle de nom de la machine.
      Par défaut, le nom est **[Nom de la Machine]_validate**.
   b. Cliquez sur **Magasin de données** pour ESXi ou **Chemin d'accès** pour Hyper-V, puis sélectionnez le magasin de données pour la machine virtuelle.
   c. [Facultatif] Modifiez le mode d'allocation du disque.
      Le paramètre par défaut est **Dynamique** pour VMware ESXi et **En expansion dynamique** pour Hyper-V.
   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.

   Remarque
   Le paramètre **Pouls de la MV** est toujours activé pour valider le statut du pouls de la machine virtuelle que signalent les outils de l'hyperviseur dans le système d'exploitation invité (VMware Tools ou Hyper-V Integration Services) en exécutant une machine virtuelle depuis la sauvegarde. Ce paramètre est conçu pour les prochaines versions, si bien qu'aucune interaction n'est possible.

9. [Facultatif] Cliquez sur **Planification**, puis modifiez la planification.
10. Si les sauvegardes sélectionnées dans **Éléments à valider** sont chiffrées, activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement. Sinon, ignorez cette étape.
11. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
12. Cliquez sur **Créer**.

Nettoyage

Le nettoyage est une opération consistant à supprimer des sauvegardes obsolètes en fonction de règles de rétention.

Emplacements pris en charge

Les plans de nettoyage prennent en charge tous les emplacements de sauvegarde, sauf les dossiers NFS, les serveurs SFTP et Secure Zone.

Pour créer un nouveau plan de nettoyage

1. Cliquez sur **Plans** > **Nettoyage**.
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. Cliquez sur **Agent**, puis sélectionnez l'agent qui exécutera le nettoyage.
   Vous pouvez sélectionner n'importe quel agent ayant accès à l'emplacement de sauvegarde.
5. Cliquez sur **Éléments à nettoyer**, puis sélectionnez les sauvegardes que ce plan devra nettoyer.
   Vous pouvez passer d'une sélection des sauvegardes ou d'une sélection d'emplacements entiers à l'autre à l'aide de l'option **Emplacements** / **Sauvegardes** en haut à droite.
   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.
6. [Facultatif] Cliquez sur **Planification**, puis modifiez la planification.
7. [Facultatif] Cliquez sur **Règles de rétention**, puis indiquez les règles de rétention, comme décrit dans « Règles de rétention ».
8. Si les sauvegardes sélectionnées dans **Éléments à nettoyer** sont chiffrées, activez l'option **Mot de passe de la sauvegarde**, puis indiquez le mot de passe de chiffrement. Sinon, ignorez cette étape.
9. [Facultatif] Pour modifier les options du plan, cliquez sur l'icône en forme d'engrenage.
10. Cliquez sur **Créer**.

Conversion en une machine virtuelle

Vous pouvez créer un plan séparé pour la conversion vers une machine virtuelle et exécuter ce plan manuellement ou selon un calendrier.

Pour des informations sur les prérequis et les limites, veuillez vous référer à « Ce que vous devez savoir à propos de la conversion ».

Pour créer un plan de conversion en une machine virtuelle

1. Cliquez sur **Plans** > **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**
   - **HC3 de Scale Computing**
   - **VMware Workstation**
   - **Fichiers VHDX**

   Remarque
   Pour économiser de l'espace, chaque conversion en fichiers VHDX écrase les fichiers VHDX 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 HC3 de Scale Computing] 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 d'une sélection des sauvegardes ou d'une sélection d'emplacements entiers à l'autre à l'aide de l'option **Emplacements** / **Sauvegardes** en haut à droite.

   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.
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 HC3 de Scale Computing] 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**.

Support de démarrage

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

Support de démarrage

Un support de démarrage est un support physique (CD, DVD, lecteur flash USB ou autre support amovible compatible avec le BIOS de la machine, en tant que périphérique de démarrage) qui vous permet d'exécuter l'agent de protection dans un environnement Linux ou Windows Preinstallation Environment (WinPE), sans l'aide d'un système d'exploitation.

Un support de démarrage est le plus souvent utilisé pour :

- Restaurer un système d'exploitation qui ne parvient pas démarrer
- Accéder aux données ayant survécu dans un système corrompu et les sauvegarder
- Déployer un système d'exploitation sur un système nu
- Créer des volumes dynamiques ou basiques sur un système nu
- Sauvegarder secteur par secteur un disque avec un système de fichiers qui n'est pas pris en charge
- Sauvegarder hors ligne toutes les données ne pouvant pas être sauvegardées en ligne, par exemple parce que les données sont verrouillées par une application en cours d'exécution ou parce que l'accès là celles-ci est trop restreint.

Un ordinateur peut aussi être démarré à partir du serveur PXE d'Acronis, des services de déploiement Windows (WDS) ou des services d'installation à distance (RIS). Ces serveurs contenant des composants de démarrage peuvent également être considérés comme une sorte de support de démarrage. Vous pouvez créer un support de démarrage ou configurer le serveur PXE ou WDS/RIS en utilisant le même assistant.

Créer un support de démarrage ou en télécharger un tout prêt ?

Avec Bootable Media Builder, vous pouvez créer votre propre support de démarrage (basé sur Linux ou basé sur WinPE) pour ordinateurs Windows, Linux ou macOS. Pour obtenir un support de démarrage doté de toutes les fonctionnalités, spécifiez une clé de licence Acronis Cyber Protect. Sans cette clé, votre support de démarrage sera limité aux opérations de restauration.

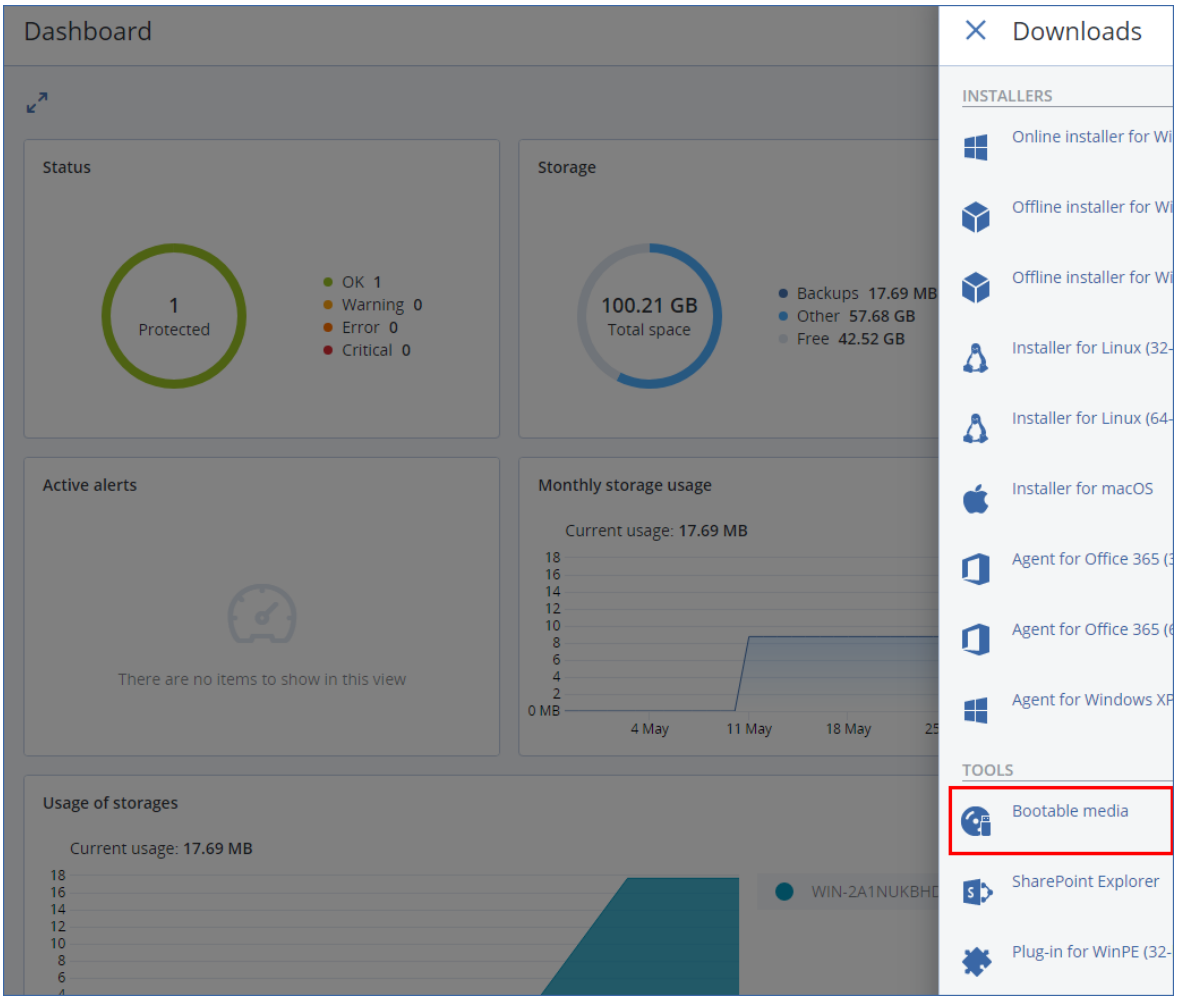
Remarque
Le support de démarrage n'est pas compatible avec les lecteurs hybrides.

Vous pouvez aussi télécharger un support de démarrage tout prêt (basé sur Linux uniquement). Le support de démarrage téléchargé ne peut être utilisé que pour les opérations de récupération et l'accès à Acronis Universal Restore. Il ne vous permet pas de sauvegarder des données, de valider ou d'exporter des sauvegardes, de gérer des disques, ni d'utiliser des scripts. Le support de démarrage téléchargé n'est pas compatible avec les ordinateurs macOS.

Remarque
Le support de démarrage tout prêt n'est pas compatible avec les nœuds de stockage, les emplacements de bandes et les emplacements SFTP. Si vous souhaitez utiliser ces emplacements de stockage dans votre déploiement sur site, vous devez créer votre propre support de démarrage à l'aide de Bootable Media Builder. Voir https://kb.acronis.com/content/61566.

Pour télécharger un support de démarrage tout prêt

1. Dans la console Web Cyber Protect, cliquez sur l'icône de compte dans le coin supérieur droit, puis cliquez sur **Téléchargements**.
2. Sélectionnez **Support de démarrage**.



Vous pouvez graver le fichier ISO téléchargé sur un CD/DVD ou créer un lecteur flash USB de démarrage à l'aide d'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.

Si la console Web Cyber Protect n'est pas accessible, vous pouvez télécharger le support de démarrage tout prêt depuis votre compte sur le portail client Acronis :

1. Accédez à https://account.acronis.com.
2. Trouvez Acronis Cyber Protect, puis cliquez sur **Téléchargements**.
3. Sur la page qui s'ouvre, trouvez **Téléchargements supplémentaires**, puis cliquez sur **ISO de support de démarrage (pour Windows et Linux)**.

Support de démarrage basé sur Linux ou sur WinPE ?

Basé sur Linux

Un support de démarrage basé sur Linux contient un agent de protection de démarrage basé sur le noyau Linux. L'agent peut démarrer et réaliser des opérations sur n'importe quel matériel compatible avec un PC, y compris un système nu et des machines avec des systèmes de fichiers corrompus ou incompatibles. Les opérations peuvent être configurées et contrôlées localement ou à distance, dans la console Web Cyber Protect.

Une liste du matériel pris en charge par les supports de démarrage basés sur Linux est disponible dans l'article de la base de connaissances suivant : http://kb.acronis.com/content/55310.

Basé sur WinPE

Un support de démarrage basé sur WinPE contient un système Windows minimal appelé Windows Preinstallation Environment (WinPE) et un plug-in Acronis pour WinPE, qui est une modification de l'agent de protection qui peut être exécutée dans l'environnement de préinstallation.

WinPE se révèle être la solution de démarrage la plus pratique dans les grands environnements avec un matériel hétérogène.

Avantages :

- Utiliser Acronis Cyber Protect dans Windows Preinstallation Environment fournit plus de fonctionnalités que d'utiliser un support de démarrage basé sur un environnement Linux. Après avoir démarré un matériel compatible PC sous WinPE, vous pouvez non seulement utiliser un agent de protection, mais aussi les commandes et scripts de l'environnement de préinstallation (PE), ainsi que les autres plug-ins que vous y avez ajoutés.
- 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 grappes RAID seulement. Un support basé sur WinPE 2.x ou ultérieur permet le chargement dynamique des pilotes des périphériques nécessaires.

Limites :

- 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).
- Lorsqu'une machine est démarrée avec une support de démarrage PE, vous ne pouvez pas sélectionner de supports optiques tels que les CD, DVD ou Blu-ray (BD) comme destination de sauvegarde.

Bootable Media Builder

Bootable Media Builder permet de créer des supports de démarrage. Il est disponible pour les déploiements sur site uniquement.

Bootable Media Builder est installé par défaut avec le serveur de gestion. Vous pouvez installer Media Builder séparément sur toute machine fonctionnant sous Windows ou Linux. Les systèmes d'exploitation pris en charge sont les mêmes que pour les agents correspondants.

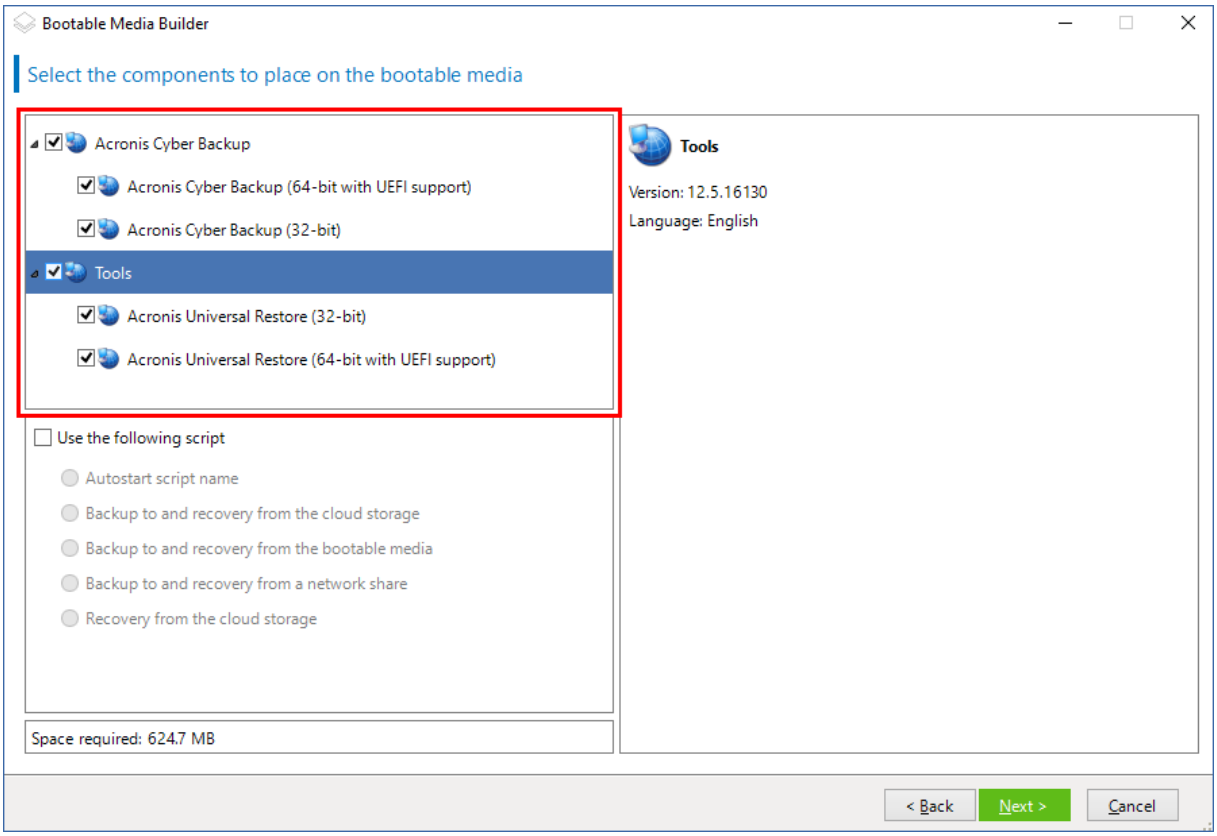
Pourquoi utiliser Media Builder ?

Le support de démarrage disponible au téléchargement dans la console Web Cyber Protect peut uniquement être utilisé à des fins de restauration. Ce support est basé sur un noyau Linux. Contrairement à Windows PE, il ne permet pas d'implanter des pilotes personnalisés à la volée.

- Media Builder vous permet de créer des supports de démarrage personnalisés et complets basés sur Linux ou WinPE avec la fonction de sauvegarde.
- En plus de créer un support physique de démarrage, vous pouvez transférer ses composants aux services de déploiement Windows (WDS) et utiliser le démarrage réseau.
- Le support de démarrage tout prêt n'est pas compatible avec les nœuds de stockage, les emplacements de bandes et les emplacements SFTP. Si vous souhaitez utiliser ces emplacements de stockage dans votre déploiement local sur site, vous devez créer votre propre support de démarrage à l'aide de Bootable Media Builder. Voir https://kb.acronis.com/content/61566.

32 bits ou 64 bits ?

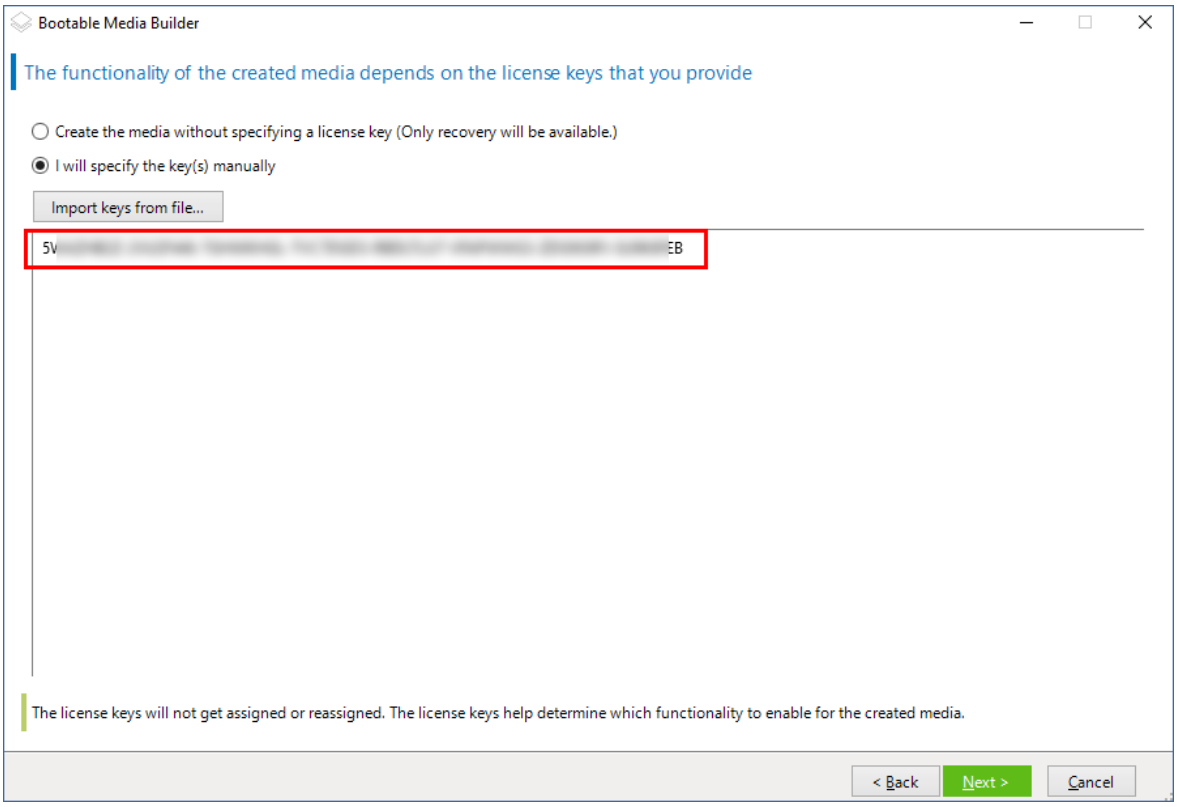
Bootable Media Builder crée un support avec des composants 32 bits et 64 bits. Dans la plupart des cas, vous avez besoin d'un support 64 bits pour démarrer une machine qui utilise l'interface UEFI (Unified Extensible Firmware Interface).



Support de démarrage basé sur un environnement Linux

Pour créer un support de démarrage basé sur Linux

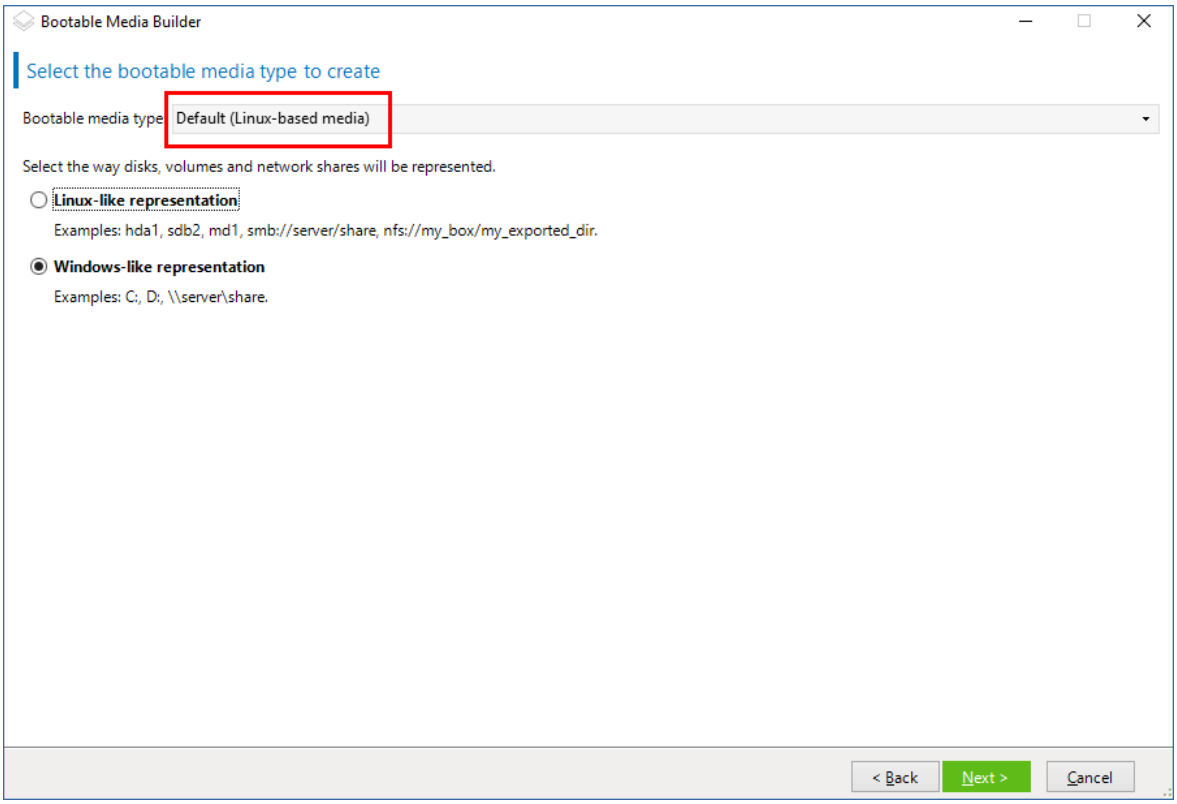
1. Démarrez **Bootable Media Builder**.
2. Pour créer un support de démarrage complet, spécifiez une clé de licence Acronis Cyber Protect. Cette clé permet de déterminer les fonctionnalités qui seront incluses dans le support de démarrage. Aucune licence ne sera révoquée à partir des ordinateurs.
   Si vous n'indiquez aucune clé de licence, le support de démarrage qui en résulte ne peut être utilisé que pour les opérations de récupération.



3. Sélectionnez **Type de support de démarrage : Défaut (support basé sur Linux)**.

   Sélectionnez la manière dont les volumes et les ressources réseau seront représentés :

   - Un support 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 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).



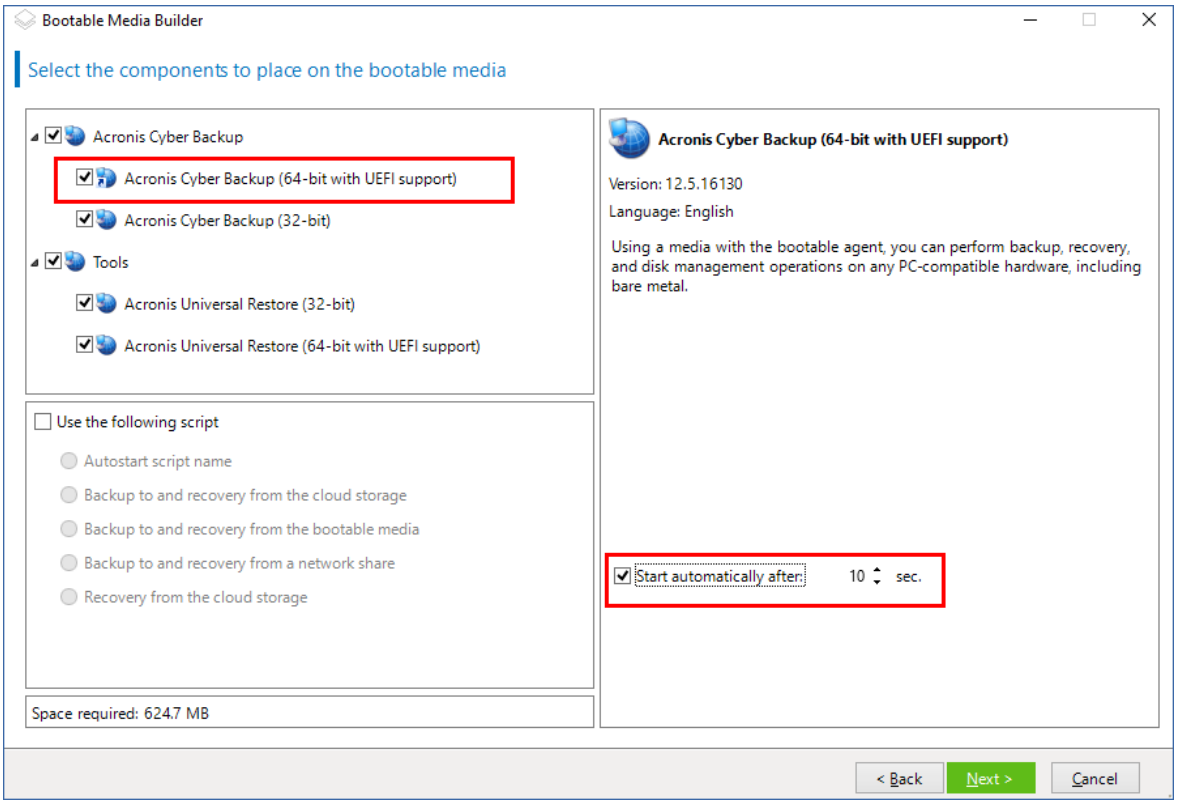
4. [Facultatif] Spécifiez les paramètres du noyau Linux. Séparez des paramètres multiples par des espaces.

   Par exemple, pour pouvoir sélectionner un mode d'affichage pour l'agent de démarrage chaque fois que le support démarre, saisissez : **vga=ask**.

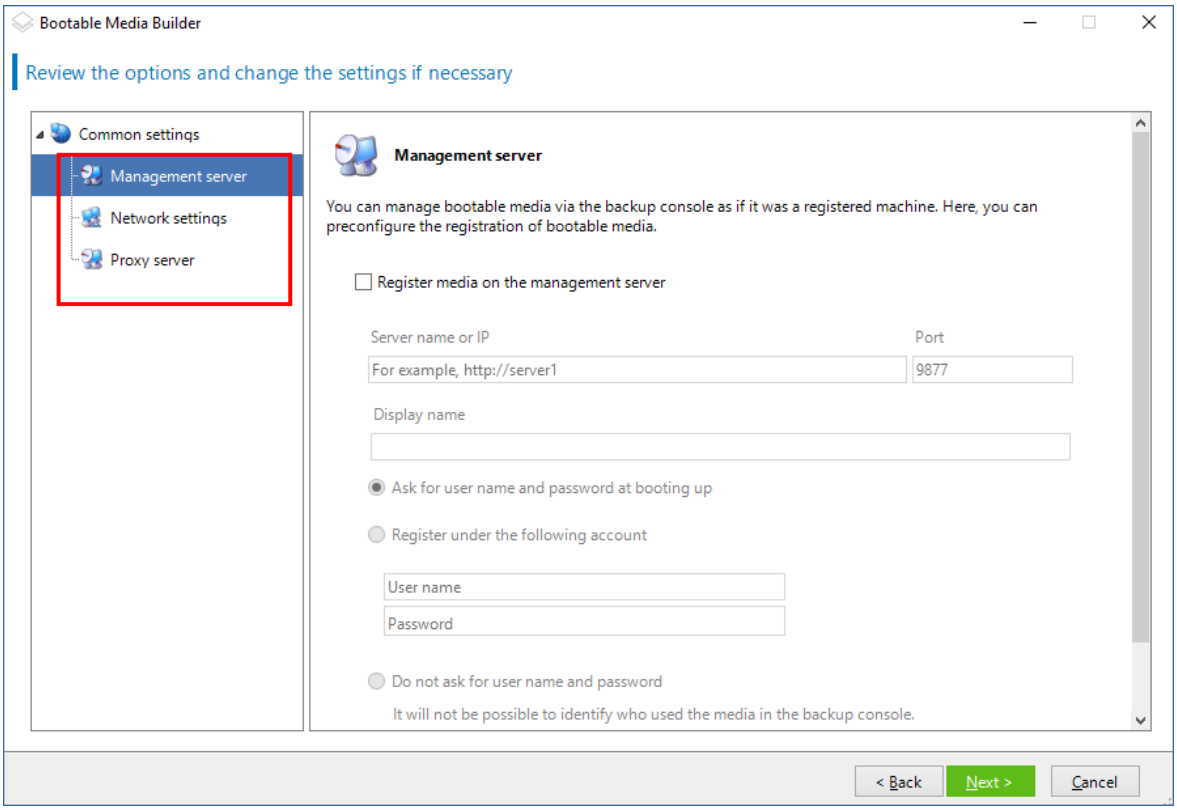
   Pour plus d'informations sur les paramètres disponibles, reportez-vous à Paramètres du noyau.
5. [Facultatif] Sélectionnez la langue qui sera utilisée dans le support de démarrage.
6. Sélectionnez les composants à placer sur le support : l'agent de démarrage Acronis Cyber Protect et/ou Universal Restore si vous prévoyez de restaurer le système sur du matériel différent.

   L'agent de démarrage vous permet d'effectuer des opérations de sauvegarde, de restauration et de gestion de disque sur tout matériel compatible PC, y compris les machines sans système d'exploitation de base.

   Universal Restore vous permet de démarrer un système d'exploitation restauré sur une machine virtuelle ou sur un matériel différent. L'outil trouve et installe les pilotes pour les périphériques qui sont critiques pour le démarrage du système d'exploitation, tels que les contrôleurs de stockage, la carte-mère ou le chipset.
7. [Facultatif] Spécifiez l'intervalle de délai d'expiration pour le menu de démarrage, ainsi que le composant qui démarrera automatiquement au délai d'expiration. Pour cela, cliquez sur le composant souhaité dans le volet en haut à gauche, puis définissez l'intervalle. Cela permet une opération automatique sur site lors du démarrage à partir d'un WDS/RIS.
   Si ce paramètre n'est pas configuré, le chargeur attendra que vous choisissiez quoi démarrer entre le système d'exploitation (s'il est présent) ou le composant.



8. [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.
9. [Facultatif] Sélectionnez le mode d'enregistrement du support sur le serveur de gestion lors du démarrage. Pour plus d'informations concernant les paramètres d'inscription, consultez la section Serveur de gestion.



10. [Facultatif] Spécifiez les paramètres réseau : Les paramètres TCP / IP à affecter aux adaptateurs réseau de la machine. Pour obtenir plus d'informations, consultez l'article "Paramètres réseau" (p. 387).
11. [Facultatif] Spécifiez un port réseau : Le port TCP sur lequel l'agent de démarrage écoute en attente d'une connexion entrante.
12. [Facultatif] Si un serveur proxy est activé sur votre réseau, spécifiez son nom d'hôte/adresse IP et le port.
13. Sélectionnez le type de support. Vous pouvez :
    - Créer une image ISO. Vous pouvez ensuite la graver sur un CD/DVD ; vous en servir pour créer un lecteur flash USB de démarrage ; ou la connecter à une machine virtuelle ;
    - Créer un fichier ZIP.
    - Transférer les composants sélectionnés vers le serveur Acronis PXE.
    - télécharger les composants sélectionnés sur un WDS/RIS.
14. [Facultatif] Ajoutez des lecteurs système Windows à utiliser par Universal Restore. Cette fenêtre apparaît si Universal Restore est ajouté à un support et qu'un support autre que WDS/RIS est sélectionné.
15. Si vous y êtes invité, spécifiez le nom d'hôte/adresse IP et les informations d'identification pour WDS/RIS, ou un chemin d'accès au fichier ISO du support.
16. Vérifiez vos paramètres sur l'écran Résumé et cliquez sur **Continuer**.

Paramètres du noyau

Cette fenêtre vous permet de spécifier un ou plusieurs paramètres du noyau Linux. Ils seront automatiquement appliqués au démarrage 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 ces paramètres en appuyant sur F11 dans le menu de démarrage.

Paramètres

Lorsque vous spécifiez plusieurs paramètres, séparez-les avec des espaces.

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 peut être différent sur des machines différentes. Nous recommandons d'abord l'utilisation du paramètre **vga=ask** pour choisir une valeur pour *mode_number*.

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.

Sans ce paramètre, 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**

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 périphérique 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.

Scripts sur un support de démarrage

Si vous voulez que le support de démarrage exécute un ensemble déterminé d'opérations, vous pouvez spécifier un script lors de la création du support dans le support de démarrage. À chaque redémarrage du support, le script sera exécuté au lieu d'afficher l'interface utilisateur.

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 :

- Sauvegarde vers et restauration depuis le stockage dans le Cloud (**entire_pc_Cloud**)
- Sauvegarde vers et restauration depuis le support de démarrage (**entire_pc_local**)

- Sauvegarde vers et restauration depuis un partage réseau (**entire_pc_share**)
- Restauration depuis le stockage dans le Cloud (**golden_image**)

Les scripts se trouvent sur la machine sur laquelle le support de démarrage est installé, dans les répertoires suivants :

- Sous Windows : %**ProgramData%\Acronis\MediaBuilder\scripts**
- Sous Linux : **/var/lib/Acronis/MediaBuilder/scripts/**

Sauvegarde vers et restauration depuis le stockage sur le Cloud

Ce script sauvegarde une machine vers le stockage sur le Cloud ou restaure la machine depuis sa sauvegarde la plus récente créée par ce script dans le stockage sur le Cloud. Au démarrage, le script invite l'utilisateur à choisir entre sauvegarde, restauration et démarrage de l'interface utilisateur.

Dans le support de démarrage, spécifiez les paramètres de script suivants :

1. Les nom d'utilisateur et mot de passe pour le stockage sur le Cloud.
2. [Facultatif] Un mot de passe que le script utilisera pour chiffrer les sauvegardes ou y accéder.

Sauvegarde vers et restauration depuis un support de démarrage

Ce script sauvegarde une machine vers le support de démarrage ou restaure la machine depuis sa sauvegarde la plus récente créée par ce script sur le même support. Au démarrage, le script invite l'utilisateur à choisir entre sauvegarde, restauration et démarrage de l'interface utilisateur.

Dans le support de démarrage, vous pouvez spécifier le mot de passe que le script utilisera pour chiffrer les sauvegardes ou y accéder.

Sauvegarde vers et restauration depuis un partage réseau

Ce script sauvegarde une machine vers un partage réseau ou restaure la machine depuis sa sauvegarde la plus récente créée par ce script sur un partage réseau. Au démarrage, le script invite l'utilisateur à choisir entre sauvegarde, restauration et démarrage de l'interface utilisateur.

Dans le support de démarrage, spécifiez les paramètres de script suivants :

1. Le chemin du partage réseau.
2. Les nom d'utilisateur et mot de passe du partage réseau.
3. [Facultatif] Le nom du fichier de sauvegarde. La valeur par défaut est **AutoBackup**. Si vous voulez que le script ajoute les sauvegardes à une sauvegarde existante ou qu'il effectue une restauration depuis une sauvegarde avec un nom n'ayant pas une valeur par défaut, remplacez la valeur par défaut par le nom de fichier de cette sauvegarde.

   Pour trouver le nom du fichier de sauvegarde

   a. Dans la console Web 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 du fichier de sauvegarde**.

4. [Facultatif] Un mot de passe que le script utilisera pour chiffrer les sauvegardes ou y accéder.

Restauration du stockage Cloud

Ce script restaure la machine depuis sa sauvegarde la plus récente créée dans le stockage sur le Cloud. Au démarrage, le script invite l'utilisateur à spécifier :

1. Les nom d'utilisateur et mot de passe pour le stockage sur le Cloud.
2. le mot de passe si la sauvegarde est chiffrée.

Nous vous recommandons de ne stocker les sauvegardes que d'une seule machine sous ce compte de stockage dans le Cloud. Sinon, si la sauvegarde d'une autre machine est plus récente que celle de la machine utilisée, le script choisira la sauvegarde de l'autre machine.

Scripts personnalisés

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.

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`	nombre	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 `enum` nombre si `type` est `number`, `spinner` ou `checkbox`	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` (l'état effacé) ou `1` (l'état sélectionné).
`order`	nombre (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)	nombre	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)	nombre	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)	nombre	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`)	nombre	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

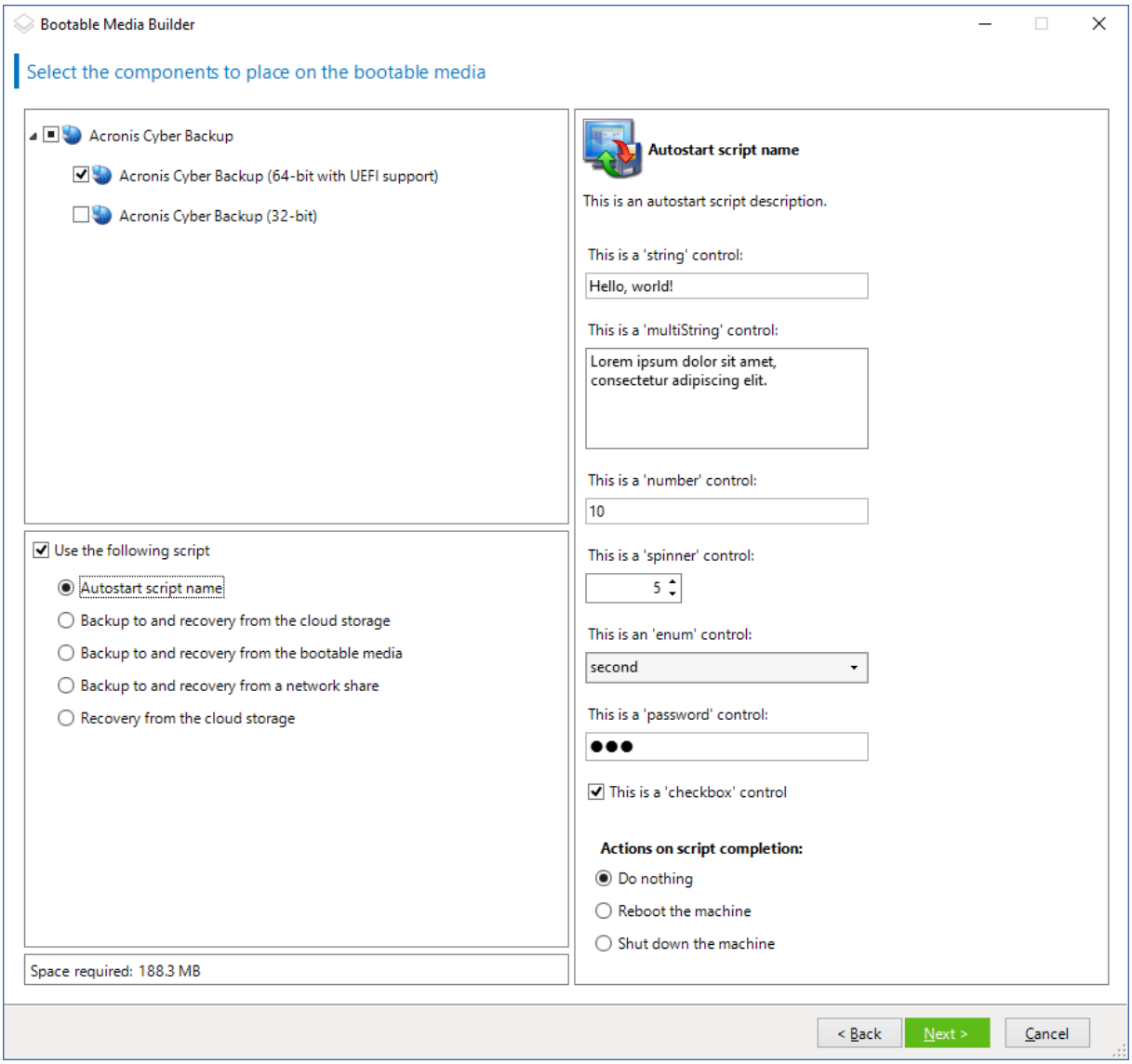
Nom	Description
`string`	Zone de texte sans contrainte d'une seule ligne, utilisée pour saisir ou modifier des chaînes courtes.
`multiString`	Zone de texte sans contrainte de plusieurs lignes, utilisée pour saisir ou modifier des chaînes longues.
`password`	Zone de texte sans contrainte d'une seule ligne, utilisée pour saisir des mots de passe en toute sécurité.
`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",
                "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
        }
    }
}
```

Voici à quoi cela ressemble dans le support de démarrage.



Serveur de gestion

Lors de la création d'un support de démarrage, vous avez la possibilité de préconfigurer l'enregistrement du support sur le serveur de gestion.

L'enregistrement du support vous permet de gérer le support via la console Web Cyber Protect comme s'il s'agissait d'une machine enregistrée. En plus du côté pratique de l'accès distant, cela permet à un administrateur de pouvoir suivre toutes les opérations exécutées sur un support de démarrage. Les opérations sont répertoriées dans **Activités** afin qu'il soit possible de voir qui a lancé une opération et à quel moment.

Si l'enregistrement n'était pas préconfiguré, il est encore possible d'enregistrer le support après le démarrage de la machine depuis ce dernier.

Pour préconfigurer l'enregistrement sur le serveur de gestion

1. Cochez la case **Enregistrer le support sur le serveur de gestion**.
2. Dans **Nom du serveur ou IP**, spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé. Vous pouvez utiliser l'un des formats suivants :
   - `http://<serveur>`. Par exemple, `http://10.250.10.10` ou `http://server1`
   - `<adresse IP>`. Par exemple, `10.250.10.10`
   - `<nom d'hôte>`. Par exemple, `server1` ou `server1.example.com`
3. Dans **Port**, spécifiez le port qui sera utilisé pour accéder au serveur de gestion. La valeur par défaut est 9877.
4. Dans **Nom affiché**, indiquez le nom qui sera affiché pour cet ordinateur dans la console Web Cyber Protect. Si vous laissez ce champ vide, le nom affiché sera défini sur l'un des paramètres suivants :
   - Si la machine est déjà enregistrée sur le serveur de gestion, elle aura le même nom.
   - Sinon, le nom de domaine complet (FQDN) ou l'adresse IP de la machine seront utilisés.
5. Sélectionnez le compte à utiliser pour enregistrer le support sur le serveur de gestion. Les options suivantes sont disponibles :
   - **Demander le nom d'utilisateur et le mot de passe lors du démarrage**

     Les accréditations devront être fournies à chaque fois qu'une machine démarrera depuis le support.

     Pour un enregistrement réussi, votre compte doit figurer dans la liste des administrateurs du serveur de gestion (**Paramètres** > **Comptes**). Dans la console Web Cyber Protect, le support sera disponible sous l'organisation ou sous une unité spécifique en fonction des permissions accordées au compte spécifié.

     Dans l'interface du support de démarrage, vous pourrez modifier le nom d'utilisateur et le mot de passe en cliquant sur **Outils** > **Enregistrer le support sur le serveur de gestion**.
   - **Enregistrer sous le compte suivant**

     La machine sera enregistrée automatiquement à chaque fois qu'elle démarrera à partir du support.

     Le compte que vous indiquez doit figurer dans la liste des administrateurs du serveur de gestion (**Paramètres** > **Comptes**). Dans la console Web Cyber Protect, le support sera disponible sous l'organisation ou sous une unité spécifique en fonction des permissions accordées au compte spécifié.

     Dans l'interface du support de démarrage, il *ne sera pas* possible de modifier les paramètres d'enregistrement.

Paramètres réseau

Lors de la création du support de démarrage, vous avez la possibilité de 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.

Une fois que l'agent amorçable démarre sur une machine, sa configuration est appliquée sur la carte d'interface réseau (Network Interface Card - NIC) de la machine. Si les paramètres n'ont pas été préconfigurés, l'agent utilise la configuration DHCP automatique. Vous avez également la possibilité de configurer les paramètres réseau manuellement lorsque l'agent amorçable est en cours d'exécution sur la machine.

Préconfiguration de plusieurs connexions réseau

Vous pouvez préconfigurer les paramètres TCP / IP pour dix cartes d'interface 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 NIC existante dans la fenêtre de l'assistant, ses paramètres sont sélectionnés pour enregistrement 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 NIC inexistante, si besoin.

Une fois que l'agent amorçable démarre sur le serveur, il récupère la liste des NIC disponibles. La liste est classée par logement occupé par les cartes réseau : la plus proche du processeur est en haut.

L'agent amorçable affecte les paramètres appropriés à chaque NIC connue, identifiant les NIC par l’adresse MAC. Une fois que les NIC ayant une adresse MAC connue sont configurées, les paramètres que vous avez créés pour les NIC inexistantes sont affectés aux NIC restantes en commençant par la NIC la plus haute.

Vous pouvez personnaliser un support amorçable pour n'importe quelle machine, et pas seulement pour la machine sur laquelle le support est créé. Pour cela, configurez les NIC en fonction de l'ordre de leur case sur cette machine : NIC1 occupe la case la plus proche du processeur, NIC2 est dans la case suivante et ainsi de suite. Lorsque l'agent amorçable démarre sur cette machine, il ne trouvera pas de NIC ayant une adresse MAC connue et il configurera les NIC dans le même ordre que vous l'avez fait précédemment.

Exemple

L'agent amorçable pourrait utiliser l'un des adaptateurs réseau pour la communication avec la console d’administration au travers du réseau de production. Une configuration automatique pourrait être faite pour cette connexion. Une quantité assez importante de données à restaurer pourrait être transférée à travers la seconde NIC, incluse dans le réseau de sauvegarde dédié au moyen de paramètres TCP / IP statiques.

Port réseau

Lors de la création d'un support de démarrage, vous avez la possibilité de préconfigurer le port réseau que l'agent de démarrage utilise pour les connexions entrantes depuis l'utilitaire `acrocmd`. Le choix est possible entre :

- le port par défaut
- le port actuellement utilisé
- le nouveau port (saisir le numéro du port)

Si le port n'a pas été préconfiguré, l'agent utilise le port 9876.

Pilotes pour Universal Restore

Lors de la création d'un support amorçable, vous avez la possibilité d'ajouter les pilotes Windows sur le support. Les pilotes seront utilisés par Universal Restore pour démarrer Windows s'il a été migré vers un matériel différent.

Vous serez en mesure de configurer Universal Restore :

- pour rechercher dans le support les pilotes qui correspondent le plus au matériel cible
- pour obtenir à partir du support les pilotes de stockage de masse que vous spécifiez explicitement. Ceci est nécessaire quand le matériel cible a un contrôleur de stockage de masse spécifique (tel que SCSI, RAID, ou adaptateur Fiber Channel) pour le disque dur.

Les pilotes seront placés dans le dossier invisible Pilotes sur le support amorçable. Les pilotes ne sont pas chargés sur la RAM de la machine cible, par conséquent, le support doit rester inséré ou connecté pendant toute la durée de l'opération Universal Restore.

L'ajout de pilotes à des supports de démarrage est possible lorsque vous créez un support amovible ou son support ISO ou détachable, tel qu'un lecteur flash. Les pilotes ne peuvent pas être téléchargés sur WDS/RIS.

Les pilotes ne peuvent être ajoutés à la liste que par groupes, en ajoutant les fichiers INF ou les dossiers contenant de tels fichiers. La sélection de pilotes individuels à partir des fichiers INF n'est pas possible, mais le media builder affiche le contenu du fichier pour votre information.

Pour ajouter des pilotes :

1. Cliquez sur **Ajouter** et naviguez vers le fichier INF ou un dossier contenant les fichiers INF.
2. Sélectionnez le fichier INF ou le dossier.
3. Cliquez sur **OK**.

Les pilotes peuvent être supprimés de la liste seulement par groupe, en supprimant les fichiers INF.

Pour supprimer les pilotes :

1. Sélectionnez le fichier INF.
2. Cliquez sur **Supprimer**.

Support de démarrage basé sur WinPE

Bootable Media Builder offre deux méthodes pour intégrer Acronis Cyber Protect avec WinPE :

- Créer une image ISO de PE avec le plug-in depuis le début.
- Ajout du plug-in Acronis à un fichier WIM pour n'importe quelle raison future (création manuelle d'ISO, ajout d'autres outils à l'image et ainsi de suite).

Vous pouvez créer des images PE basées sur WinRE sans préparation supplémentaire, ou créer des images PE après avoir installé le kit d'installation automatisée Windows (AIK) ou le kit de déploiement et d'évaluation Windows (ADK).

Images PE basées sur WinRE

La création d'images basées sur WinRE est prise en charge pour les systèmes d'exploitation suivants :

- Windows 7 (64 bits)
- Windows 8, 8.1, 10 (32 bits et 64 bits)
- Windows Server 2012, 2016, 2019 (64 bits)

Images PE

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 pour Windows 10)

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).

Les images PE basées sur WinPE 4 et versions plus récentes nécessitent environ 1 Go de RAM pour fonctionner.

Remarque
La fonctionnalité de gestion de disques n'est pas disponible pour les supports de démarrage basé sur Windows PE 4.0 et versions ultérieures. Par conséquent, la gestion des disques est prise en charge pour Windows 7 et versions antérieures. Pour exécuter des opérations de gestion des disques sous Windows 8 et versions ultérieures, vous devez installer Acronis Disk Director. Pour plus d'informations, consultez cet article dans la base de connaissances : https://kb.acronis.com/content/47031.

Préparation : WinPE 2.x et 3.x

Pour pouvoir créer ou modifier des images PE 2.x ou 3.x, installez Bootable Media Builder sur une machine sur laquelle le kit d'installation automatisée Windows (AIK) est installé. Si vous n'avez pas de machine avec le AIK, préparez-la comme suit :

Pour préparer une machine avec le AIK

1. Téléchargez et installez le kit d'installation automatisée Windows.
   Kit d'installation automatisée (AIK) pour Windows Vista (PE 2.0) :
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=fr
   Kit d'installation automatisée (AIK) pour Windows Vista SP1 et Windows Server 2008 (PE 2.1) :
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=fr
   Kit d'installation automatisée (AIK) pour Windows 7 (PE 3.0) :
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=fr
   Kit d'installation automatisée (AIK) supplément pour Windows 7 SP1 (PE 3.1) :
   http://www.microsoft.com/fr-fr/download/details.aspx?id=5188
   Vous pouvez prendre connaissance de la configuration requise en suivant les liens ci-dessus.
2. [Facultatif] Gravez le Kit Windows AIK sur un DVD ou copiez-le sur un lecteur flash.
3. Installez Microsoft .NET Framework à partir de ce kit (NETFXx86 ou NETFXx64, selon votre matériel).
4. Installez l'analyseur Microsoft Core XML (MSXML) 5.0 ou 6.0 à partir de ce kit.
5. Installez Windows AIK à partir de ce kit.
6. Installez Bootable Media Builder sur la même machine.

Il est recommandé de vous familiariser avec la documentation d'aide fournie avec Windows AIK. Pour accéder à la documentation, sélectionnez **Microsoft Windows AIK -> Documentation** dans le menu de démarrage.

Préparation : WinPE 4.0 et versions ultérieures

Pour pouvoir créer ou modifier des images PE 4 ou de version ultérieure, installez Bootable Media Builder sur une machine où Windows Assessment and Deployment Kit (ADK) est installé. Si vous n'avez pas de machine avec le ADK, préparez-la comme suit :

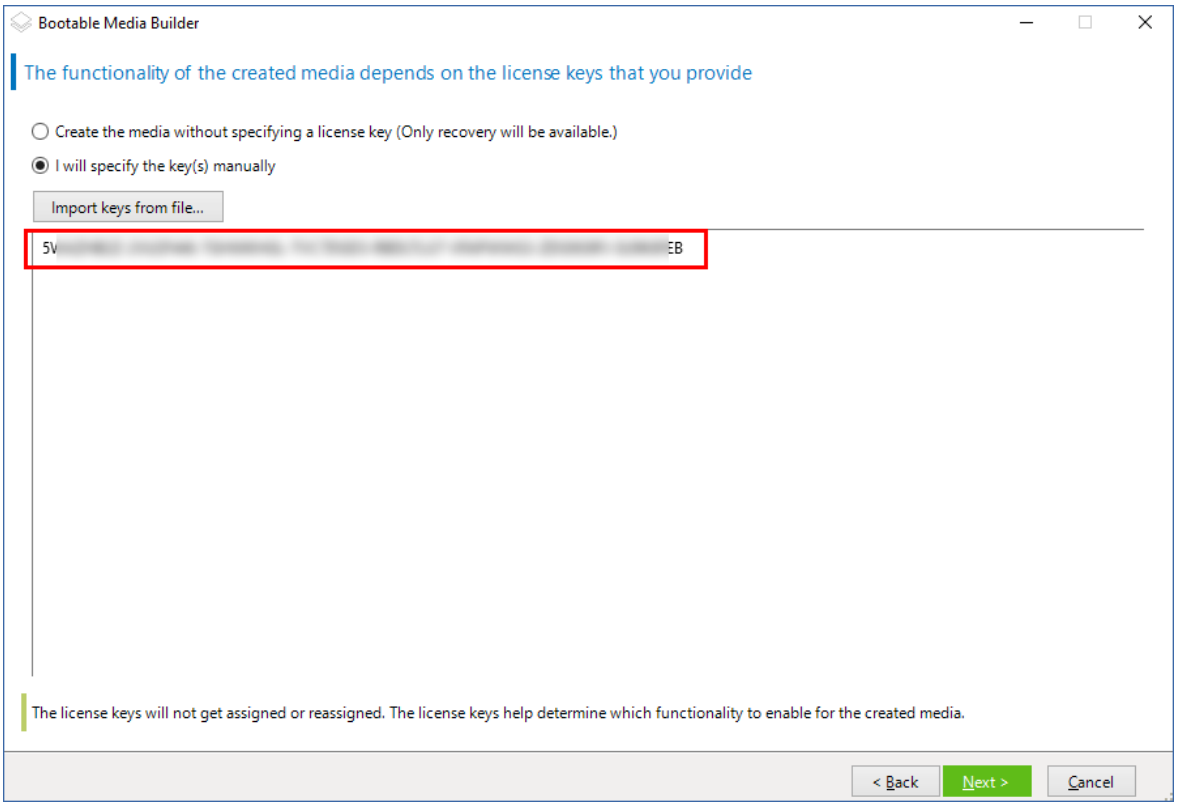
Pour préparer une machine avec le ADK

1. Télécharger le programme d'installation du kit de déploiement et d'évaluation.
   Assessment and Deployment Kit (ADK) pour Windows 8 (PE 4.0) : http://www.microsoft.com/fr-fr/download/details.aspx?id=30652.
   Assessment and Deployment Kit (ADK) pour Windows 8.1 (PE 5.0) : http://www.microsoft.com/fr-fr/download/details.aspx?id=39982.
   Kit de déploiement et d'évaluation Windows (ADK) pour Windows 10 (PE pour Windows 10) : https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.
   Vous pouvez prendre connaissance de la configuration requise en suivant les liens ci-dessus.
2. Installez le kit de déploiement et d'évaluation sur la machine.
3. Installez Bootable Media Builder sur la même machine.

Ajout du plug-in Acronis à WinPE

Pour ajouter le plug-in Acronis à WinPE :

1. Démarrez Bootable Media Builder.
2. Pour créer un support de démarrage complet, spécifiez une clé de licence Acronis Cyber Protect. Cette clé permet de déterminer les fonctionnalités qui seront incluses dans le support de démarrage. Aucune licence ne sera révoquée à partir des ordinateurs.
   Si vous n'indiquez aucune clé de licence, le support de démarrage qui en résulte ne peut être utilisé que pour les opérations de récupération.



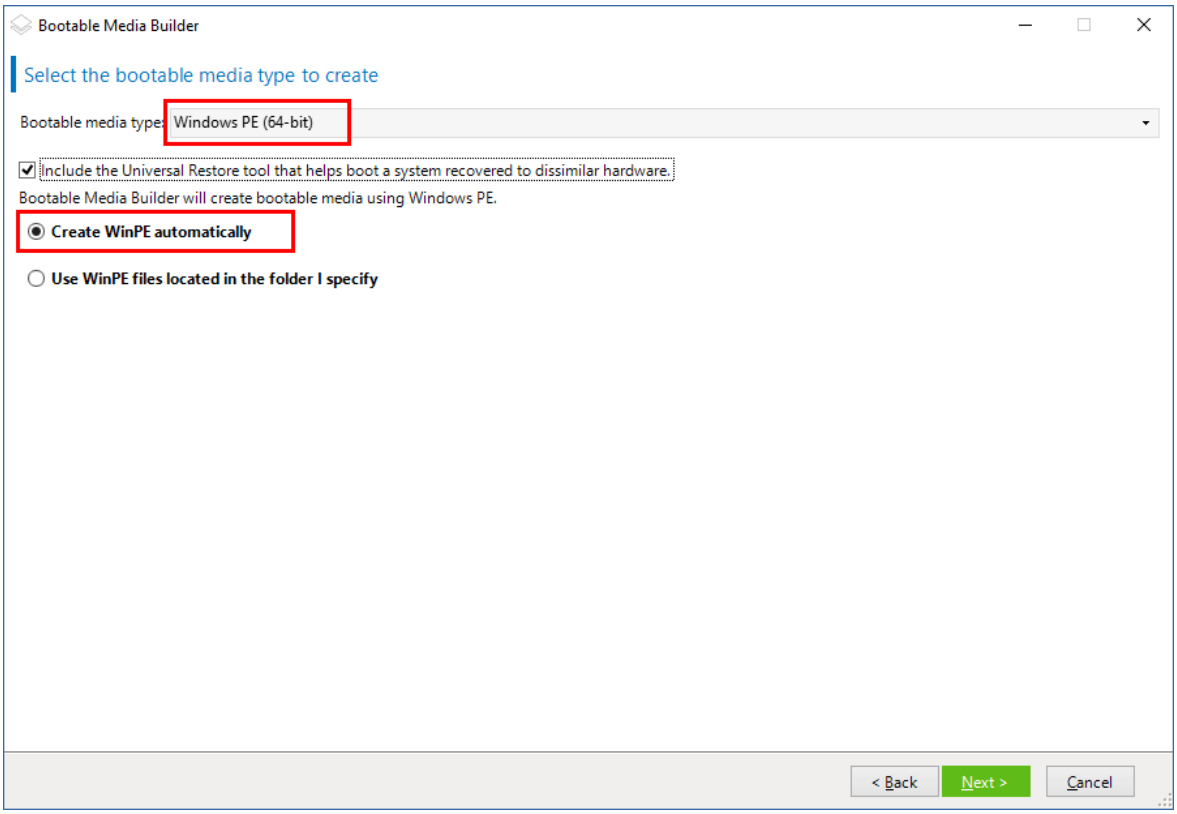
3. Sélectionnez **Type de support de démarrage : Windows PE** ou **Type de support de démarrage : Windows PE (64 bits)**. Un support 64 bits est nécessaire pour démarrer une machine qui utilise l'interface micrologicielle extensible unifiée (Unified Extensible Firmware Interface) (UEFI).

   Si vous avez sélectionné **Type de support de démarrage : Windows PE**, commencez par ce qui suit :

   - Cliquez sur **Télécharger le plug-in pour WinPE (32 bits)**.
   - Enregistrez le plug-in sous **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

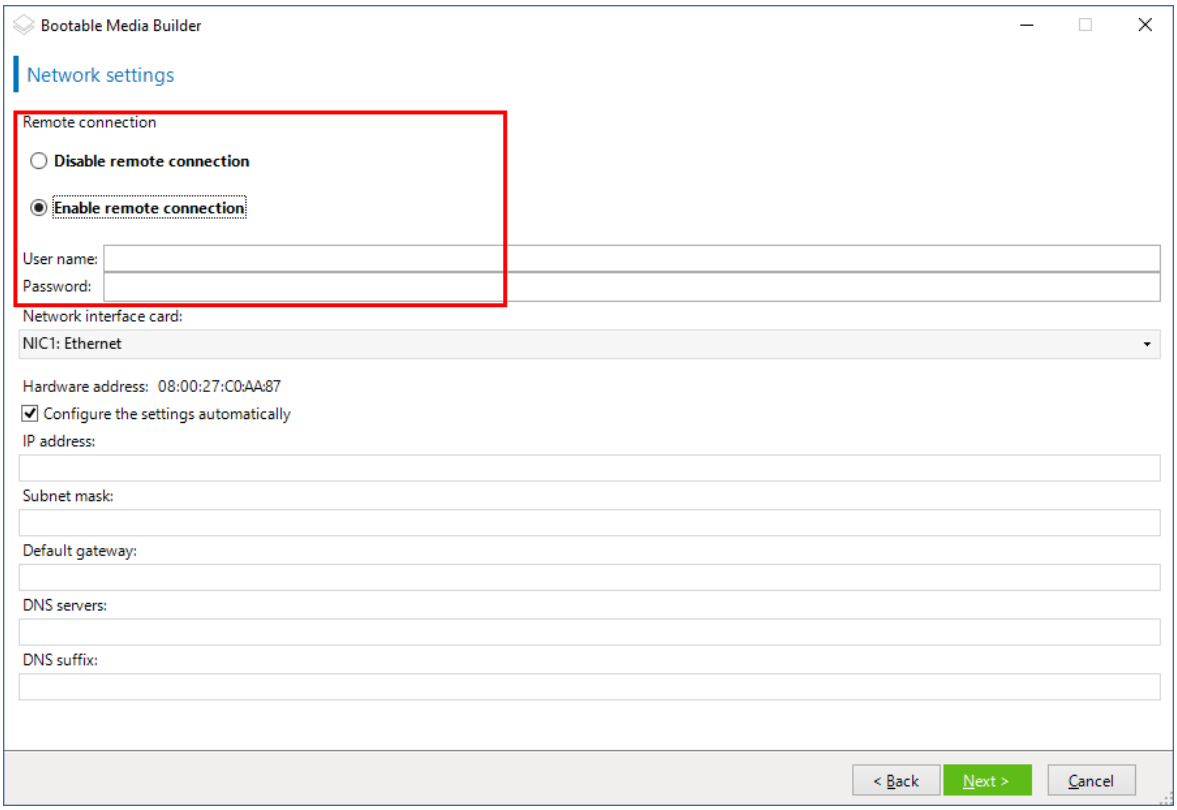
   Si vous prévoyez de restaurer un système d'exploitation sur un matériel différent ou une machine virtuelle et que vous souhaitez vous assurer de la capacité de démarrage du système, cochez la case **Inclure l'outil Universal Restore...**.
4. Sélectionnez **Créer WinPE automatiquement**.

   Le logiciel exécute le script approprié et passe à la fenêtre suivante.



5. Sélectionnez la langue qui sera utilisée dans le support de démarrage.
6. Indiquez si vous voulez activer ou désactiver la connexion à distance à une machine démarrée à partir du support. Si celle-ci est activée, saisissez un nom d'utilisateur et un mot de passe à renseigner dans une ligne de commande si l'utilitaire `acrocmd` est exécuté sur un autre ordinateur. Vous pouvez également laisser ces champs vides, auquel cas la connexion à distance par le biais de la ligne de commande sera possible sans identifiant.

   Ces identifiants sont également requis lorsque vous enregistrez le support sur le serveur de gestion depuis la console Web Cyber Protect.



7. Spécifiez les paramètres réseau pour les adaptateurs réseau de la machine ou choisissez la configuration automatique DHCP.

Remarque
Les paramètres réseau sont disponibles uniquement avec les licences Acronis Cyber Protect 15 Advanced et Acronis Cyber Protect 15 Backup Advanced. Pour comparer en détail les différentes fonctionnalités, consultez cet article de la base de connaissances.

8. [Facultatif] Sélectionnez le mode d'enregistrement du support sur le serveur de gestion lors du démarrage. Pour plus d'informations concernant les paramètres d'inscription, consultez la section Serveur de gestion.
9. [Facultatif] Spécifiez les pilotes Windows à ajouter à Windows PE.

   Après avoir démarré une machine dans Windows PE, les pilotes peuvent vous aider à accéder au périphérique où se trouve la sauvegarde. Ajoutez les pilotes 32 bits si vous utilisez une distribution WinPE 32 bits ou les pilotes 64 bits si vous utilisez une distribution WinPE 64 bits.

   Vous pourrez également pointer vers les pilotes ajoutés lorsque vous configurerez Universal Restore pour Windows. Pour Universal Restore, ajoutez les pilotes 32 bits ou 64 bits selon que vous avez l'intention de restaurer un système d'exploitation Windows 32 bits ou 64 bits.

   Pour ajouter des pilotes :

   - Cliquez sur **Ajouter** et spécifiez le chemin d'accès au fichier .inf nécessaire pour un périphérique SCSI, un disque RAID, un contrôleur SATA, une carte réseau, un lecteur de bandes ou un autre périphérique correspondant.

- Répétez cette procédure pour chaque pilote que vous souhaitez inclure dans le support WinPE résultant.

10. Choisissez si vous voulez créer une image ISO ou WIM, ou transférer le support sur un serveur (WDS ou RIS).
11. Spécifiez le chemin d'accès complet au fichier image obtenu, y compris le nom du fichier, ou spécifiez le serveur et fournissez le nom d'utilisateur et le mot de passe pour y accéder.
12. Vérifiez vos paramètres sur l'écran Résumé et cliquez sur **Continuer**.
13. Gravez l'image .ISO sur CD ou DVD à l'aide d'un outil tiers ou copiez-la vers un lecteur flash de démarrage.

Lorsqu'une machine démarre sous WinPE, l'agent démarre automatiquement.

Pour créer une image de 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:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Utiliser l'outil **Oscdimg**. Pour l'exemple ci-dessus, saisissez :

```
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.

Pour plus d'informations sur la personnalisation de Windows PE 2.x et 3.x, consultez le guide de l'utilisateur de l'environnement de préinstallation Windows (Winpe.chm). Les informations concernant la personnalisation de Windows PE 4.0 et versions ultérieures sont disponibles dans la bibliothèque Microsoft TechNet.

Connexion à une machine démarrée à partir d'un support

Quand une machine est démarrée à partir d'un support amorçable, le terminal de la machine affiche une fenêtre système avec la(les) adresse(s) IP obtenue(s) à partir de DHCP ou configurée(s) 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** qui apparaît vous permet de configurer les paramètres réseau pour chaque carte d'interface réseau (NIC) de la machine.

Les modifications apportées pendant une session seront perdues après le redémarrage de la machine.

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**.

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.

Connexion à distance

Pour vous connecter au support à distance, enregistrez-le sur le serveur de gestion comme décrit dans la section « Enregistrer le support sur le serveur de gestion ».

Enregistrer le support sur le serveur de gestion

L'enregistrement du support de démarrage vous permet de gérer le support via la console Web Cyber Protect comme s'il s'agissait d'une machine enregistrée. Cela s'applique à tous les supports de démarrage, quelle que soit la méthode de démarrage (support physique, Startup Recovery Manager, serveur Acronis PXE, WDS ou RIS). Cependant, il n'est pas possible d'enregistrer un support de démarrage créé dans macOS.

L'enregistrement du support est possible uniquement si au moins une licence Advanced Acronis Cyber Protect est ajoutée au serveur de gestion.

Vous pouvez enregistrer le support à partir de l'interface utilisateur du support.

Les paramètres d'enregistrement peuvent être préconfigurés dans l'option Serveur de gestion du support de démarrage. Si tous les paramètres d'inscription sont préconfigurés, le support apparaît

automatiquement dans la console Web Cyber Protect. Si certains paramètres sont préconfigurés, certaines étapes des procédures suivantes peuvent ne pas être disponibles.

Enregistrer le support à partir de l'interface utilisateur du support

Le support peut être téléchargé ou créé en utilisant le support de démarrage.

Pour enregistrer le support à partir de l'interface utilisateur du support

1. Démarrez la machine à partir du support.
2. Effectuez l'une des actions suivantes :
   - Dans la fenêtre de démarrage, sous **Serveur de gestion**, cliquez sur **Modifier**.
   - Dans l'interface du support de démarrage, cliquez sur **Outils** > **Enregistrer le support sur le serveur de gestion**.
3. Dans **Vous enregistrer :**, spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé. Vous pouvez utiliser l'un des formats suivants :
   - `http://<serveur>`. Par exemple, `http://10.250.10.10` ou `http://server`
   - `<adresse IP>`. Par exemple, `10.250.10.10`
   - `<nom d'hôte>`. Par exemple, `serveur` ou `serveur.exemple.com`.
4. Dans **Nom d'utilisateur** et **Mot de passe**, indiquez les informations d'identification d'un compte de la liste des administrateurs de serveur de gestion (**Paramètres** > **Comptes**). Dans la console Web Cyber Protect, le support sera disponible sous l'organisation ou sous une unité spécifique en fonction des permissions accordées au compte spécifié.
5. Dans **Nom affiché**, indiquez le nom qui sera affiché pour cet ordinateur dans la console Web Cyber Protect. Si vous laissez ce champ vide, le nom affiché sera défini sur l'un des paramètres suivants :
   - Si la machine est déjà enregistrée sur le serveur de gestion, elle aura le même nom.
   - Sinon, le nom de domaine complet (FQDN) ou l'adresse IP de la machine seront utilisés.
6. Cliquez sur **OK**.

Opérations locales avec support de démarrage

Les opérations avec le support de démarrage sont semblables aux opérations de sauvegarde et de récupération exécutées sur le système d'exploitation en cours d'exécution. Les différences sont les suivantes :

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
Nous vous recommandons 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 sauvegardes créés en utilisant un support de démarrage possèdent des noms de fichiers simplifiés. Des noms standard sont affectés aux sauvegardes seulement si celles-ci sont ajoutées à une archive existante qui possède une dénomination standard, ou si la destination ne prend pas en charge les noms de fichiers simplifiés.
4. Le support de démarrage avec une représentation des volumes de type Linux ne peut pas écrire de sauvegarde sur un volume formaté NTFS. Utilisez plutôt un support avec une représentation des volumes de type Windows si nécessaire. Pour changer la représentation du volume de support de démarrage, cliquez sur **Outils** > **Modifier la représentation des volumes**.
5. Les tâches ne peuvent pas être planifiées. Si vous devez répéter une opération, configurez-la de toutes pièces.
6. 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.
7. Les emplacements de stockage centralisés ne sont pas affichés dans l'arborescence des dossiers de la fenêtre **Archive**.

   Pour accéder à un emplacement de stockage géré, saisissez cette chaîne dans le champ **Chemin d'accès** :

   bsp://adresse_du_nœud/nom_de l'emplacement_de_stockage/

   Pour accéder à un emplacement de stockage centralisé non géré, saisissez le chemin d'accès complet vers le dossier de l'emplacement de stockage.

   Après avoir saisi les informations d'identification d'accès, vous verrez une liste des archives situées dans l'emplacement de stockage.

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. Sur la ligne de commande, saisissez **vga=ask**, puis continuez le redémarrage.
3. Choisissez le mode vidéo approprié pris en charge à partir de la liste en entrant son numéro (**318**, par exemple) et appuyez ensuite 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**), en le saisissant dans la fenêtre **Paramètres kernel**.

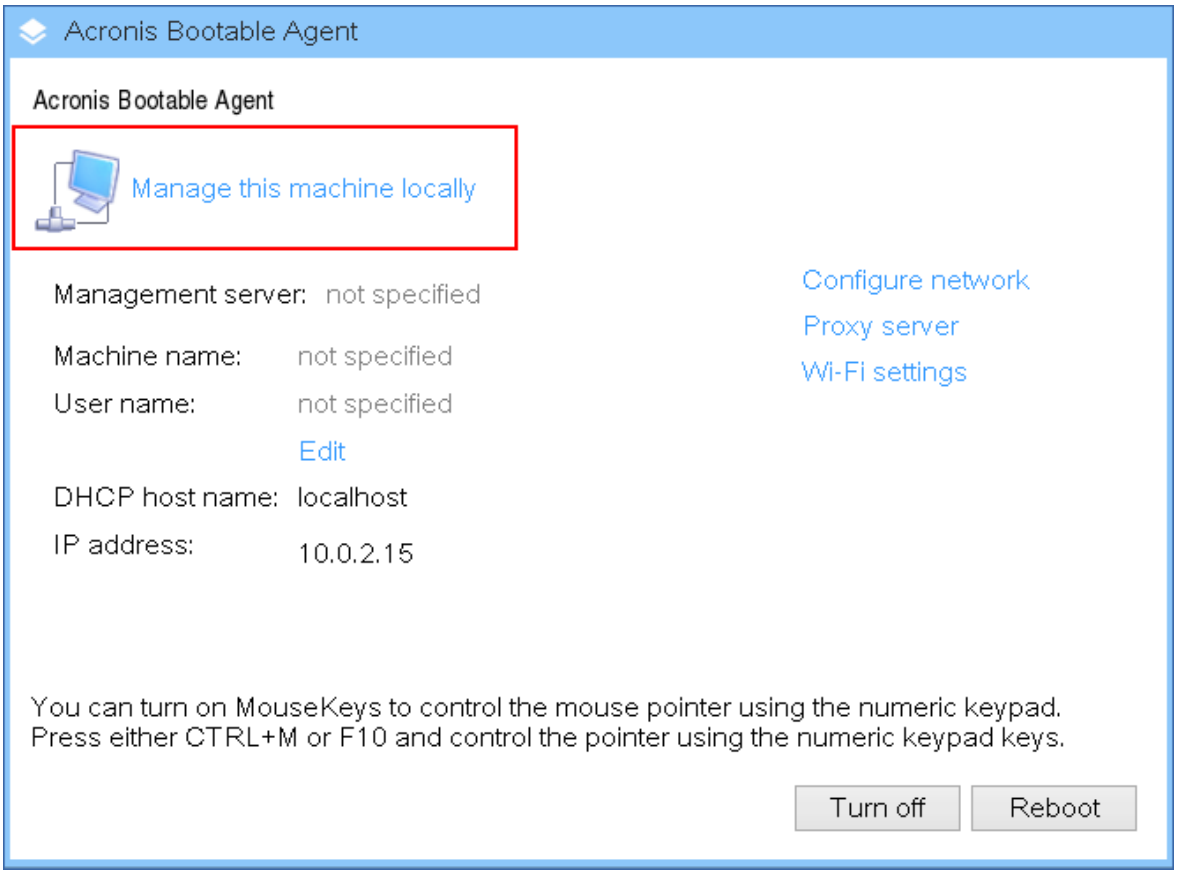
Sauvegarde avec support de démarrage sur site

Vous ne pouvez sauvegarder les données qu'avec un support de démarrage que vous avez créé avec Bootable Media Builder et à l'aide de votre clé de licence Acronis Cyber Protect. Pour plus d'informations sur la création d'un support de démarrage, reportez-vous respectivement aux sections Support de démarrage basé sur un environnement Linux ou Support de démarrage basé sur un environnement Windows-PE.

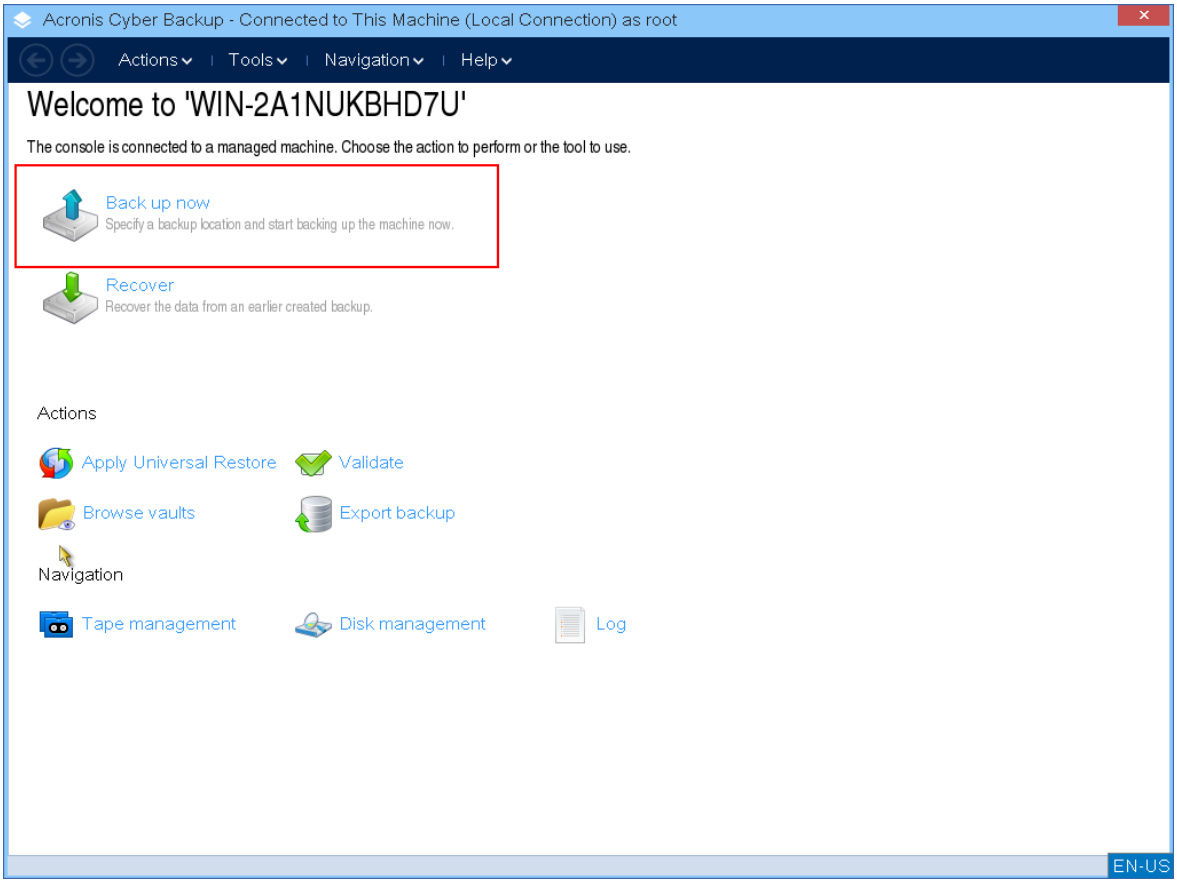
Pour sauvegarder des données sur le support de démarrage

1. Démarrez à partir du support de secours amorçable Acronis.

2. Pour sauvegarder la machine locale, cliquez sur **Gérer cet ordinateur localement**. Pour les connexions à distance, reportez-vous à Enregistrer le support sur le serveur de gestion.



3. Cliquez sur **Sauvegarder maintenant**.

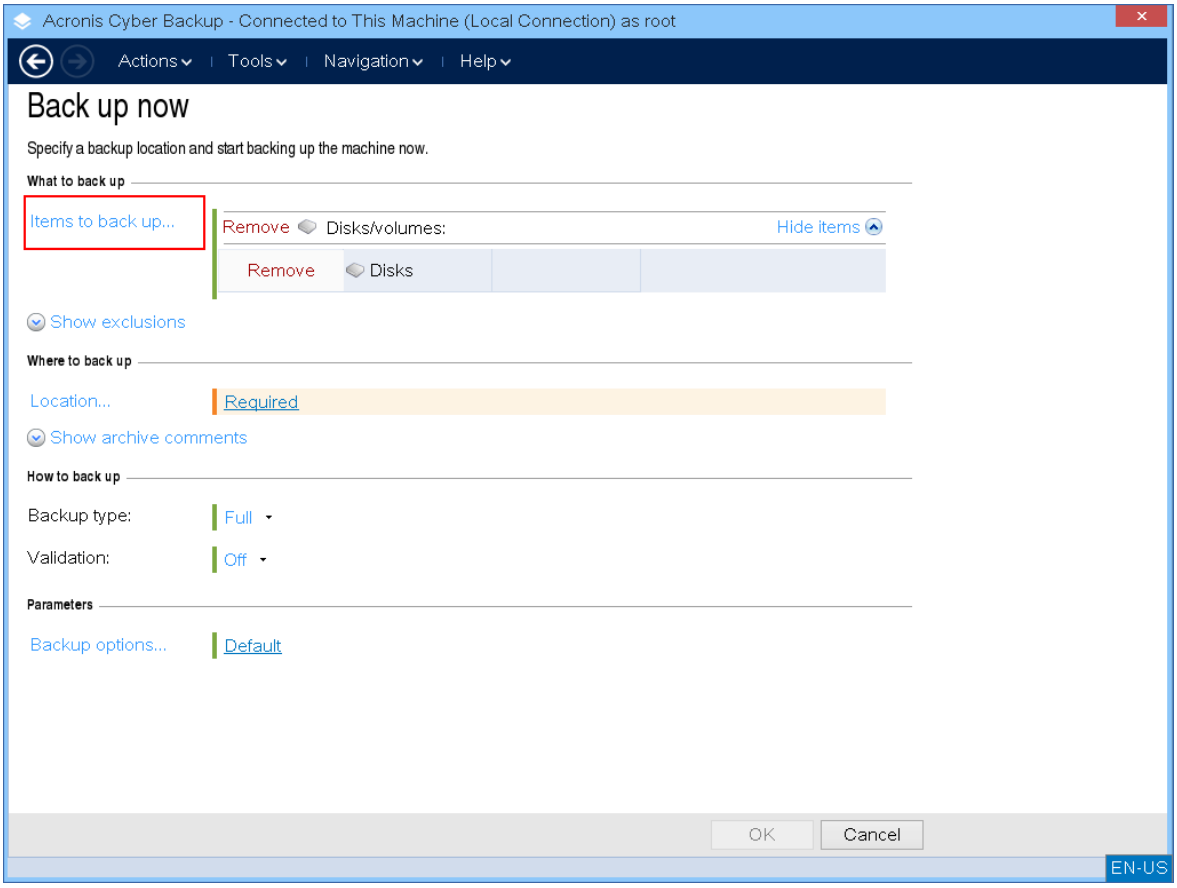


4. Tous les disques non amovibles de l'ordinateur sont sélectionnés automatiquement pour la sauvegarde. Pour modifier les données qui seront sauvegardées, cliquez sur **Éléments à sauvegarder**, puis sélectionnez le disque ou le volume souhaité.

   Lorsque vous sélectionnez les données à sauvegarder, le message suivant peut s'afficher : « *Cet ordinateur ne peut pas être sélectionné directement. Une version antérieure de l'agent est installée sur la machine. Utilisez les règles pour sélectionner cet ordinateur pour la sauvegarde.* » Ce problème d'interface peut être ignoré. Continuez en sélectionnant les disques ou volumes que vous souhaitez sauvegarder.

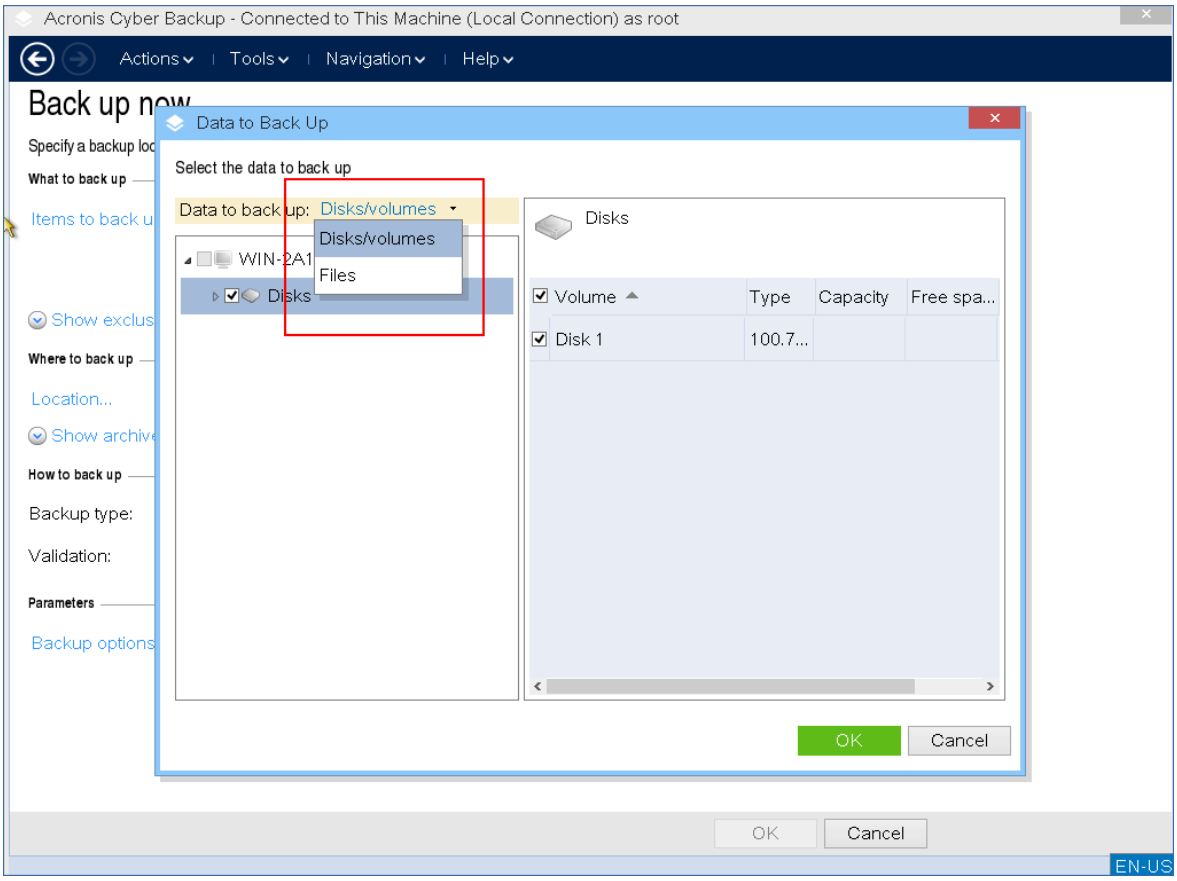
   Remarque

   Avec le support de démarrage basé sur Linux, vous constaterez que les lettres de lecteur sont différentes de celles sous Windows. Essayez d'identifier le lecteur ou la partition dont vous avez besoin en fonction de sa taille ou de son nom.

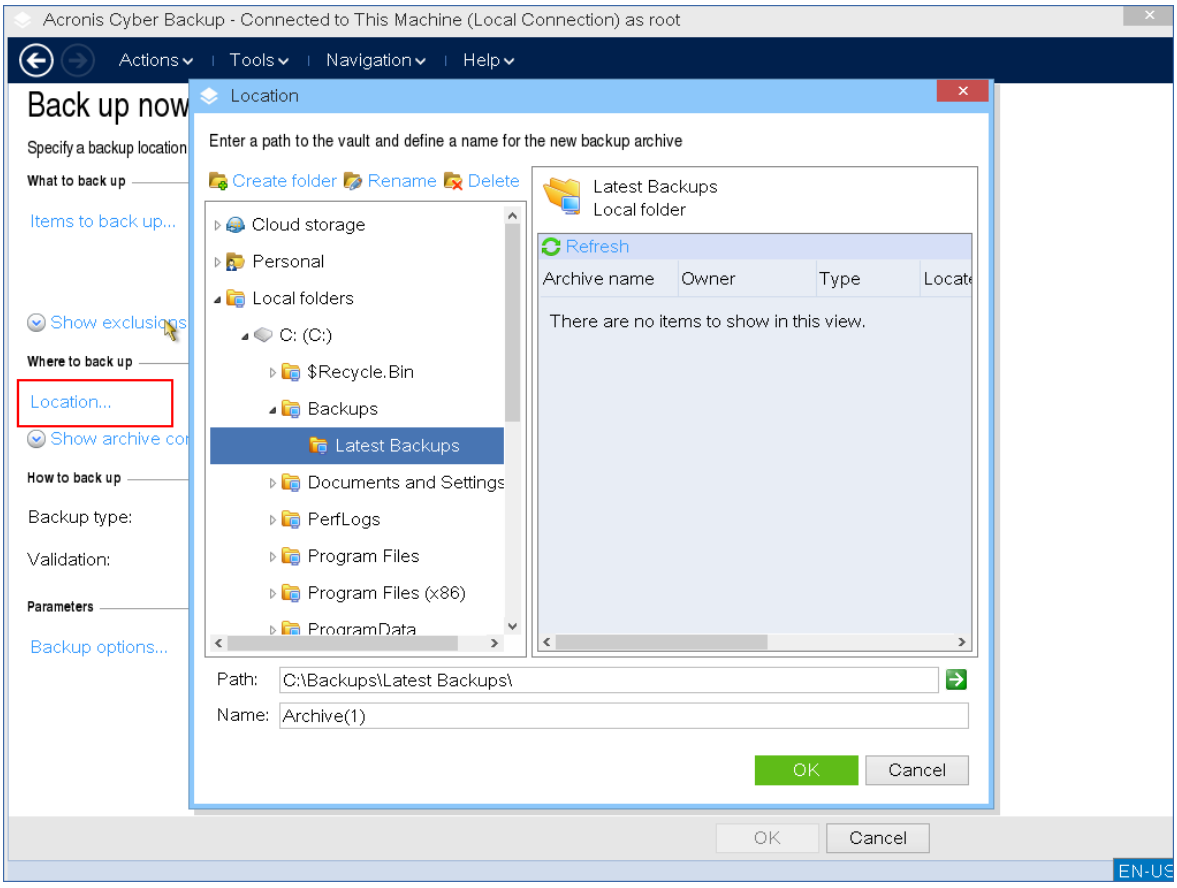


5. Si vous devez sauvegarder des fichiers ou des dossiers au lieu de disques, sélectionnez **Fichiers** dans **Données à sauvegarder**.

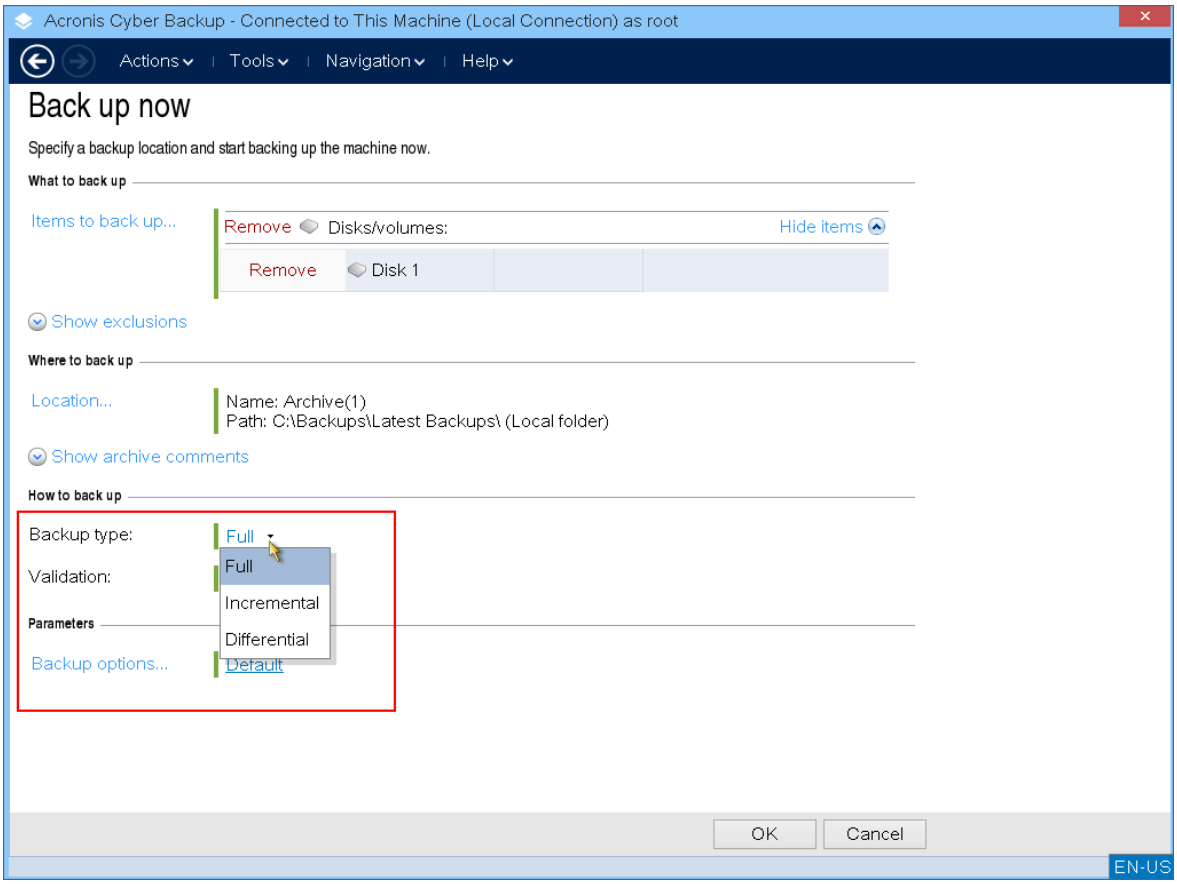
   Seules les sauvegardes disque/partition et fichier/dossier sont disponibles sur le support de démarrage. Les autres types of sauvegarde tels que la sauvegarde de bases de données ne sont disponibles que sur le système d'exploitation en cours d'exécution.



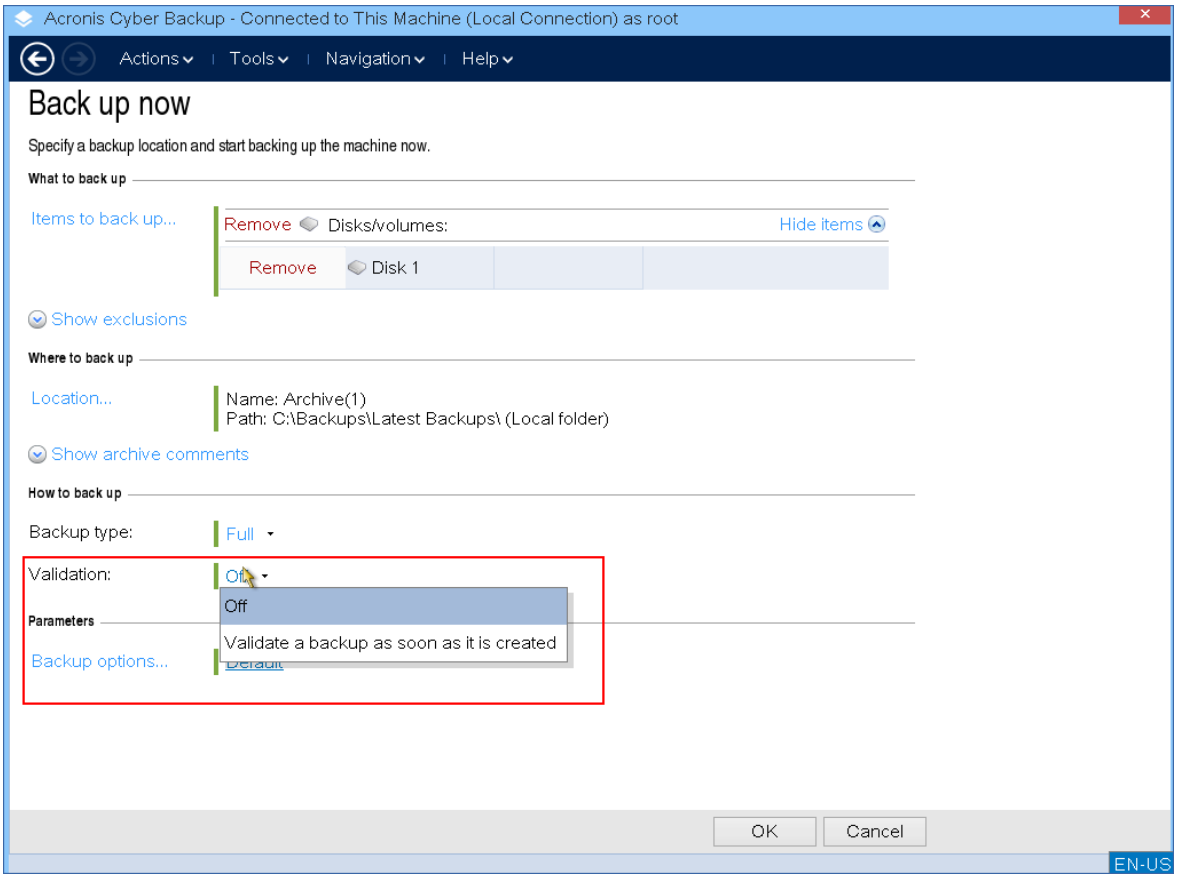
6. Cliquez sur **Emplacement** et sélectionnez l'emplacement d'enregistrement de la sauvegarde.



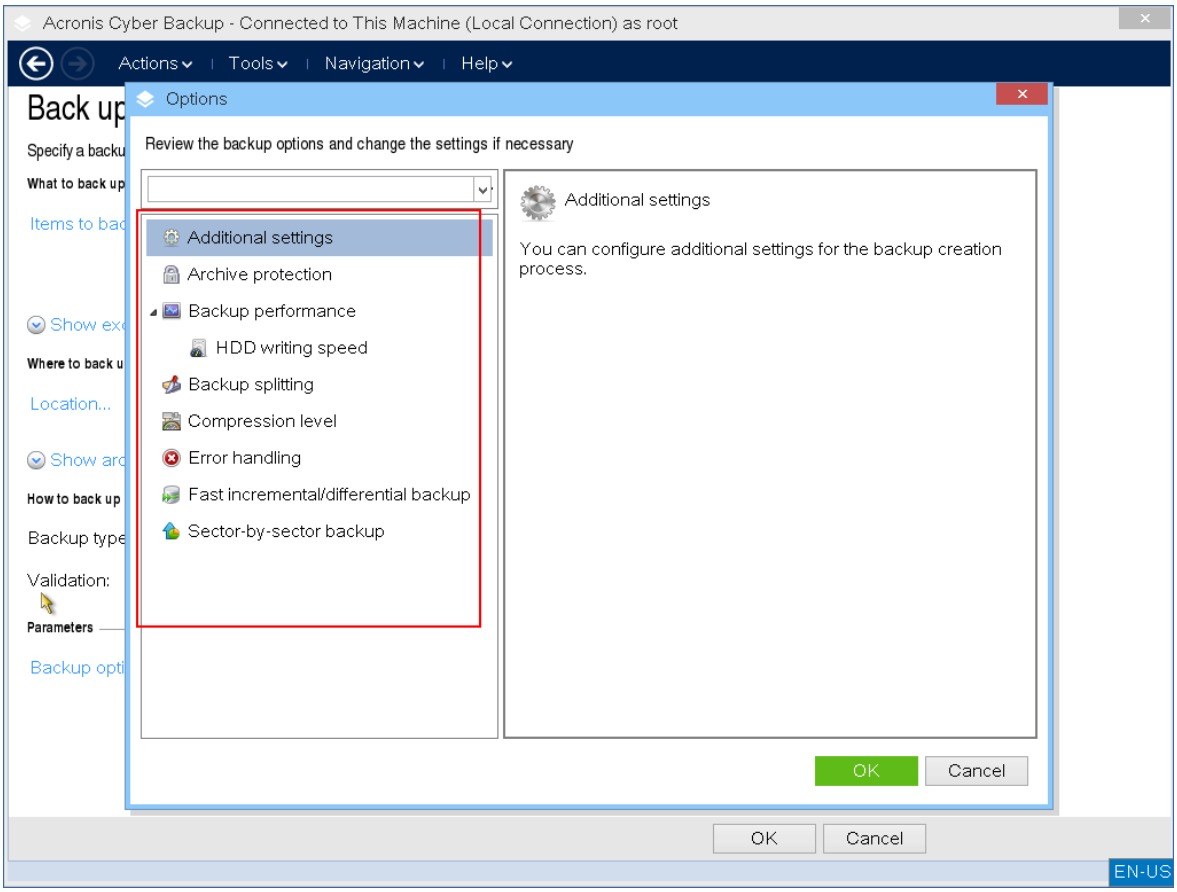
7. Spécifiez l'emplacement et le nom de votre sauvegarde.
8. Spécifiez le type de sauvegarde. S'il s'agit de la première sauvegarde dans cet emplacement, une sauvegarde complète sera créée. Si vous poursuivez une chaîne de sauvegardes, vous pouvez sélectionner **Incrémentielle** ou **Différentielle** pour gagner de l'espace. Pour plus d'informations sur les types de sauvegarde, reportez-vous à l'article https://kb.acronis.com/content/1536.



9. [Facultatif] Si vous souhaitez valider le fichier de sauvegarde, sélectionnez **Valider automatiquement les sauvegardes dès qu'elles sont créées**.

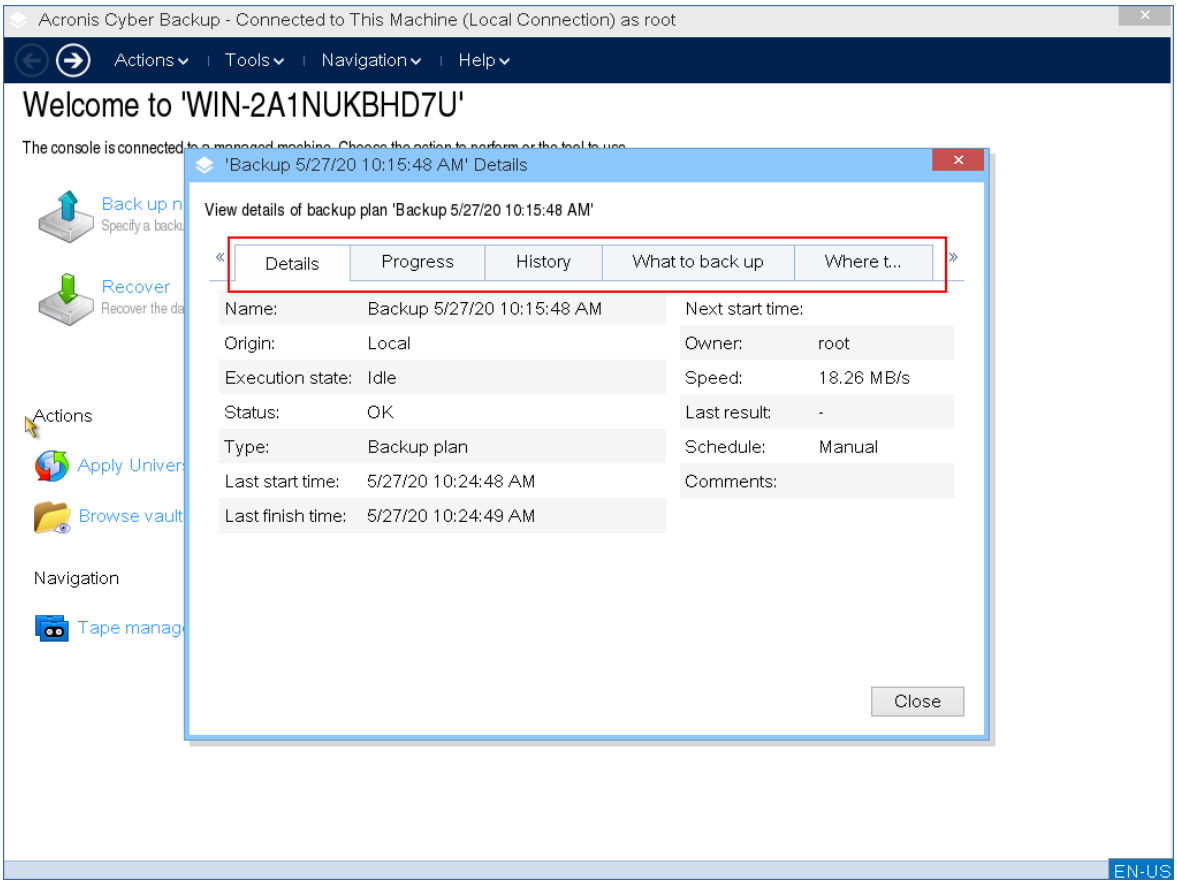


10. [Facultatif] Spécifiez les options de sauvegarde dont vous avez besoin : mot de passe pour le fichier de sauvegarde, fractionnement de la sauvegarde ou traitement des erreurs.



11. Cliquez sur **OK** pour lancer la sauvegarde.

    Le support de démarrage lit les données du disque, les compresse dans un fichier .tib, puis écrit ce fichier dans l'emplacement sélectionné. Il ne crée pas d'instantané de disque, car aucune application n'est en cours d'exécution.
12. Vous pouvez vérifier l'état de la tâche de sauvegarde et d'autres informations concernant la sauvegarde dans la fenêtre qui s'affiche.

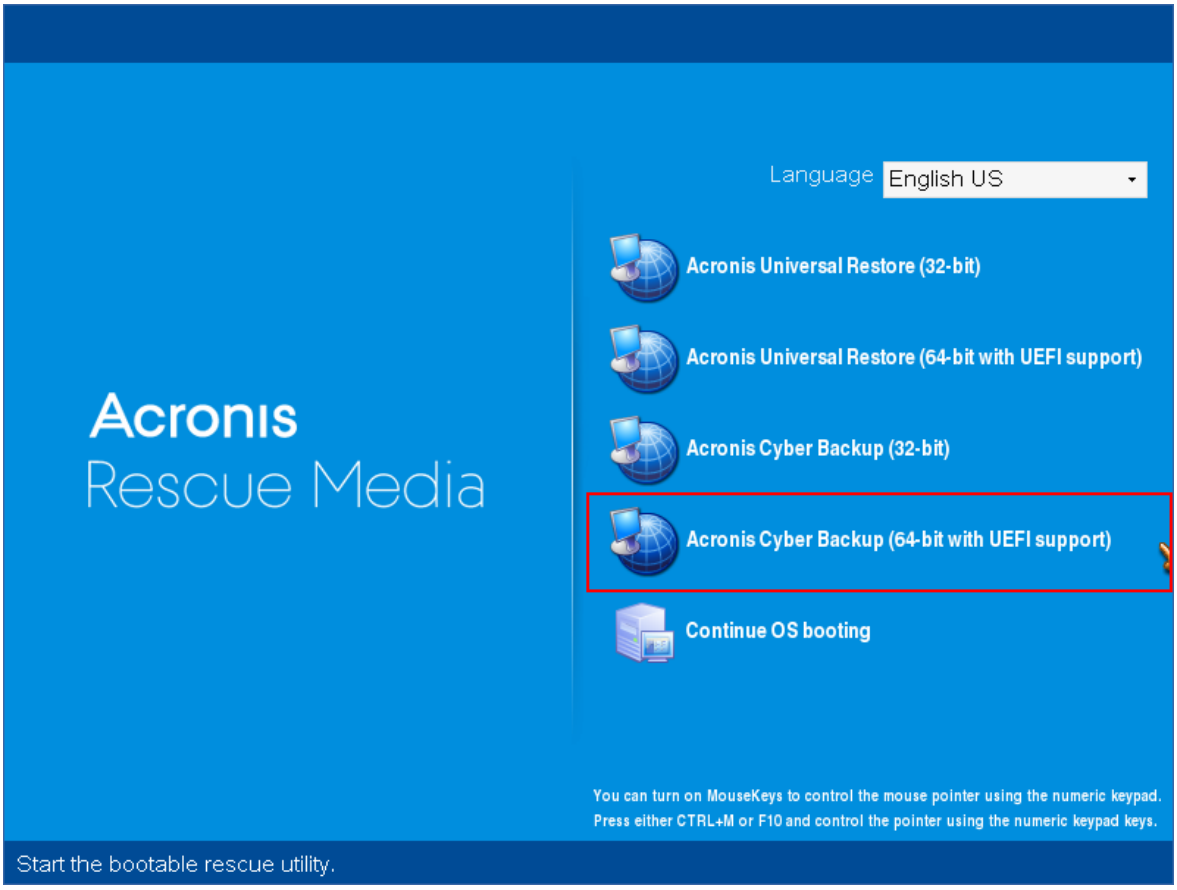


Reprise avec support de démarrage sur site

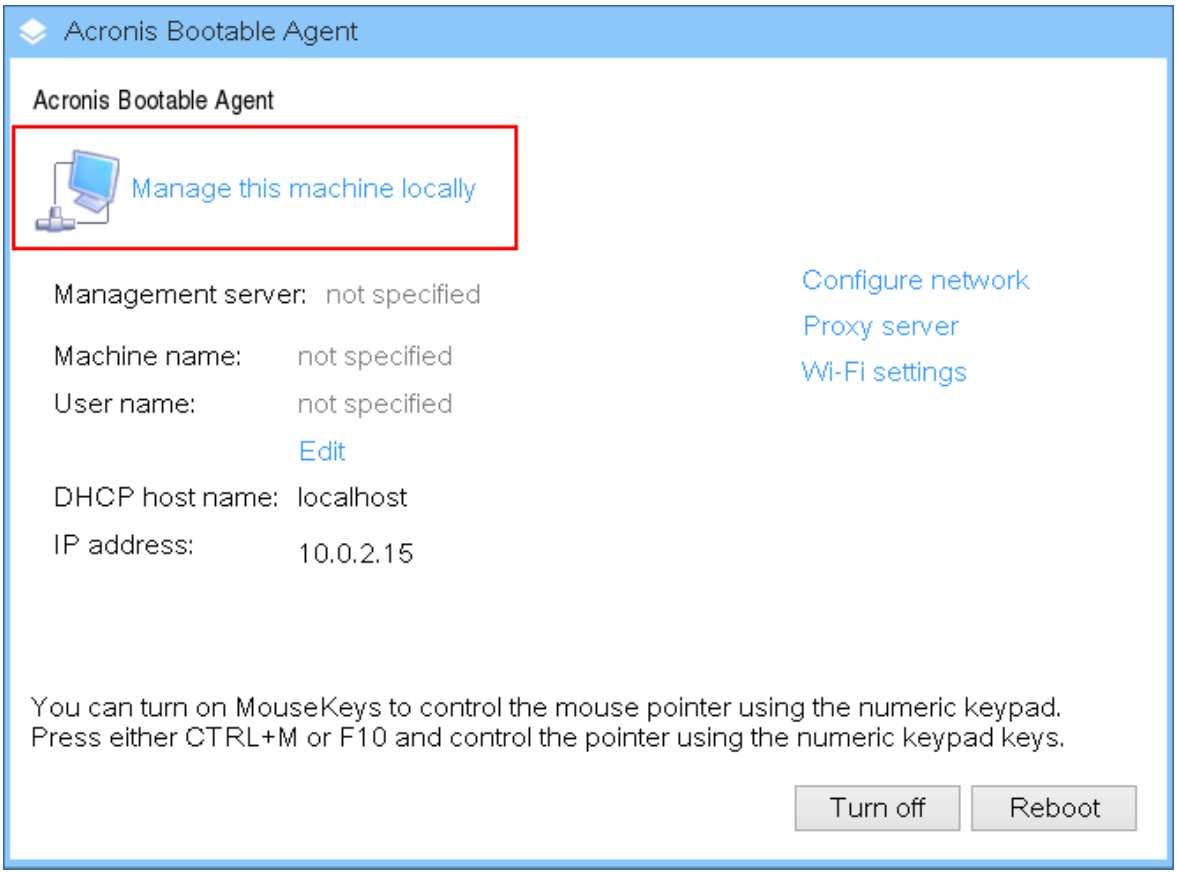
L'opération de récupération est disponible sur le support de démarrage créé avec Bootable Media Builder et sur le support de démarrage tout prêt téléchargé.

Pour récupérer des données sur le support de démarrage

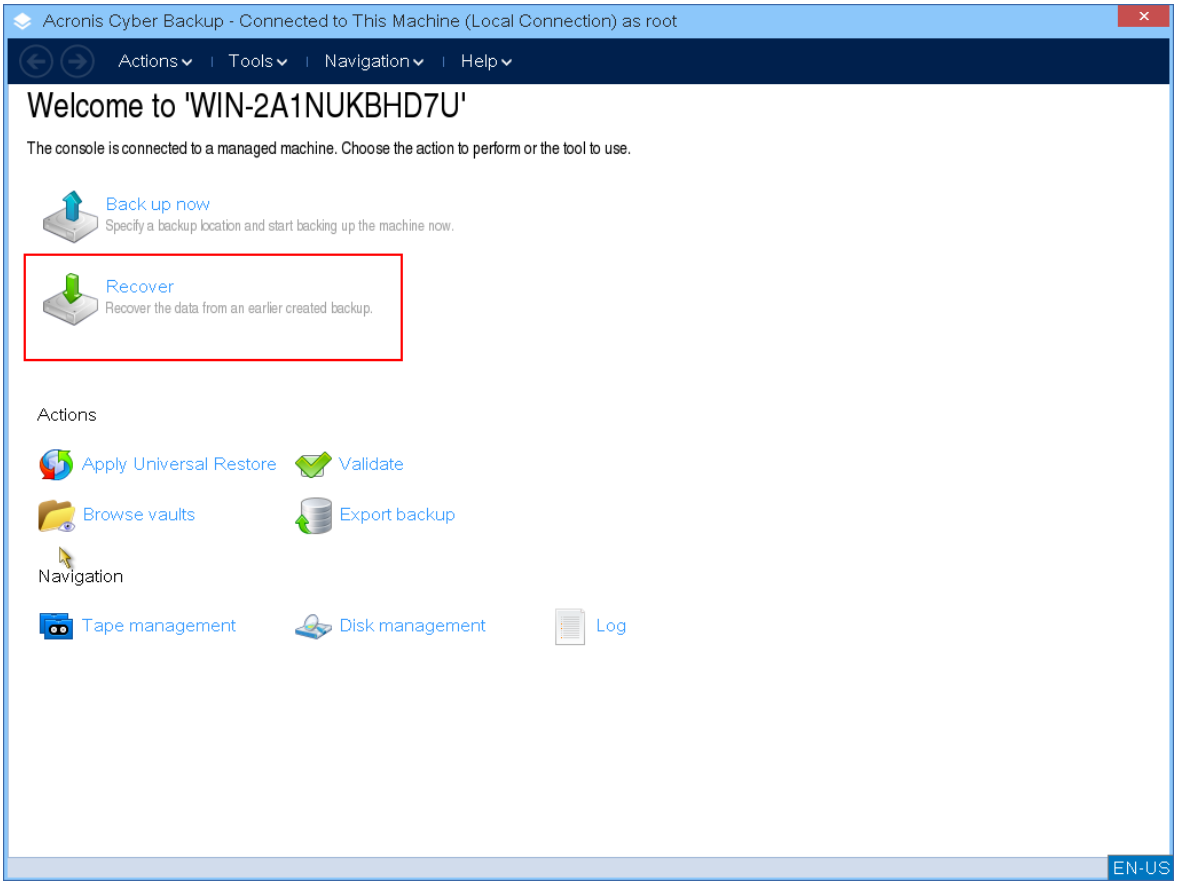
1. Démarrez à partir du support de secours amorçable Acronis.



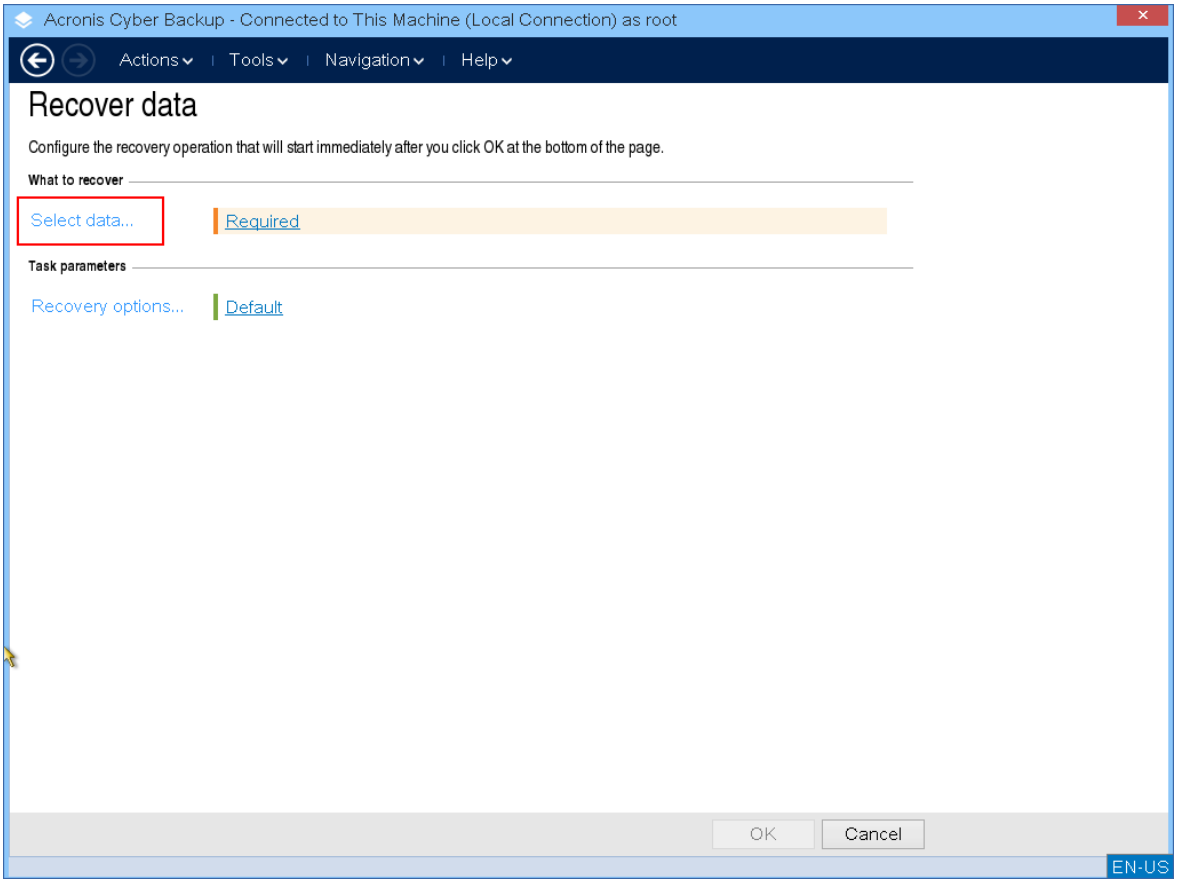
2. Pour récupérer les données sur la machine locale, cliquez sur **Gérer cet ordinateur localement**. Pour les connexions à distance, reportez-vous à Enregistrer le support sur le serveur de gestion.



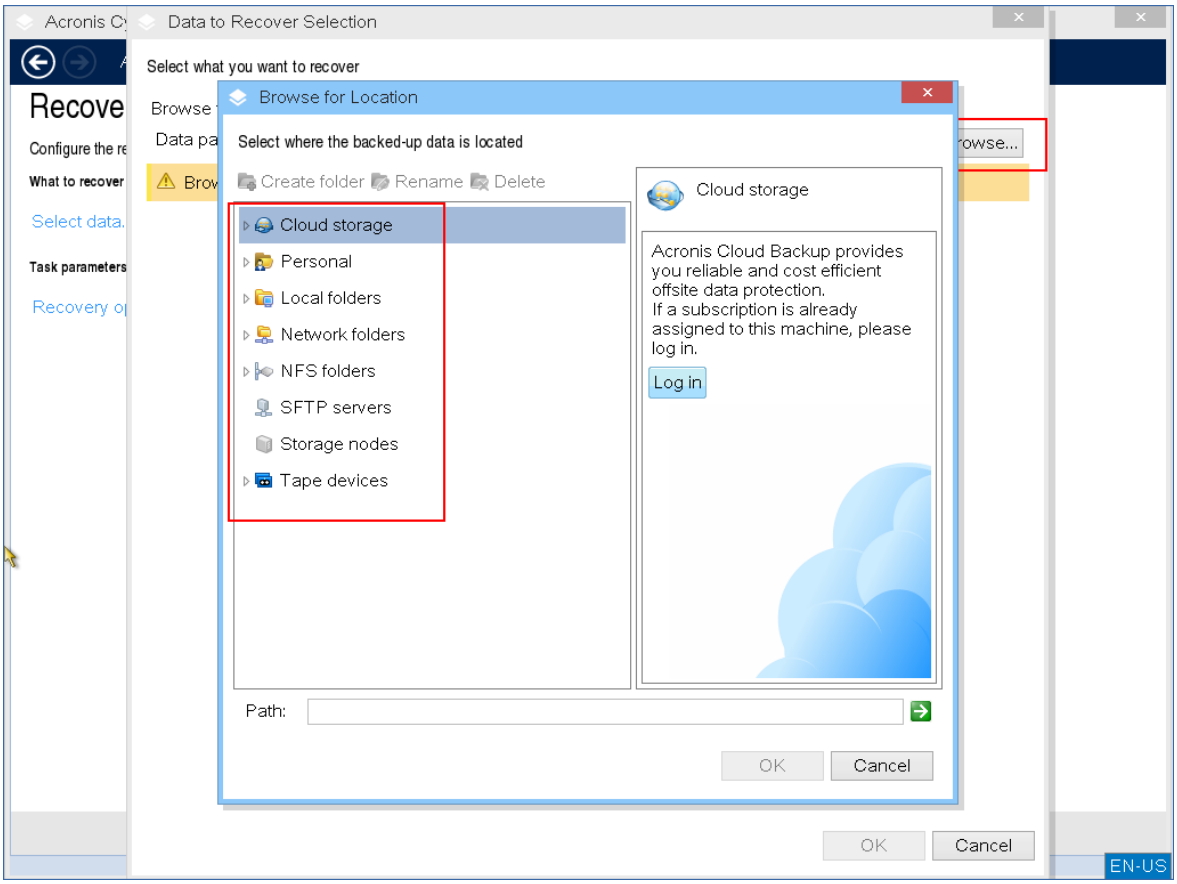
3. Cliquez sur **Restaurer**.



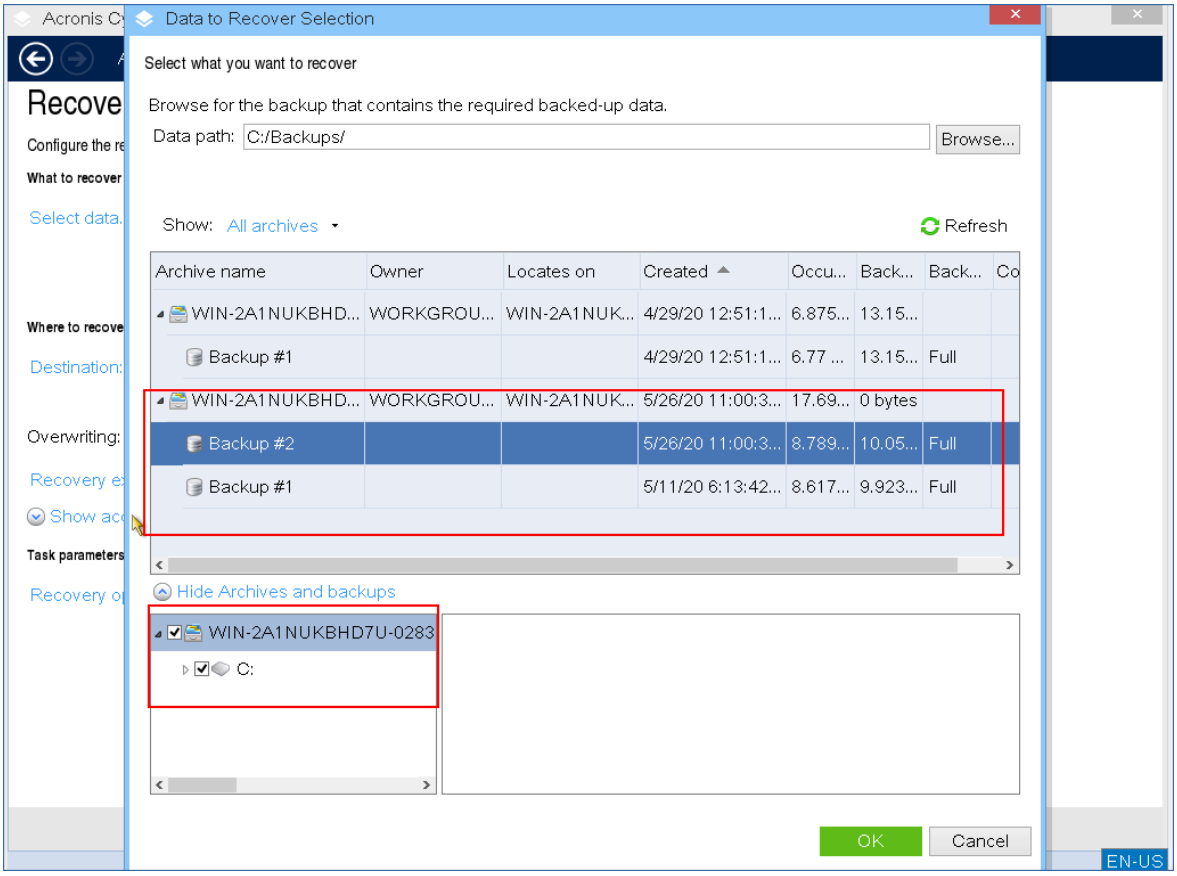
4. Dans **Quoi restaurer**, cliquez sur **Sélectionner les données**.



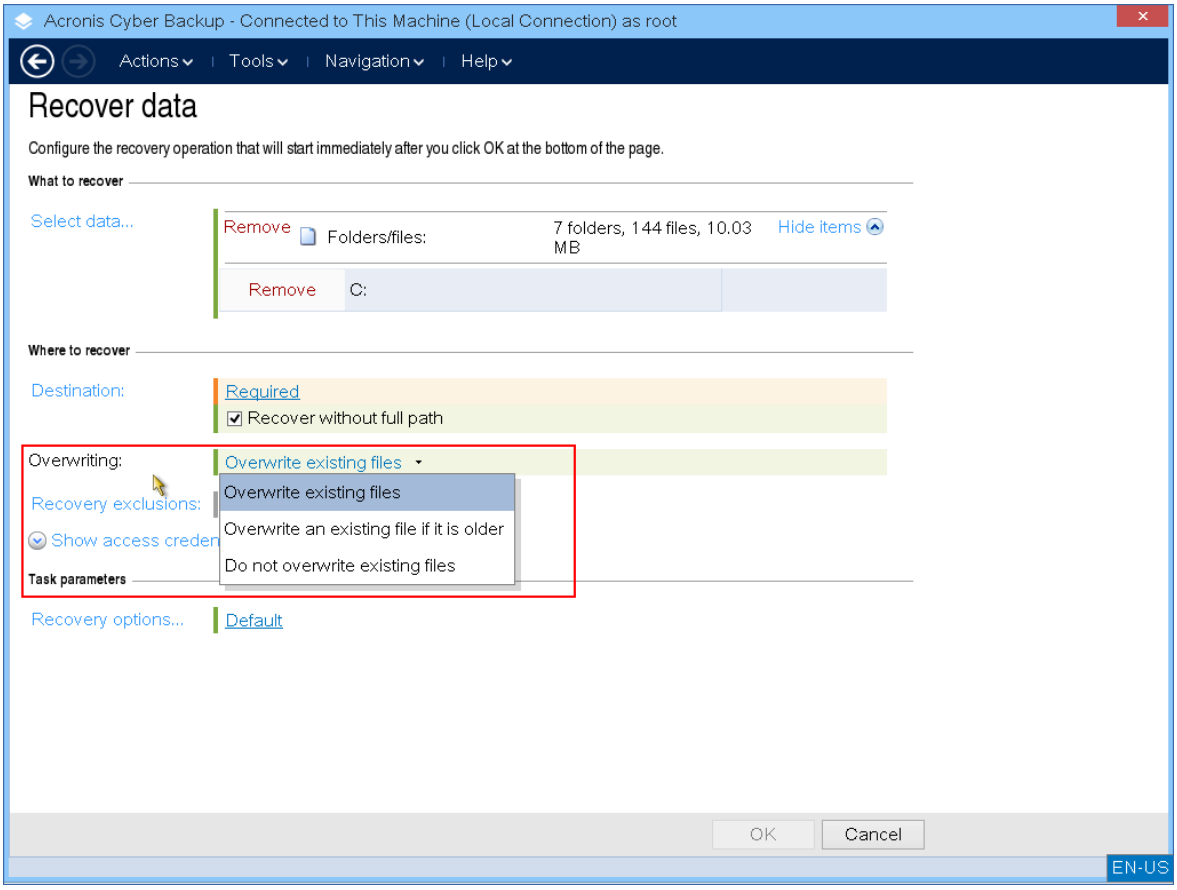
5. Cliquez sur **Parcourir** et sélectionnez l'emplacement de sauvegarde.



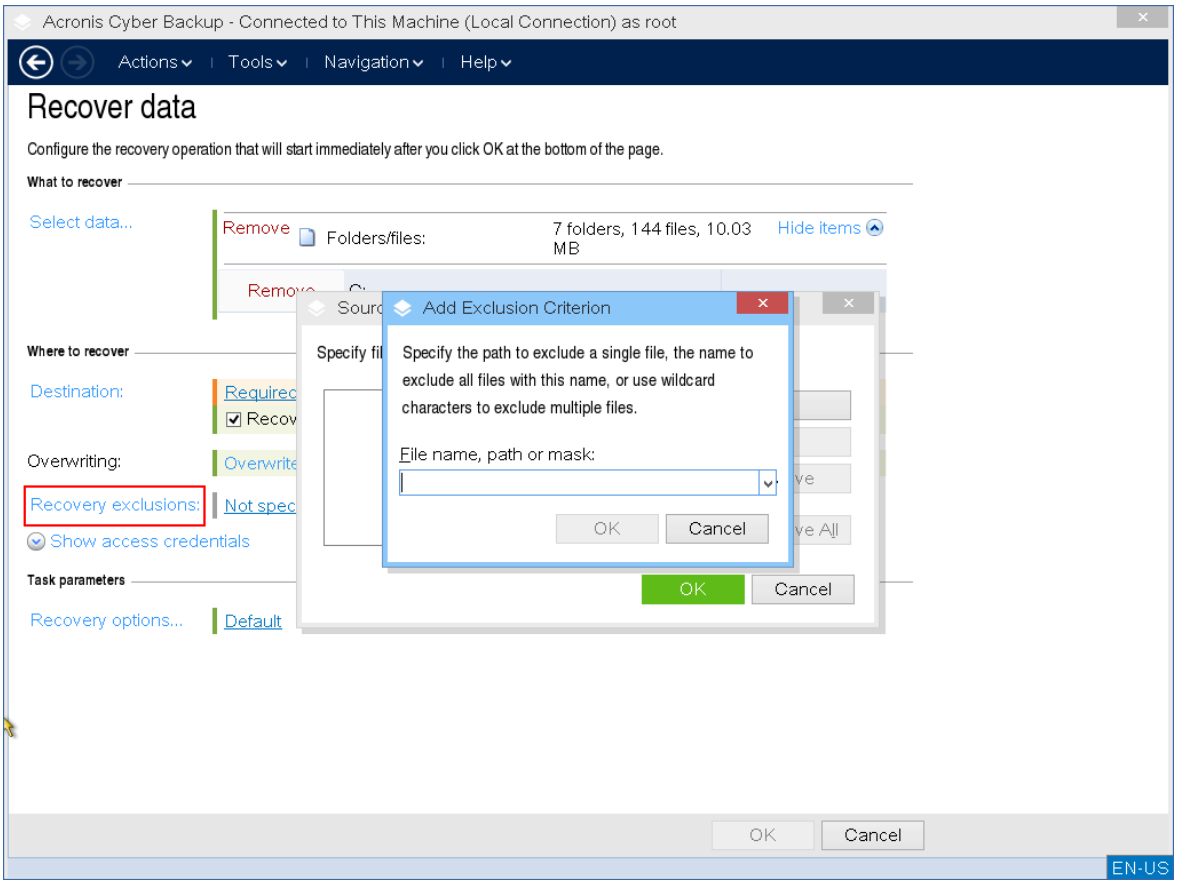
6. Sélectionnez le fichier de sauvegarde à restaurer.



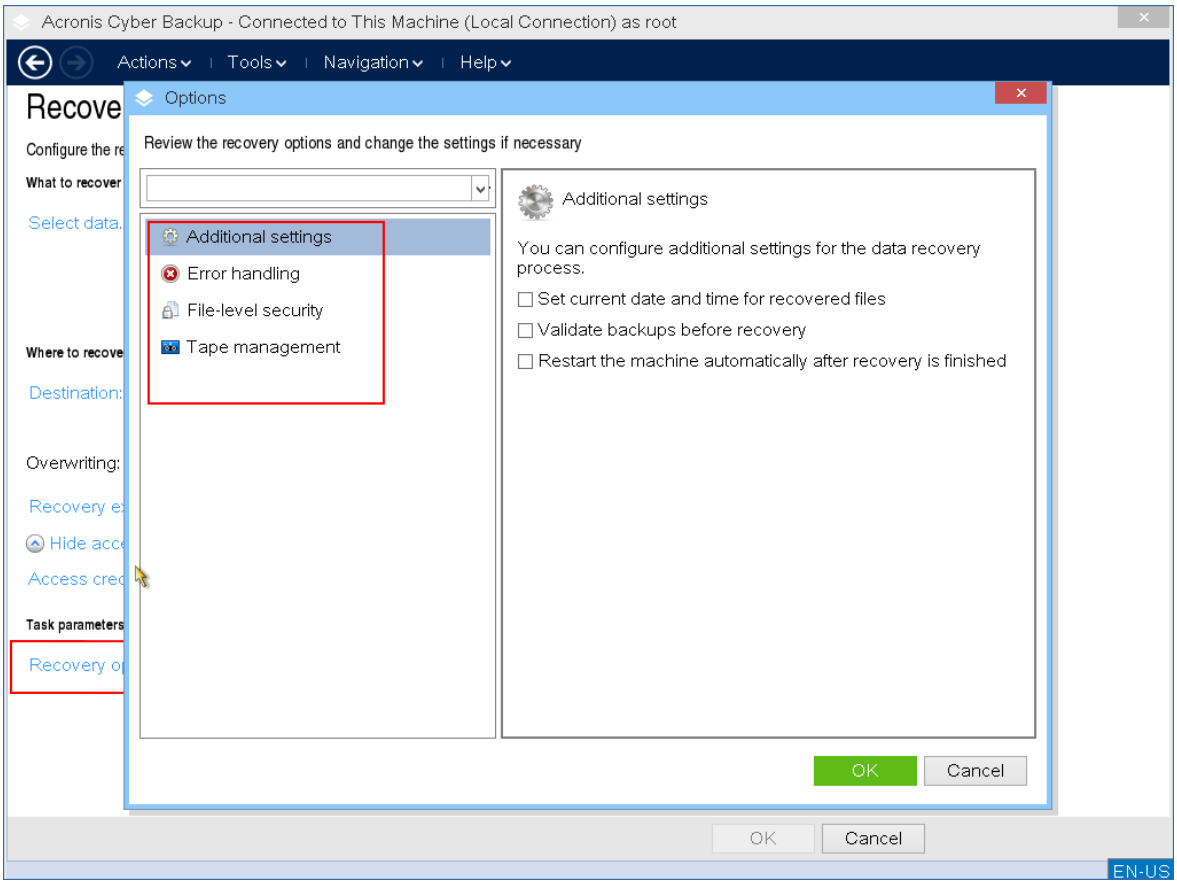
7. Dans le volet inférieur gauche, sélectionnez les lecteurs/volumes (ou fichiers/dossiers) que vous souhaitez restaurer, puis cliquez sur **OK**.
8. [Facultatif] Configurez les règles d'écrasement.



9. [Facultatif] Configurez les exclusions de récupération.



10. [Facultatif] Configurez les options de récupération.



11. Vérifiez que les paramètres sont corrects, puis cliquez sur **OK**.

Remarque

Pour récupérer des données sur un matériel différent, vous devez utiliser Acronis Universal Restore.

Acronis Universal Restore n'est pas disponible lorsque la sauvegarde est située dans Acronis Secure Zone.

Gestion de disques avec support de démarrage

Le support de démarrage Acronis vous permet de préparer une configuration disque/volume pour la restauration des images de volume sauvegardées avec Acronis Cyber Protect.

Parfois, une fois le volume sauvegardé et son image placée dans un stockage sûr, la configuration du disque sur la machine peut changer en raison d'un remplacement de disque dur ou d'une perte de matériel. Dans ce cas, vous pouvez recréer la configuration de disque nécessaire pour que l'image du volume puisse être restaurée exactement « en l'état » ou avec toute modification de la structure des disques ou des volumes que vous considérez comme nécessaire.

Pour éviter d'éventuelles pertes de données, veuillez prendre toutes les précautions nécessaires.

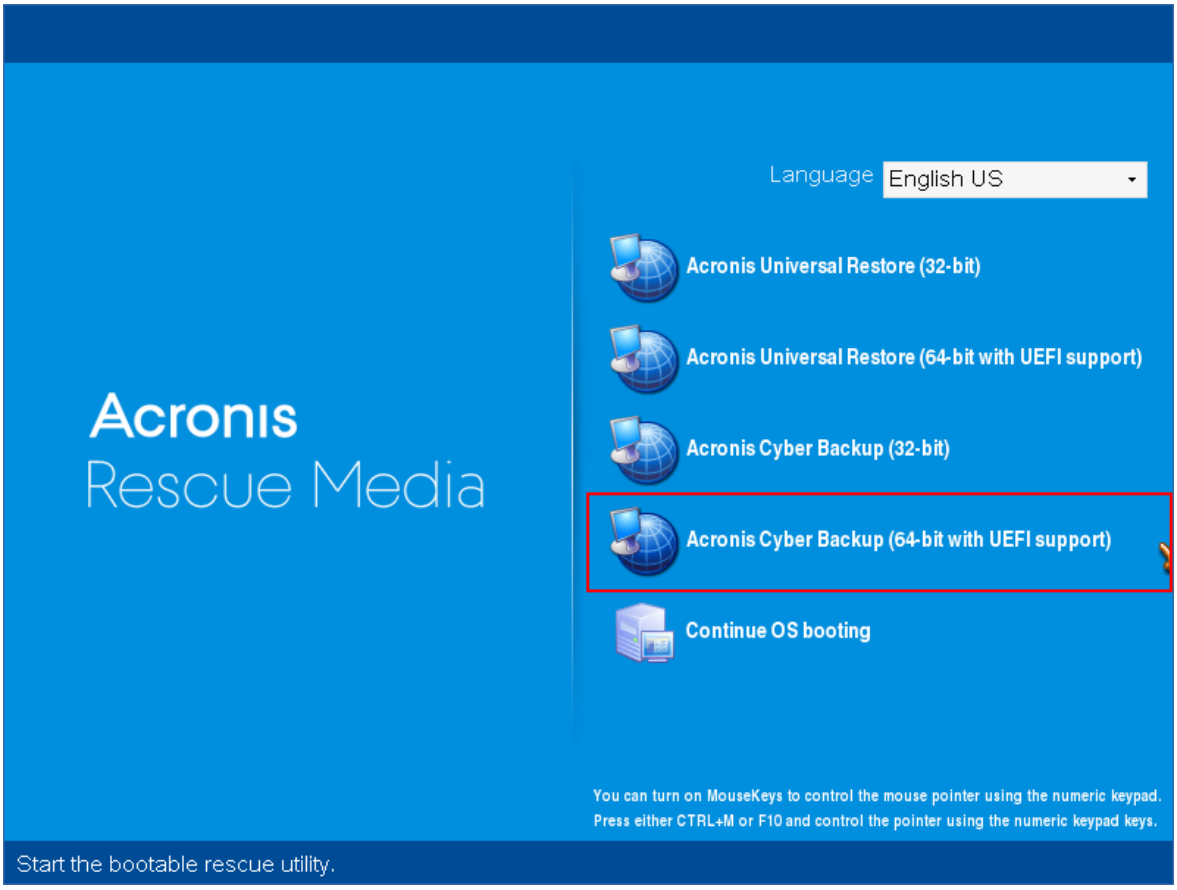
Important
Toutes les opérations sur disques ou volumes comportent un certain risque en termes d'endommagement des données. Les opérations sur le système, les volumes amorçables ou les volumes de données doivent être effectuées très attentivement pour empêcher d'éventuels problèmes liés au démarrage ou au stockage de données sur disque dur.
Les opérations avec les disques durs et volumes prennent un certain temps, et toute coupure de courant, extinction involontaire de l'ordinateur ou appui accidentel sur le bouton Reset pendant la procédure pourrait entraîner l'endommagement de volumes et une perte de données.

Vous pouvez exécuter des opérations de gestion des disques sur un ordinateur vierge ne pouvant pas démarrer ou sur un ordinateur autre que Windows. Vous aurez besoin d'un support de démarrage que vous avez créé avec Bootable Media Builder et à l'aide de votre clé de licence Acronis Cyber Protect. Pour plus d'informations sur la création d'un support de démarrage, reportez-vous respectivement aux sections Support de démarrage basé sur un environnement Linux ou Support de démarrage basé sur un environnement Windows-PE.

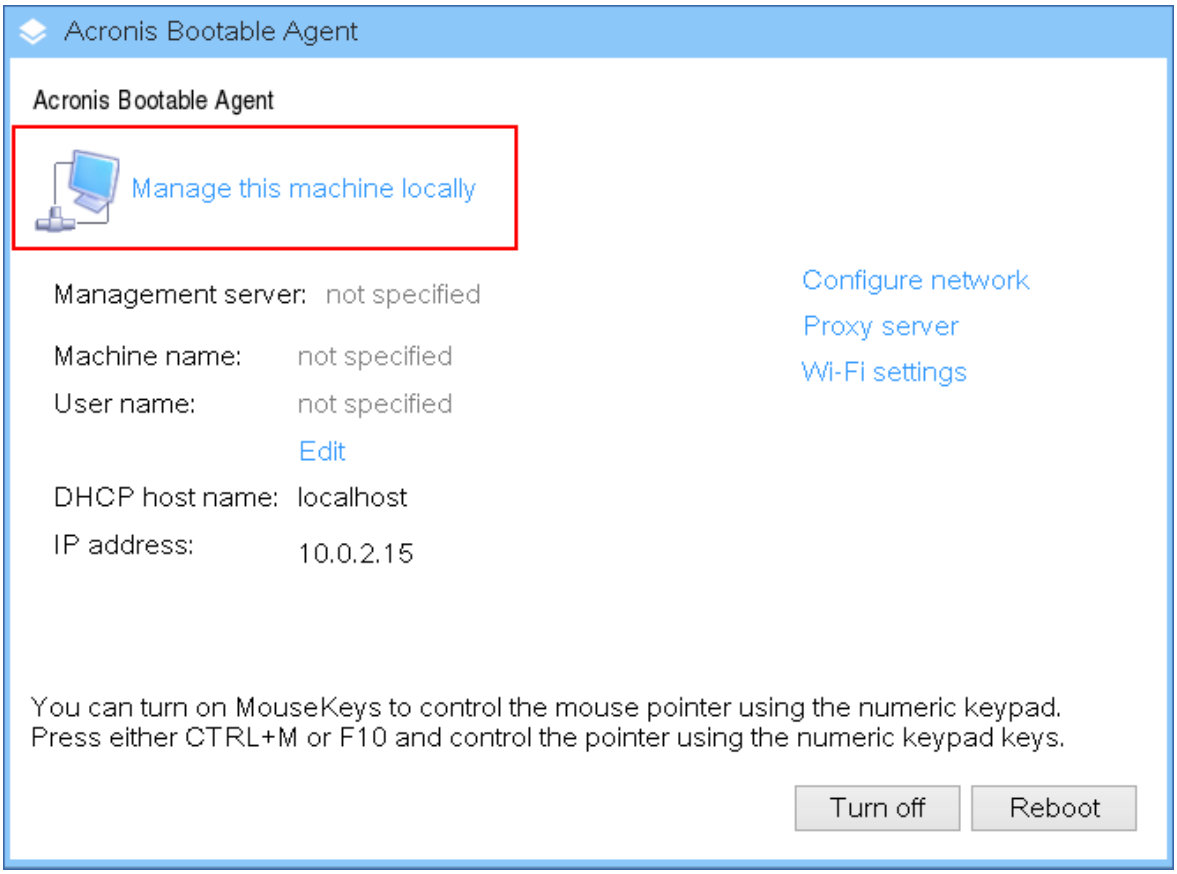
Remarque
La fonctionnalité de gestion de disques n'est pas disponible pour les supports de démarrage basé sur Windows PE 4.0 et versions ultérieures. Par conséquent, la gestion des disques est prise en charge pour Windows 7 et versions antérieures. Pour exécuter des opérations de gestion des disques sous Windows 8 et versions ultérieures, vous devez installer Acronis Disk Director. Pour plus d'informations, consultez cet article dans la base de connaissances : https://kb.acronis.com/content/47031.

Pour exécuter des opérations de gestion des disques

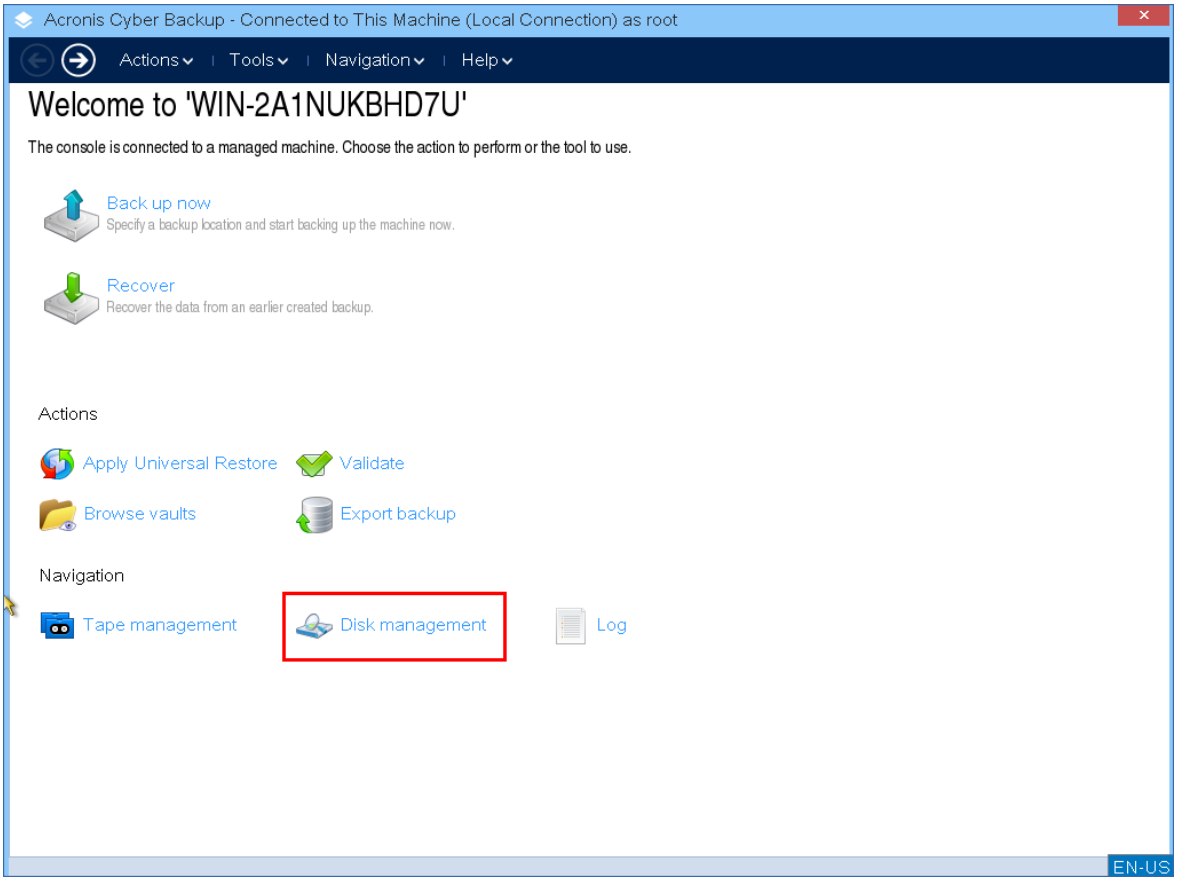
1. Démarrez à partir du support de secours amorçable Acronis.



2. Pour utiliser la machine locale, cliquez sur **Gérer cet ordinateur localement**. Pour les connexions à distance, reportez-vous à Enregistrer le support sur le serveur de gestion.



3. Cliquez sur **Gestion des disques**.



Remarque
Avec un support de démarrage, les opérations de gestion de disques risquent de ne pas fonctionner correctement si les espaces de stockage sont configurés sur la machine.

Systèmes de fichiers pris en charge

Le support de démarrage prend en charge la gestion de disques avec les systèmes de fichiers suivants :

- FAT 16/32
- NTFS

Si vous devez exécuter des opérations sur un volume avec un autre système de fichiers, utilisez Acronis Disk Director. Elle fournit plus d'outils et d'utilitaires pour gérer des disques et des volumes avec les systèmes de fichiers suivants :

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

Précautions basiques

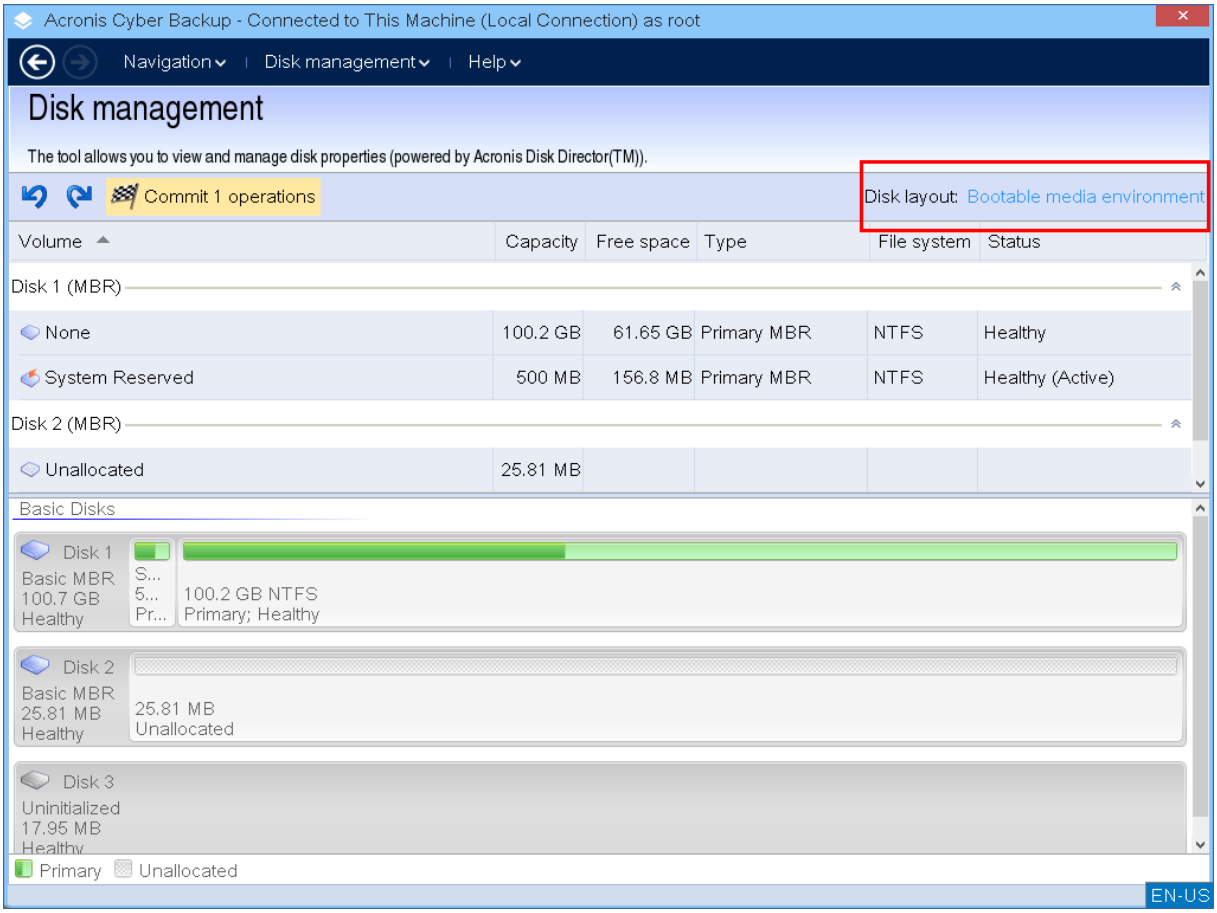
Pour éviter tout dommage de la structure des disques et des volumes ou la perte de données, veuillez prendre toutes les précautions nécessaires et suivre ces règles :

1. Sauvegardez le disque sur lequel les volumes seront créés ou gérés. Conserver vos données sauvegardées les plus importantes sur un autre disque dur, un partage réseau ou un support amovible vous permettra d'utiliser des volumes de disque en sachant que vos données sont en sécurité.
2. Testez votre disque pour vous assurer qu'il fonctionne parfaitement et ne contient pas de secteurs défectueux ou d'erreurs de système de fichiers.
3. N'effectuez pas d'opération sur un disque/volume pendant l'exécution d'autres logiciels ayant accès au niveau inférieur du disque.

Choisir le système d'exploitation pour la gestion de disque

Sur une machine ayant deux systèmes d'exploitation ou plus, la représentation des disques et volumes dépend de quel système d'exploitation est présentement utilisé. Le même volume peut avoir des lettres différentes en fonction des systèmes d'exploitation.

Lorsque vous effectuez une opération de gestion de disques, vous devez spécifier la disposition du disque pour laquelle le système d'exploitation sera affiché. Pour ce faire, cliquez sur le nom du système d'exploitation, à côté de l'étiquette **Disposition du disque**, puis choisissez le système d'exploitation de votre choix dans la fenêtre qui s'ouvre.



Opérations de disque

Grâce au support de démarrage, vous pouvez exécuter les opérations suivantes de gestion de disques :

- Initialisation de disque : initialise le nouveau matériel ajouté au système
- Clonage du disque de base : transfère les données complètes à partir du disque MBR de base de la source vers le disque de destination
- Conversion de disque : MBR vers GPT : convertit une table de partition MBR en GPT
- Conversion de disque : GPT vers MBR : convertit une table de partition GPT en MBR

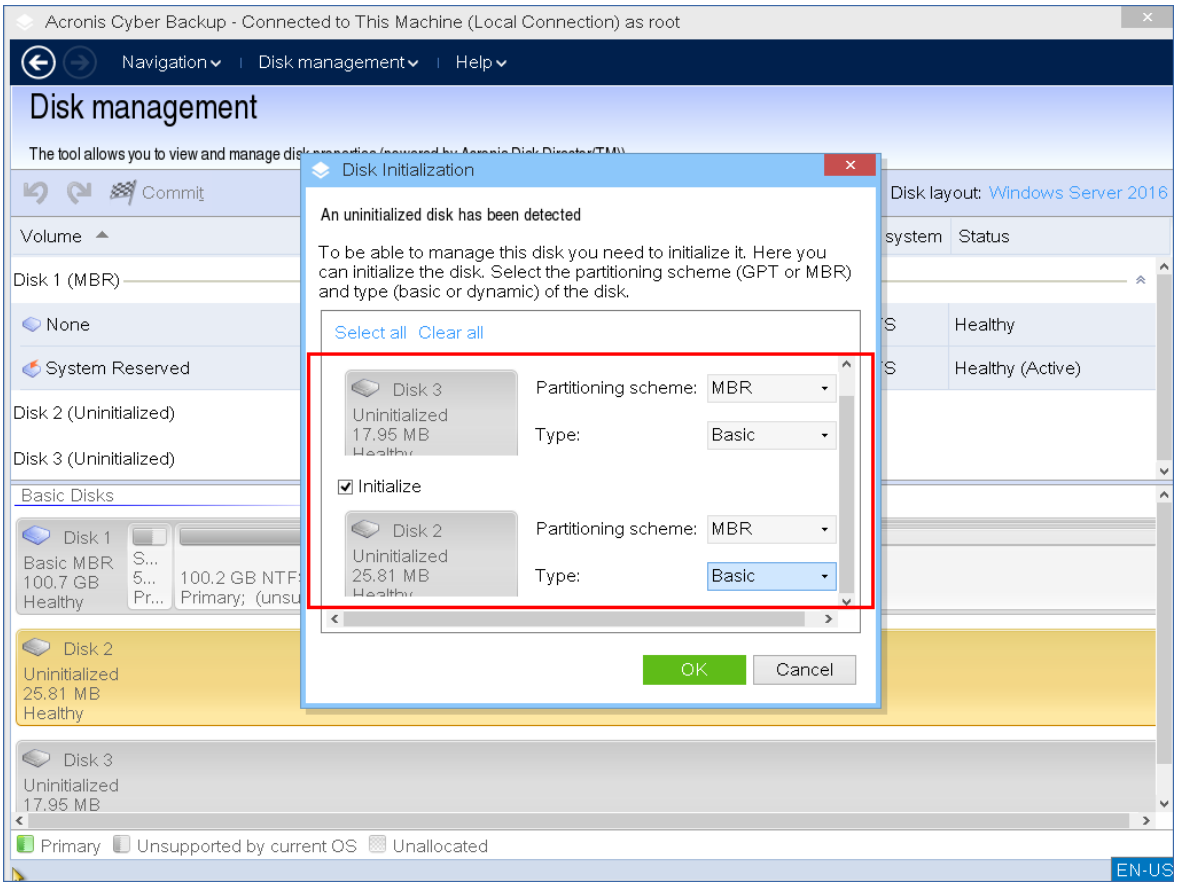
- Conversion de disque : Base à dynamique : convertit un disque de base en disque dynamique
- Conversion de disque : Dynamique à Base : convertit un disque dynamique en disque de base

Initialisation de disque

Le support de démarrage affiche les disques non initialisés sous forme de bloc gris avec une icône grise, ce qui indique qu'ils sont inutilisables par le système.

Pour initialiser un disque

1. Cliquez avec le bouton droit de la souris sur le disque souhaité, puis cliquez sur **Initialiser**.
2. Dans la fenêtre **Initialisation de disque**, définissez le schéma de partitionnement du disque (MBR ou GPT) et le type de disque (de base ou dynamique).
3. En cliquant sur **OK**, vous ajouterez une opération en attente d'initialisation du disque.
4. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.
5. Après l'initialisation, l'espace disque reste non alloué. Pour pouvoir l'utiliser, vous devez y créer un volume.



Clonage de disque basique

Vous pouvez cloner des disques MBR de base avec un support de démarrage Linux complet. Le clonage de disque n'est pas disponible dans le support de démarrage tout prêt que vous pouvez

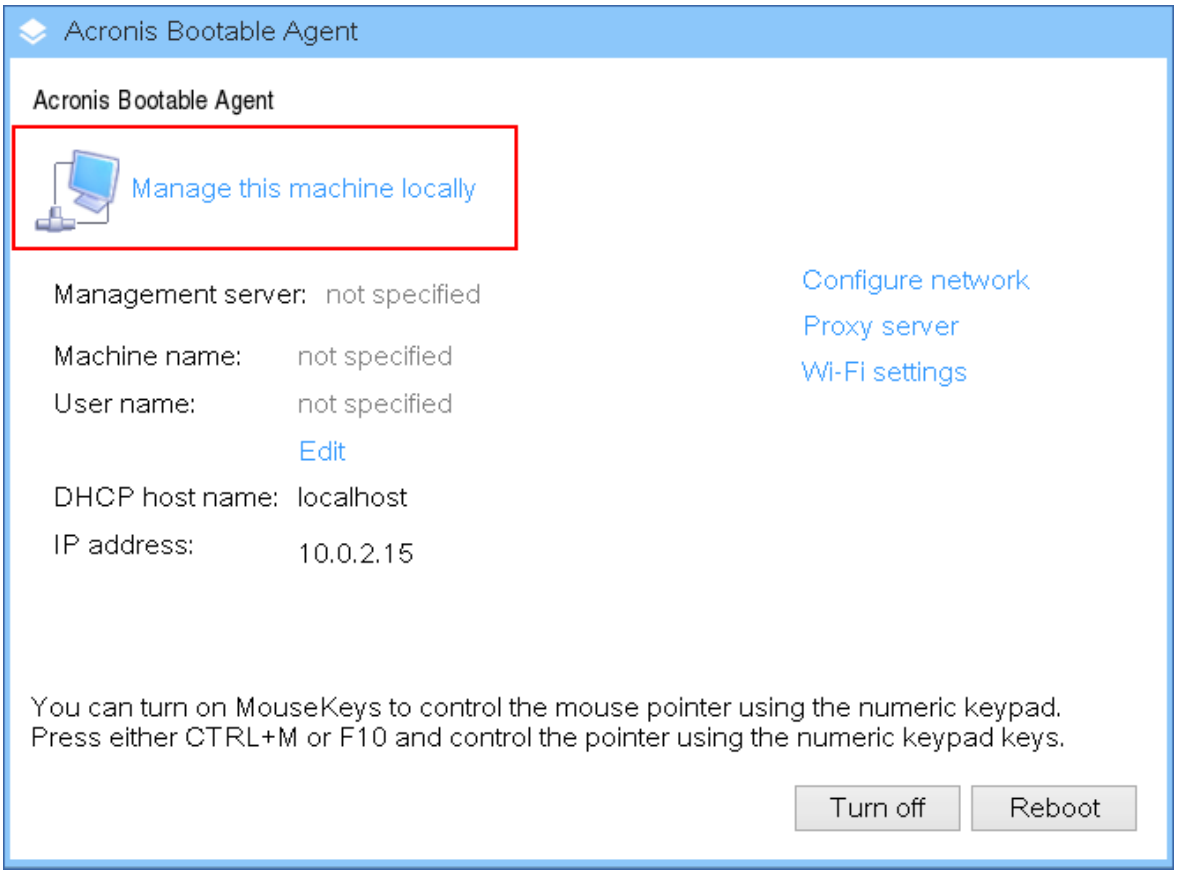
télécharger ou dans un support de démarrage créé sans clé de licence.

Remarque
Vous pouvez également cloner les disques à l'aide de l'utilitaire de ligne de commande Acronis Cyber Protect.

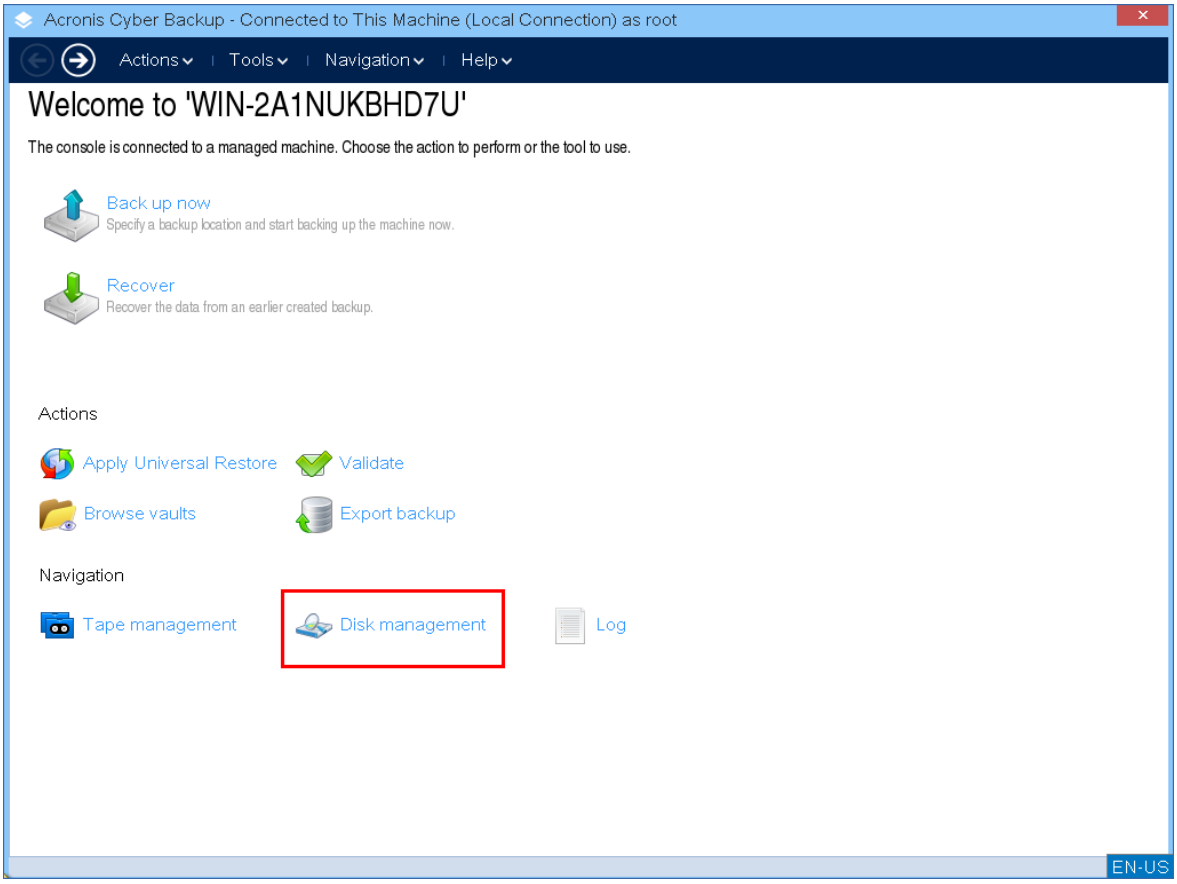
Pour cloner des disques de base dans un support de démarrage

1. Démarrez à partir du support de secours amorçable Acronis.

2. Pour cloner un disque de la machine locale, cliquez sur **Gérer cet ordinateur localement**. Pour la connexion à distance, reportez-vous à Enregistrer le support sur le serveur de gestion.

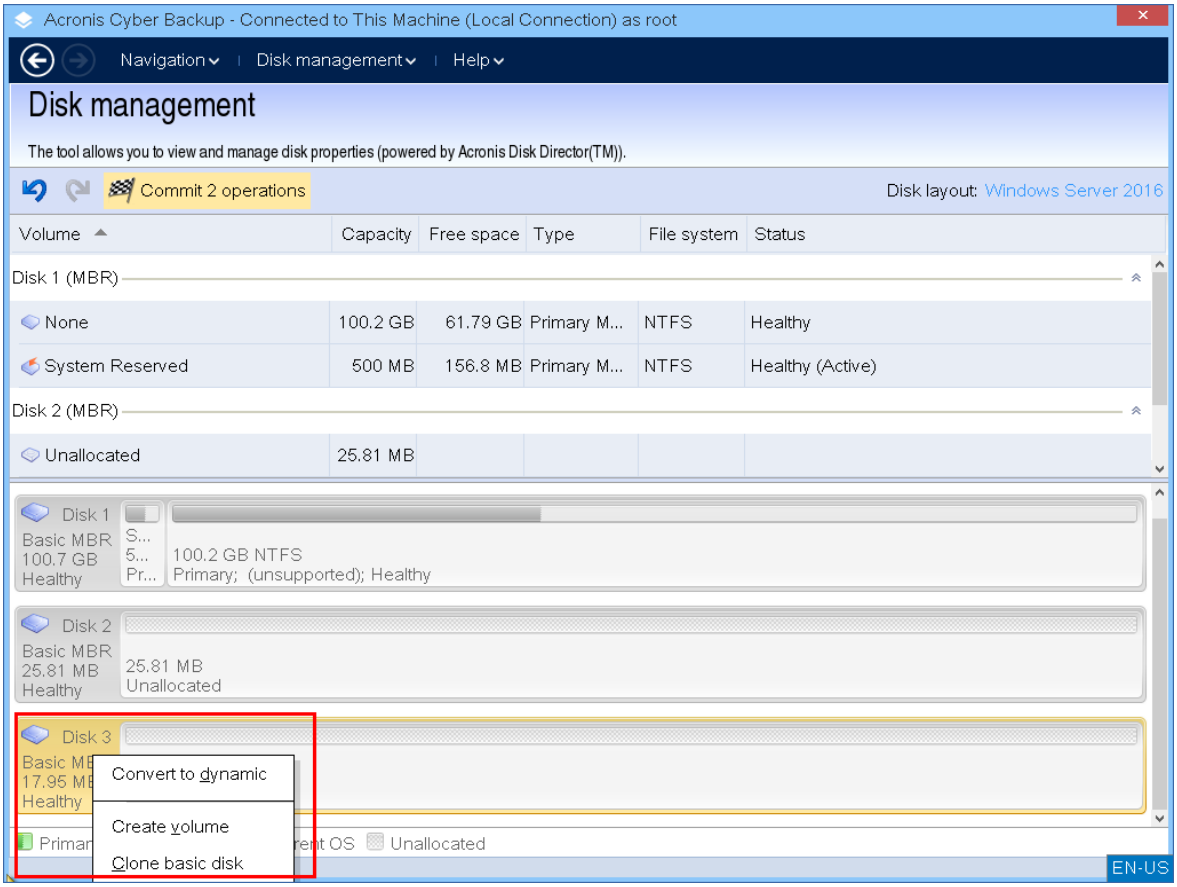


3. Cliquez sur **Gestion des disques**.

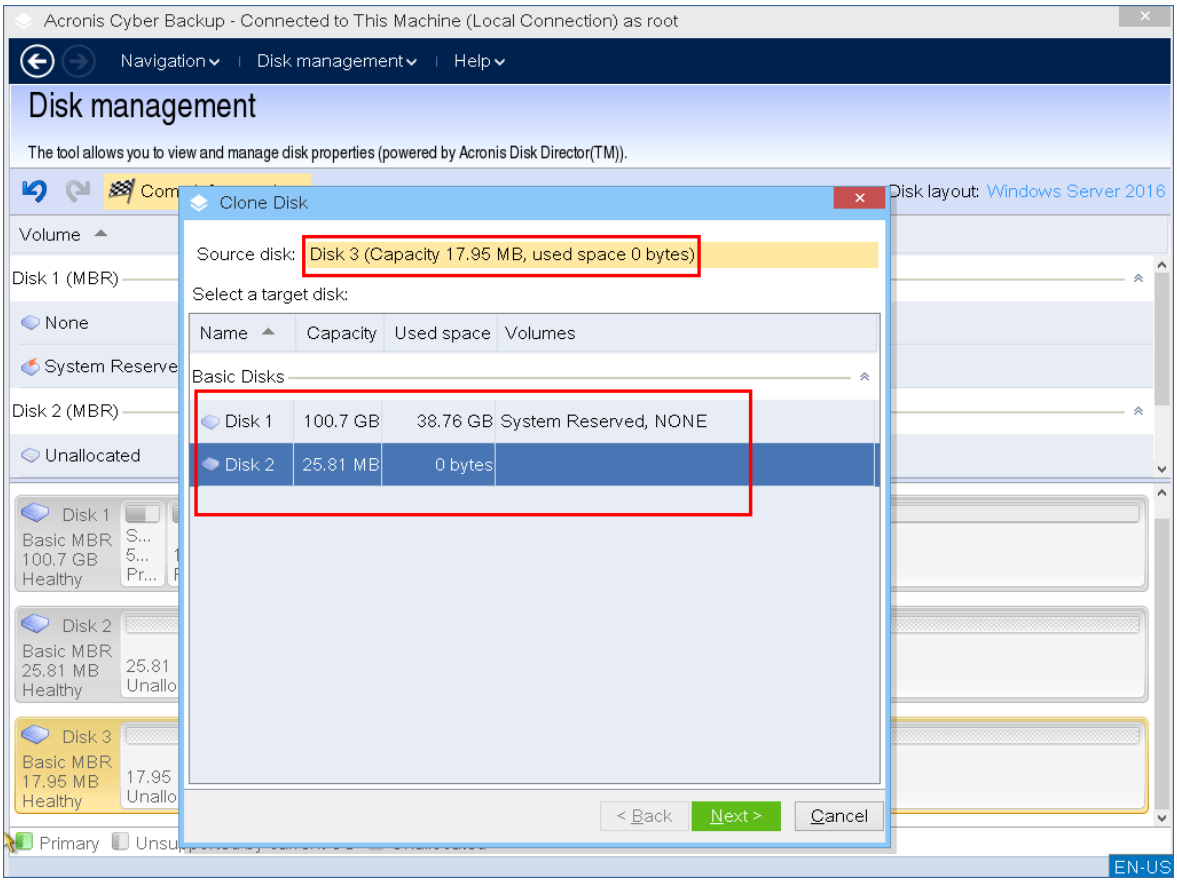


4. Les disques disponibles s'affichent. Cliquez avec le bouton droit sur le disque que vous souhaitez cloner, puis cliquez sur **Cloner un disque de base**.

Remarque
Vous ne pouvez cloner que des disques complets. Le clonage de partition n'est pas disponible.

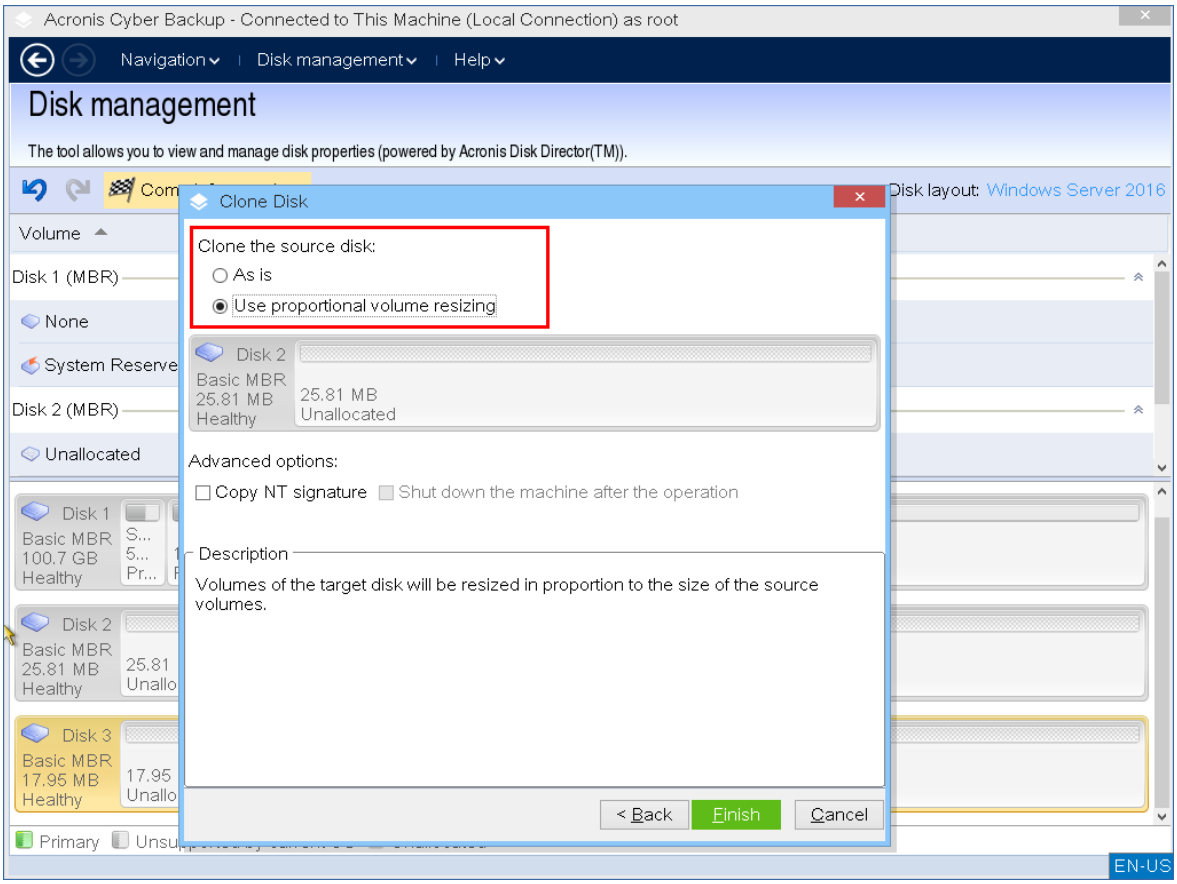


5. La liste des disques de destination possibles s'affiche. Le programme vous permet de sélectionner un disque de destination s'il est suffisant pour contenir toutes les données du disque source, sans aucune perte. Sélectionnez un disque de destination, puis cliquez sur **Suivant**.

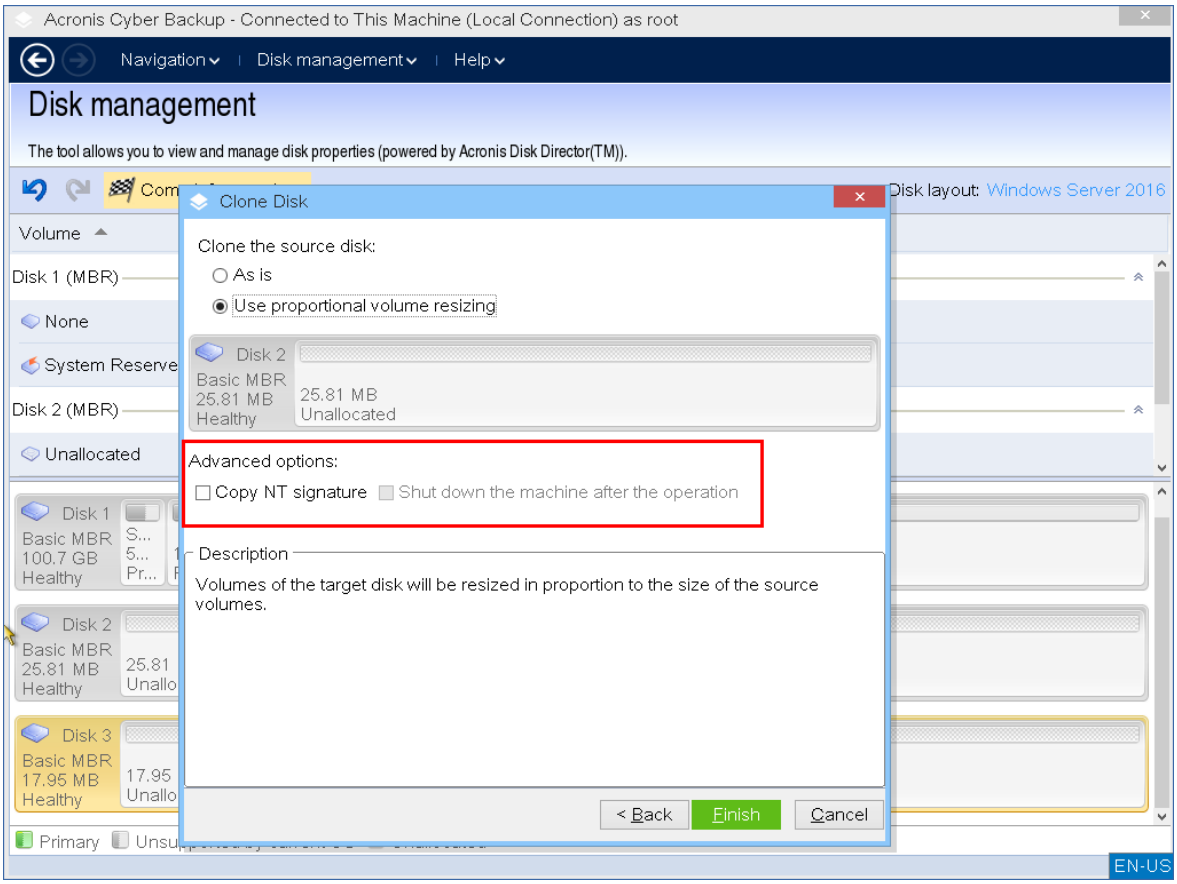


Si la capacité du disque de destination est supérieure, vous pouvez cloner le disque en l'état ou redimensionner proportionnellement les volumes du disque source pour éviter de laisser de l'espace non alloué sur le disque de disque de destination.
Si la capacité du disque de destination est inférieure, seul le redimensionnement proportionnel est disponible. Si un clonage sécurisé est impossible, même avec le redimensionnement proportionnel, vous ne pourrez pas continuer cette opération.

Important
Si le disque de destination contient des données, vous recevez cet avertissement : « *Le disque de destination sélectionné n'est pas vide. Les données sur ses volumes seront écrasées.* » Si vous continuez, toutes les données stockées sur le disque de destination seront perdues de manière irréversible.



6. Sélectionnez si vous souhaitez copier la signature NT.



Si vous clonez d'un disque comprenant un volume système, vous devez garder la capacité de démarrage du système d'exploitation sur le volume du disque de destination. Cela signifie que le système d'exploitation doit avoir les informations du volume système (la lettre du volume, par exemple) correspondant à la signature NT du disque qui est conservée sur le disque MBR. Toutefois, deux disques avec la même signature NT ne peuvent pas fonctionner correctement sous un seul système d'exploitation.

Si vous avez deux disques ayant la même signature NT et qu'ils comportent un volume système sur un ordinateur, le système d'exploitation est exécuté au démarrage à partir du premier disque, découvre ensuite la même signature sur le second, génère automatiquement une nouvelle signature NT unique et l'assigne au second disque. Par conséquent, tous les volumes du second disque perdront leurs lettres, tous les chemins d'accès seront invalides et les programmes ne trouveront plus leurs fichiers. Le système d'exploitation sur ce disque ne sera plus amorçable.

Afin de conserver la capacité de démarrage du système sur le volume du disque de disque de destination, vous pouvez :

a. **Copier la signature NT** : fournissez au disque de destination la signature NT du disque source correspondant aux clés de la base de registre qui seront également copiées sur le disque de destination.

   Pour ce faire, cochez la case **Copier la signature NT**.

   Vous recevrez l'avertissement suivant : *« S'il y a un système d'exploitation sur le disque dur, désinstallez le lecteur de disque dur source ou de destination de votre ordinateur avant de*

redémarrer l'ordinateur. Sinon, le SE démarrera à partir du premier des deux et le SE du deuxième disque ne sera plus amorçable. »

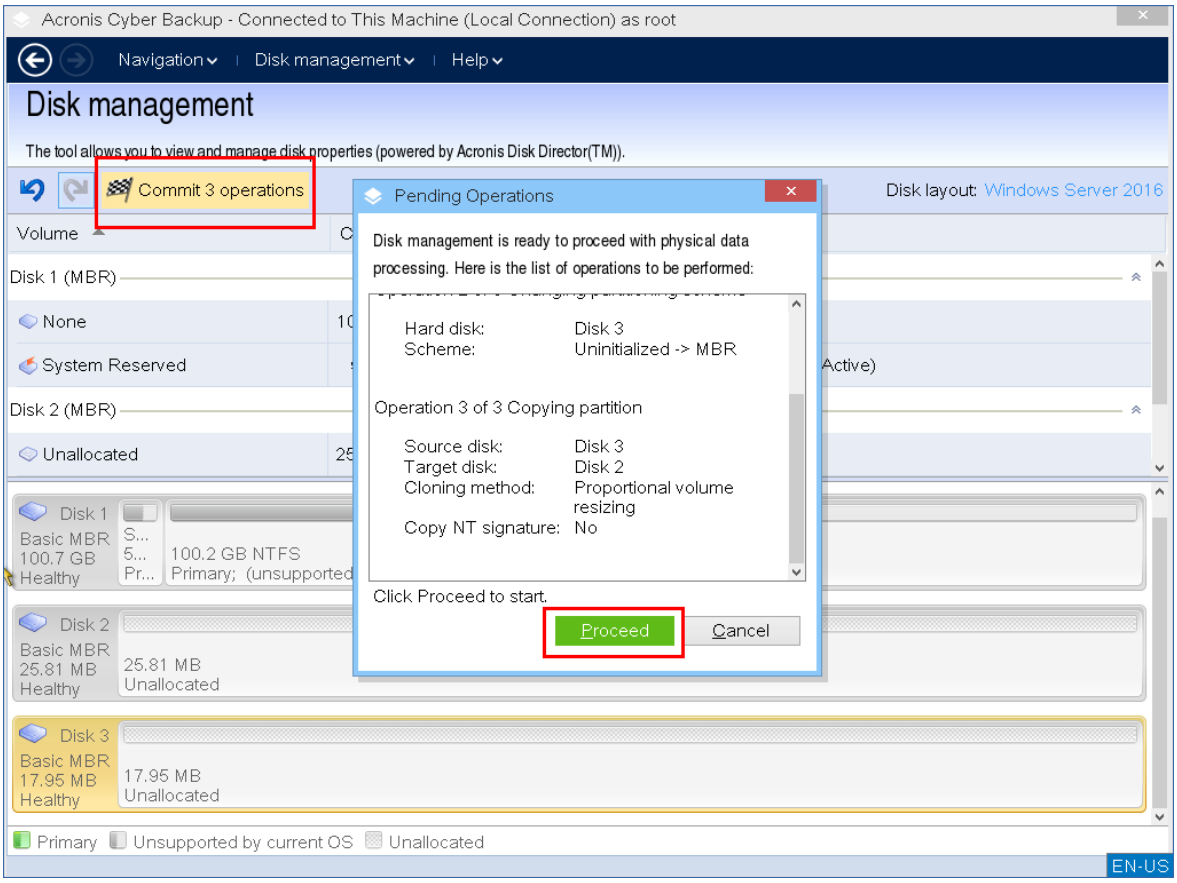
La case **Éteindre l'ordinateur après l'opération** est cochée et désactivée automatiquement.

b. **Garder la signature NT** : conservez l'ancienne signature du disque de destination et mettez à jour le système d'exploitation avec la signature.

Pour ce faire, cliquez pour désélectionner la case **Copier la signature NT**, si nécessaire.

La case **Éteindre l'ordinateur après l'opération** est désactivée automatiquement.

7. Cliquez sur **Terminer** pour ajouter une opération de clonage de disque en attente.
8. Cliquez sur **Valider**, puis sur **Continuer** dans la fenêtre **Opérations en attente**. Quitter le programme sans valider l'opération l'annulera.



9. Si vous choisissez de copier la signature NT, patientez jusqu'à la fin de l'opération et à l'arrêt de l'ordinateur, puis déconnectez le lecteur de disque dur source ou de destination de l'ordinateur.

Conversion de disque : MBR en GPT

Vous souhaiterez peut-être convertir un disque MBR de base en disque GPT de base si vous devez remplir les conditions suivantes :

- Plus de 4 volumes principaux sur un seul disque.
- Fiabilité d'un disque supplémentaire pour éviter toute possibilité d'endommagement de données.

Important
Le disque MBR de base contenant le volume de démarrage avec le système d'exploitation en cours d'exécution ne peut pas être converti en disque GPT.

Pour convertir un disque MBR de base en GPT de base

1. Cliquez avec le bouton droit sur le disque que vous souhaitez cloner, puis cliquez sur **Convertir en GPT**.
2. En cliquant sur **OK**, vous ajouterez une opération en attente de conversion du disque de MBR en GPT.
3. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Remarque
Un disque GPT partitionné un disque partitionné en GPT zone de sauvegarde à la fin de la zone partitionnée, ce qui stocke des copies de l'en-tête GPT et de la table de partitions. Si le disque est plein et que la taille des volumes ne peut pas être réduite automatiquement, l'opération de conversion de disque MBR en GPT échouera.
L'opération est irréversible. Si vous avez un volume principal appartenant à un disque MBR, que vous convertissez d'abord le disque en GPT et le reconvertissez ensuite en MBR, le volume sera logique et inutilisable comme volume système.

Conversion de disque dynamique : MBR en GPT

Le support de démarrage ne prend pas en charge la conversion directe MBR en GPT pour les disques dynamiques. Cependant, vous pouvez exécuter les conversions suivantes pour atteindre cet objectif :

1. Conversion de disque MBR : dynamique en disque de base à l'aide de l'opération **Convertir en disque de base**.
2. Conversion de disque basique : MBR en GPT à l'aide de l'opération **Convertir en GPT**.
3. Conversion de disque GPT : disque de base en dynamique à l'aide de l'opération **Convertir en dynamique**.

Conversion de disque : GPT en MBR

Si vous planifiez d'installer un SE qui ne prend pas en charge les disques GPT, il est possible de convertir le disque GPT en MBR.

Important
Le disque GPT de base qui contient le volume de démarrage avec le système d'exploitation en cours d'exécution ne peut pas être converti en secteur de démarrage principal.

Pour convertir un disque GPT en MBR

1. Cliquez avec le bouton droit sur le disque que vous souhaitez cloner, puis cliquez sur **Convertir en MBR**.
2. En cliquant sur **OK**, vous ajouterez une opération en attente de conversion de disque GBT en MBR.
3. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Remarque
Après l'opération, les volumes de ce disque deviendront logiques. Cette modification est irréversible.

Conversion de disque : disque de base en dynamique

Vous devrez peut-être convertir un disque de base en dynamique si vous :

- Prévoyez d'utiliser le disque en tant qu'élément d'un groupe de disques dynamiques
- Voulez renforcer la fiabilité du disque pour le stockage de données

Pour convertir un disque de base en disque dynamique

1. Cliquez avec le bouton droit sur le disque que vous souhaitez convertir, puis cliquez sur **Convertir en dynamique**.
2. Cliquez sur **OK**.

La conversion sera réalisée immédiatement et si nécessaire, votre ordinateur sera redémarré.

Remarque
un disque dynamique occupe le dernier mégaoctet d'un disque physique pour stocker la base de données, y compris la description en quatre niveaux (Volume-Composant-Partition-Disque) pour chaque volume dynamique. Pendant la conversion en dynamique, s'il apparaît que le disque de base est plein et que la taille de ses volumes ne peut pas être réduite automatiquement, l'opération de conversion de disque de base en dynamique échouera.
La conversion en disque dynamique du disque de base contenant des volumes système prend un certain temps, et toute coupure d'électricité, extinction non intentionnelle de l'ordinateur ou appui accidentel sur le bouton Reset pendant la procédure pourrait se traduire par l'impossibilité de redémarrer.

Contrairement au Gestionnaire de disque de Windows, le programme assure la capacité de démarrage d'un **système opérationnel hors ligne** sur le disque après l'opération.

Conversion de disque : dynamique en disque de base

Vous souhaiterez peut-être reconvertir des disques dynamiques en disques de base, par exemple, si vous voulez utiliser un système d'exploitation ne prenant pas en charge les disques dynamiques.

Pour convertir un disque dynamique en disque de base :

1. Cliquez avec le bouton droit sur le disque que vous souhaitez convertir, puis cliquez sur **Convertir en disque de base**.
2. Cliquez sur **OK**.

La conversion sera réalisée immédiatement et si nécessaire, votre ordinateur sera redémarré.

Remarque
Cette opération n'est pas disponible pour les disques dynamiques contenant des volumes fractionnés, pistés ou RAID-5.

Après la conversion, les 8 derniers Mo de l'espace disque sont réservés à la conversion ultérieure du disque de base en disque dynamique. Dans certains cas, l'espace non alloué possible et la taille maximale de volume proposée peuvent être différents (par exemple, lorsque la taille d'un des miroirs établit la taille de l'autre miroir, ou lorsque les 8 derniers Mo d'espace disque sont réservés à la conversion ultérieure du disque de base en disque dynamique).

Remarque
La conversion des disques contenant les volumes système prend un certain temps, et toute coupure d'électricité, extinction non intentionnelle de l'ordinateur ou appui accidentel sur le bouton Reset pendant la procédure pourrait se traduire par l'impossibilité de démarrer.

Par rapport au Gestionnaire de disque Windows, le programme assure :

- Conversion sûre d'un disque dynamique vers le format de base lorsqu'il contient des volumes **avec données** pour les volumes simples ou en miroir
- Dans les systèmes à amorçage multiple, la capacité de démarrage d'un système qui était **hors ligne** pendant l'opération

Opérations de volume

Grâce au support de démarrage, vous pouvez exécuter les opérations suivantes sur les volumes :

- Créer un volume : crée un nouveau volume
- Supprimer le volume : supprime le volume sélectionné
- Activer : active le volume sélectionné de façon à ce que la machine puisse démarrer avec le SE qui y est installé.
- Modifier la lettre : modifie la lettre du volume sélectionné
- Modifier le label : modifie le nom du volume sélectionné
- Formater le volume : formate un volume avec le système de fichiers

Types de volumes dynamiques

Volume simple

Un volume créé à partir d'espace libre sur un seul disque physique. Il peut se composer en une région sur le disque ou en plusieurs régions, virtuellement unies par le Gestionnaire de Disques Logiques (Logical Disk Manager - LDM). Il n'apporte ni fiabilité supplémentaire ni augmentation de vitesse ni taille supplémentaire.

Volume fractionné

Un volume créé à partir d'espaces disque libres virtuellement liés ensemble par le LDM de plusieurs disques physiques. Jusqu'à 32 disques peuvent être inclus dans un volume, surpassant ainsi les limites de taille du matériel. Toutefois, même si un seul disque échoue, toutes les données seront perdues. De la même manière, aucune partie d'un volume fractionné ne peut être retirée sans détruire l'intégralité du volume. Par conséquent, un volume fractionné ne fournit aucune fiabilité supplémentaire ni amélioration du ratio E/S.

Volume pisté

Un volume, parfois également appelé RAID 0, composé de bandes de données égales, écrites sur chaque disque du volume. Cela signifie que, pour créer un volume agrégé par bandes, vous aurez besoin de deux disques dynamiques ou plus. Les disques d'un volume agrégé par bandes ne doivent pas nécessairement être identiques, mais chaque disque doit disposer d'un espace non utilisé sur chaque disque que vous voulez inclure dans le volume. La taille du volume dépendra de la taille du plus petit espace. L'accès aux données sur un volume pisté est généralement plus rapide que l'accès aux mêmes données sur un seul disque physique car le ratio E/S est étalé sur plusieurs disques.

Les volumes agrégés par bandes sont créés pour améliorer les performances, pas pour améliorer la fiabilité : ils ne contiennent pas d'informations redondantes.

Volume miroir

Un volume tolérant aux pannes, parfois appelé RAID 1, dont les données sont dupliquées sur deux disques physiques identiques. Toutes les données sur un disque sont copiées sur un autre disque pour fournir une répétition des données. Presque tous les volumes peuvent être miroirs, y compris les volumes système et de démarrage, et si l'un des disques tombe en panne, les données peuvent être retrouvées sur le disque restant. Malheureusement, les limites du matériel en termes de taille et de performance sont encore plus rigoureuses avec l'utilisation de volumes miroirs.

Volume pisté miroir

Un volume insensible aux défaillances, parfois également appelé RAID 1+0, combinant l'avantage de la grande vitesse E/S de la structure pistée et de la répétition du type miroir.

L'inconvénient reste inhérent à l'architecture miroir : un faible ratio de taille disque à volume.

RAID-5

Un volume insensible aux défaillances dont les données sont pistées à travers une grappe de trois disques ou plus. Les disques ne doivent pas nécessairement être identiques, mais chaque disque du volume doit comprendre des blocs d'espace non alloué de même taille. La parité (valeur calculée pouvant servir à la reconstruction des données après une défaillance) est aussi pistée sur la grappe de disques et est toujours stockée sur un disque différent des données. Si un disque physique tombe en panne, la portion du volume RAID-5 qui se trouvait sur ce disque en panne peut être recréée à partir des données restantes et de la parité. Un volume RAID-5 apporte une fiabilité et est capable de surpasser les limites en termes de taille de disque avec un meilleur ratio de taille de disque-à-volume que le miroir.

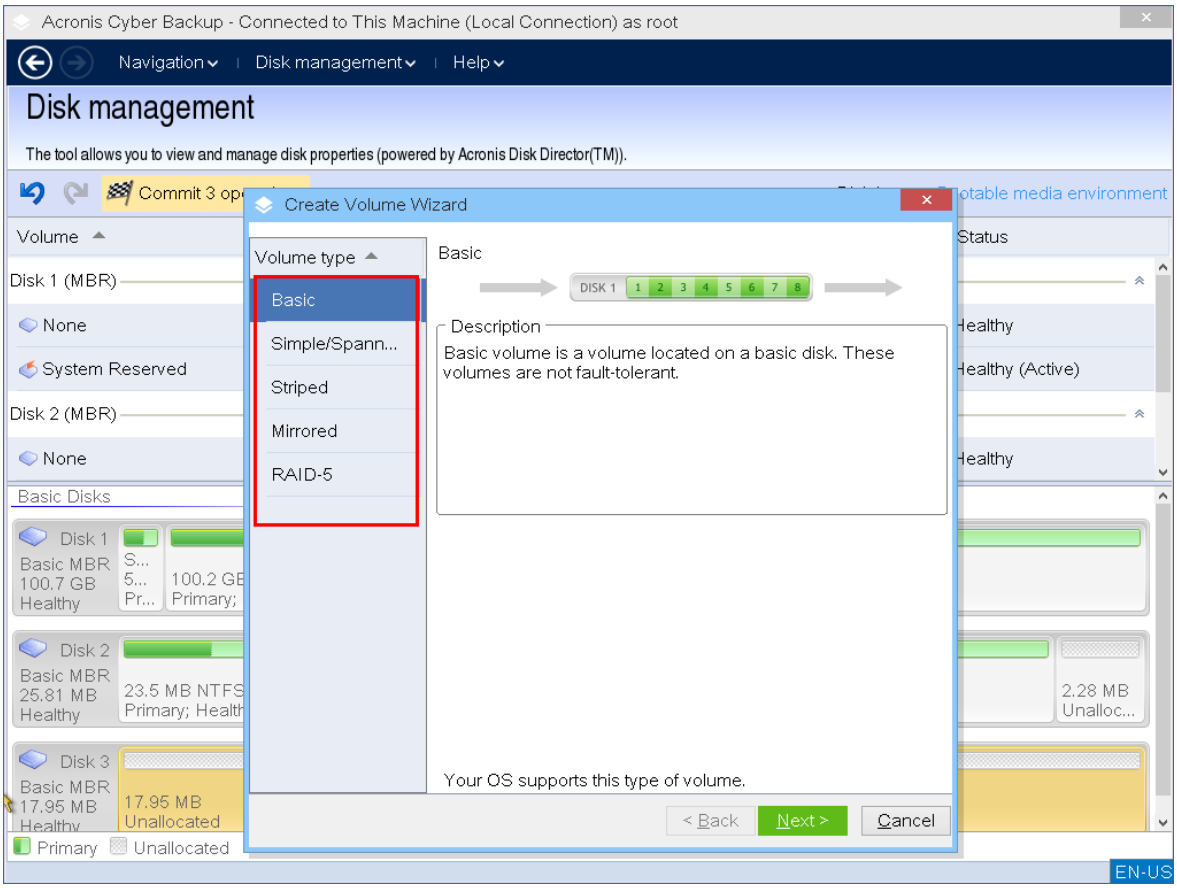
Créer un volume

Il se peut que vous ayez besoin d'un nouveau volume pour :

- Récupérer une copie de sauvegarde enregistrée précédemment dans la configuration « exactement en l'état »
- Stocker les collections de fichiers similaires séparément — par exemple, une collection MP3 ou des fichiers vidéo sur un volume séparé
- Stocker les sauvegardes (images) d'autres volumes/disques sur un volume spécial
- Installer un nouveau système d'exploitation (ou fichier d’échange) sur un nouveau volume
- Ajouter du nouveau matériel sur un ordinateur

Pour créer un volume

1. Cliquez avec le bouton droit sur l'espace non alloué d'un disque, puis cliquez sur **Créer un volume**. L'assistant **c**Créer un volume s'ouvre.



2. Sélectionnez le type de volume. Les options suivantes sont disponibles :
   - Basique
   - Simple/Fractionné
   - Pisté
   - Miroir
   - RAID-5

   Si le système d'exploitation actuel ne prend pas en charge le type de volume sélectionné, vous recevrez un avertissement et le bouton **Suivant** est désactivé. Vous devez sélectionner un autre type de volume pour continuer.
3. Spécifiez l'espace non alloué ou sélectionnez les disques de destination.
   - Pour un volume de base, spécifiez l'espace non alloué sur le disque sélectionné.
   - Pour un volume simple/fractionné, sélectionnez un ou plusieurs disques de destination.
   - Pour un volume en miroir, sélectionnez deux disques de destination.
   - Pour un volume agrégé par bandes, sélectionnez au moins deux disques de destination.
   - Pour un volume RAID-5, sélectionnez trois disques de destination.

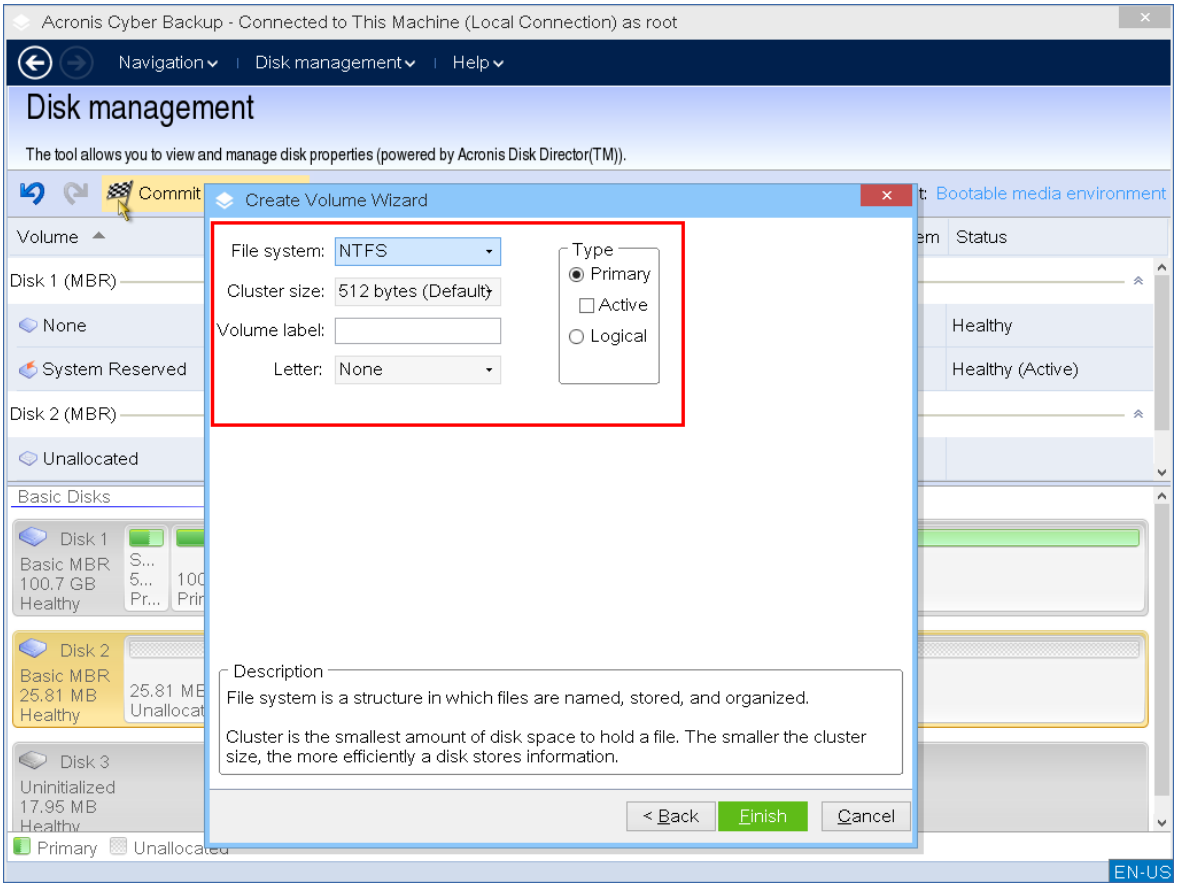
   Si vous créez un volume **dynamique** et sélectionnez un ou plusieurs disques **de base** en tant que destination, vous recevrez un avertissement vous indiquant que le disque sélectionné sera converti automatiquement en disque dynamique.

4. Définir la taille du volume.

   La valeur maximale indique généralement la taille maximale de l'espace non alloué. Dans certains cas, la valeur maximale proposée peut être différente. C'est le cas notamment lorsque la taille d'un des miroirs établit la taille de l'autre miroir ou que les 8 derniers Mo d'espace disque sont réservés à la conversion ultérieure du disque de base en disque dynamique.

   Vous pouvez choisir l'emplacement d'un nouveau volume de base sur un disque si l'espace non alloué sur ce disque est supérieur au volume.

5. Configurer les options du volume.



Vous pouvez attribuer une **lettre** au volume (par défaut, la première lettre disponible de l'alphabet) et, en option, un **label** (par défaut, aucun). Vous devez également spécifier le **Système de fichiers** et la **Taille du cluster**.

Voici les options possibles pour les systèmes de fichiers :

- FAT16 (désactivé si la taille du volume a été définie sur une valeur supérieure à 2 Go)
- FAT32 (désactivé si la taille du volume a été définie sur une valeur supérieure à 2 To)
- NTFS
- Laissez le volume non formaté.

Lorsque vous définissez la taille de cluster, vous pouvez choisir n'importe quel nombre correspondant au total prédéfini pour chaque système de fichiers. La taille de cluster suggérée par défaut est la plus adaptée au volume avec le système de fichiers choisi. Si vous définissez une taille de cluster de 64 Ko pour FAT16/FAT32 ou une taille de cluster de 8 à 64 Ko pour NTFS,

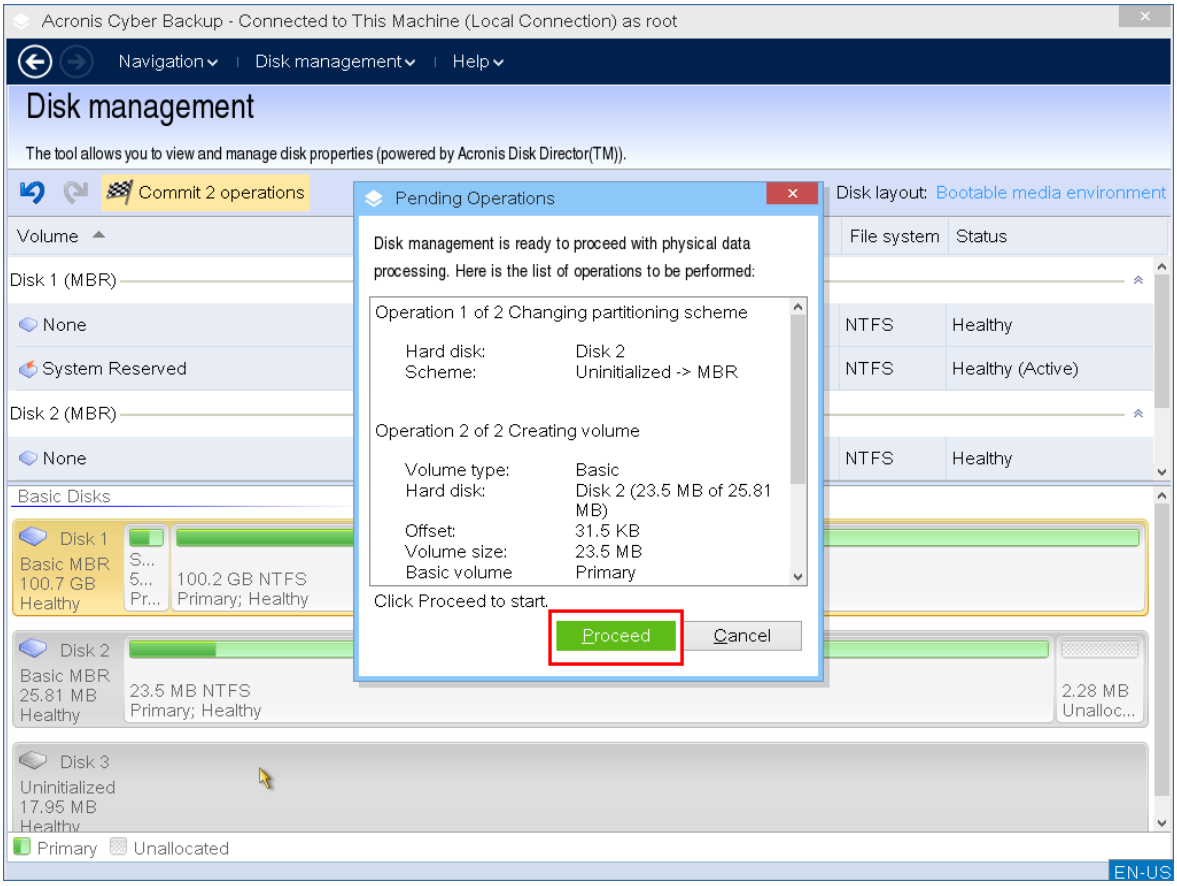
Windows peut monter le volume, mais certains programmes (par exemple, les programmes d'installation) risquent de ne pas calculer son espace disque correctement.

Si vous créez un volume de base pouvant être converti en volume système, vous pouvez également sélectionner le type de volume : **Principal** (**principal actif**) ou **Logique**. Généralement, **Primaire** est sélectionné lorsque vous souhaitez installer un système d'exploitation sur un volume. Sélectionnez la valeur **Actif** (par défaut) si vous voulez installer un système d'exploitation sur ce volume et qu'il soit lancé au démarrage de l'ordinateur. Si le bouton **Primaire** n'est pas sélectionné, l'option **Actif** sera désactivée. Si le volume est prévu pour le stockage de données, sélectionnez **Logique**.

Remarque

Un disque de base peut contenir jusqu'à quatre volumes principaux. S'il existe déjà, le disque devra être converti en dynamique. Dans le cas contraire, les options **Actif** et **Primaire** seront désactivées et vous ne pourrez sélectionner que le type de volume **Logique**.

6. Cliquez sur **Valider**, puis sur **Continuer** dans la fenêtre **Opérations en attente**. Quitter le programme sans valider l'opération l'annulera.



Supprimer un volume

Pour supprimer un volume

1. Cliquez avec le bouton droit sur le volume que vous souhaitez supprimer.
2. Cliquez sur **Supprimer le volume**.

   Remarque
   Toutes les informations stockées sur ce volume seront perdues de manière irréversible.

3. En cliquant sur **OK**, vous ajouterez une opération en attente de suppression de volume.
4. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Une fois qu'un volume est supprimé, son espace est ajouté à l'espace disque non alloué. Vous pouvez l'utiliser pour créer un nouveau volume ou pour modifier le type d'un autre volume.

Activer un volume

Si vous avez plusieurs volumes primaires, vous devez spécifier celui qui sera le volume de démarrage. Pour cela, vous pouvez activer un volume. Un disque ne peut avoir qu'un seul volume actif.

Pour activer un volume :

1. Cliquez avec le bouton droit sur le volume principal souhaité sur un disque MBR de base, puis cliquez sur **Marquer comme actif**.

   S'il n'y pas d'autre volume actif dans le système, l'opération d'activation du volume sera ajoutée à la liste d'opérations en attente. Si un autre volume actif est présent dans le système, vous êtes averti que le volume actif précédent devra tout d'abord être mis en état passif.

   Remarque
   En raison de l'activation du nouveau volume, la lettre du volume actif précédent peut être modifiée et certains des programmes installés risquent d'arrêter de fonctionner.

2. En cliquant sur **OK**, vous ajouterez une opération en attente de définition de volume actif.

   Remarque
   Même si vous avez le système d'exploitation sur le nouveau volume actif, dans certains cas, l'ordinateur ne pourra pas démarrer à partir de ce volume. Vous devrez d'abord confirmer votre décision d'activer le nouveau volume.

3. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Modifier la lettre d'un volume

Les systèmes d'exploitation Windows attribuent des lettres (C:, D:, etc.) aux volumes de disques durs au démarrage. Ces lettres sont utilisées par les applications et les systèmes d'exploitation pour localiser les fichiers et les dossiers au sein de ces volumes. Connecter un disque supplémentaire, de même que créer ou supprimer un volume sur des disques existants, peut modifier la configuration

de votre système. Par conséquent, certaines applications peuvent ne plus fonctionner normalement, ou des fichiers utilisateur peuvent ne pas être automatiquement trouvés et ouverts. Pour empêcher ceci, vous pouvez changer manuellement les lettres automatiquement attribuées aux volumes par le système d'exploitation.

Pour changer la lettre attribuée à un volume par le système d'exploitation

1. Cliquez avec le bouton droit de la souris sur le volume souhaité, puis cliquez sur **Modifier la lettre**.
2. Dans la fenêtre **Modifier la lettre**, sélectionnez une nouvelle lettre.
3. En cliquant sur **OK**, vous ajouterez une opération en attente d'attribution de lettre de volume.
4. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Modifier le label d'un volume

Le label d'un volume est un attribut optionnel. Il s'agit d'un nom attribué à un volume pour faciliter sa reconnaissance.

Pour changer le nom du volume

1. Cliquez avec le bouton droit de la souris sur le volume souhaité, puis cliquez sur **Modifier le label**.
2. Entrer une nouvelle étiquette dans le champ de texte de la fenêtre **Modifier étiquette** .
3. En cliquant sur **OK**, vous ajouterez une opération en attente de modification du nom de volume.
4. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Formater le volume

Il se peut que vous vouliez formater un volume si vous voulez modifier son système de fichiers :

- Pour économiser de l'espace supplémentaire qui se perd en raison de la taille du cluster sur les systèmes de fichiers FAT16 ou FAT32
- En tant que manière rapide et plus ou moins fiable de détruire des données restantes dans ce volume

Pour formater un volume :

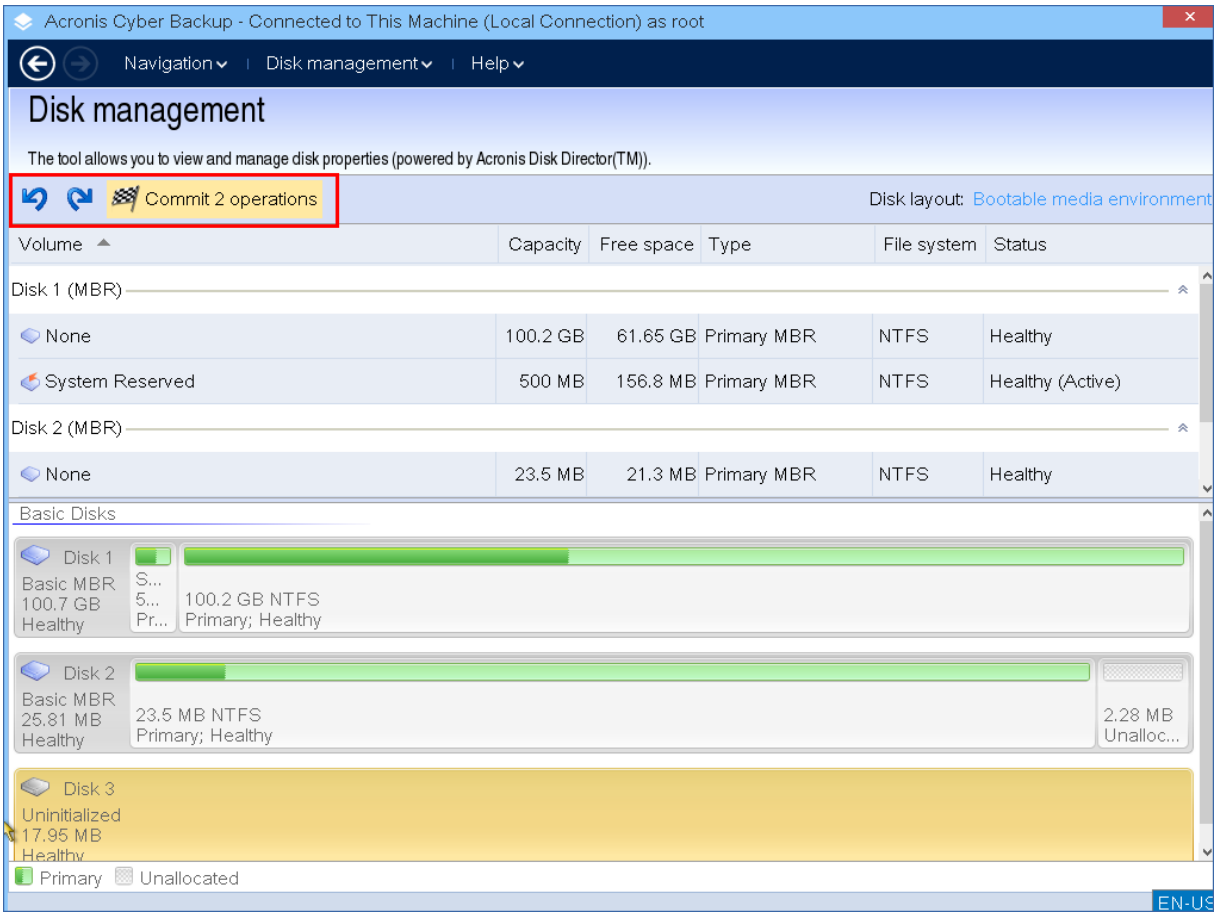
1. Cliquez avec le bouton droit de la souris sur le volume souhaité, puis cliquez sur **Formater**.
2. Sélectionnez la taille du cluster et le système de fichiers. Voici les options possibles pour les systèmes de fichiers :
   - FAT16 (désactivé si la taille du volume a été définie sur une valeur supérieure à 2 Go)
   - FAT32 (désactivé si la taille du volume a été définie sur une valeur supérieure à 2 To)
   - NTFS
3. En cliquant sur **OK**, vous ajouterez une opération en attente de formatage de volume.

4. Pour terminer l'opération ajoutée, validez-la. Quitter le programme sans valider l'opération l'annulera.

Opérations en attente

Toutes les opérations sont considérées comme étant en attente jusqu'à ce que vous émettiez et confirmiez la commande **Valider**. Vous pouvez donc contrôler toutes les opérations planifiées, vérifier les modifications prévues et annuler les opérations avant qu'elles ne soient exécutées si nécessaire.

La vue **Gestion des disques** contient la barre d'outils avec les icônes pour exécuter les actions **Annuler**, **Rétablir** et **Valider** prévues pour les opérations en attente. Ces actions peuvent également être exécutées à partir du menu **Gestion des disques**.



Toutes les opérations planifiées sont ajoutées à la liste des opérations en attente.

L'action **Annuler** vous permet d'annuler la dernière opération de la liste. Quand la liste n'est pas vide, cette action est disponible.

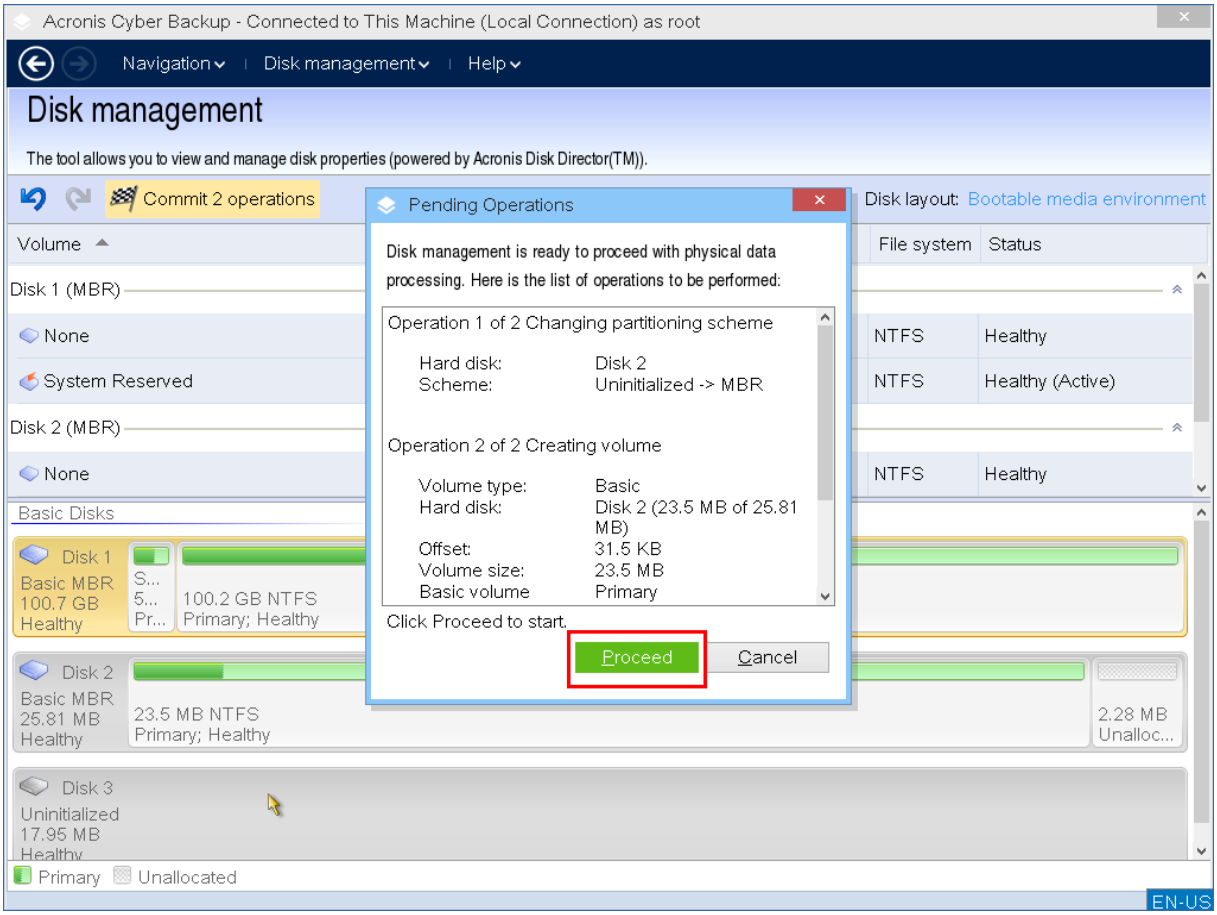
L'action **Rétablir** vous permet de rétablir la dernière opération en attente qui a été annulée.

L'action **Valider** vous transfère vers la fenêtre **Opérations en attente**, sur laquelle s'affichera la liste des opérations en attente.

Pour lancer leur exécution, cliquez sur **Continuer**.

Remarque
Vous ne serez plus en mesure d'annuler aucune action ou opération après avoir choisi l'opération **Poursuivre**.

Si vous ne souhaitez pas poursuivre la validation, cliquez sur **Annuler**. Plus aucune modification ne sera alors effectuée sur la liste des opérations en attente. Le fait de quitter le programme sans valider les opérations en attente les annule également.



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 "Enregistrer le support sur le serveur de gestion" (p. 397).

Une fois le support enregistré dans la console Cyber Protect, il apparaît dans **Périphériques** > **Support de démarrage**.

Vous pouvez gérer le support à distance à l'aide de l'interface Web. 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.

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 **Périphériques** > **Support de démarrage**.
1. 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 reprise, puis cliquez sur **Restaurer des fichiers/dossiers**.
5. Accédez au dossier requis ou servez-vous de la barre de recherche pour obtenir la liste des fichiers et dossiers requis.

   Vous pouvez utiliser un ou plusieurs caractères génériques (* et ?). Pour plus de détails sur l'utilisation de caractères génériques, voir "Filtres de fichiers" (p. 283).
6. Cliquez sur les fichiers que vous souhaitez restaurer, puis sur **Restaurer**.
7. Dans **Chemin d'accès**, sélectionnez la destination de la restauration.
8. [Facultatif] Pour définir la configuration avancée de la reprise, cliquez sur **Options de restauration**. Pour obtenir plus d'informations, consultez l'article "Options de restauration" (p. 341).
9. Cliquez sur **Démarrer la restauration**.
10. 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**

    Choisissez si vous souhaitez redémarrer automatiquement la machine.
11. Cliquez sur **Poursuivre** pour lancer la reprise. La progression de la restauration sont affichées 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 **Périphériques**, 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 reprise, puis cliquez sur **Restaurer** > **Toute la machine**.

   Si nécessaire, configurez la machine cible et le mappage de volume en suivant les indications de "Restauration d'une machine physique" (p. 321).
5. Pour définir la configuration avancée de la reprise, cliquez sur **Options de restauration**. Pour obtenir plus d'informations, consultez l'article "Options de restauration" (p. 341).
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.

8. La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour redémarrer à distance l'ordinateur démarré

1. Dans l'onglet **Périphériques**, 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 **Périphériques**, accédez au groupe **Support de démarrage**, puis sélectionnez le support que vous souhaitez utiliser pour la restauration de données.
2. Cliquez sur **Arrêter**.
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 **Périphériques**, 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 **Périphériques**, 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.

Configuration des terminaux iSCSI

Cette section explique comment configurer les terminaux Internet Small Computer System Interface (iSCSI) lorsque vous utilisez un support de démarrage. Après la réalisation des étapes suivantes, vous pourrez utiliser ces périphériques comme s'ils étaient connectés localement à la machine démarrant avec le support de démarrage.

Un **serveur cible iSCSI** (ou **portail cible**) est un serveur hébergeant le périphérique iSCSI. Une **cible iSCSI** est un composant situé sur le serveur cible. Ce composant partage les initiateurs iSCSI des listes et du périphérique qui sont autorisés à accéder au périphérique. Un **initiateur iSCSI** est un composant installé sur une machine. Ce composant fournit une interaction entre la machine et une cible iSCSI. Lorsque vous configurez l'accès à un périphérique iSCSI sur une machine démarrant avec un support de démarrage, vous devez indiquer le portail cible iSCSI du périphérique et l'un des initiateurs iSCSI mentionnés dans la cible. Si la cible est partagé sur plusieurs périphériques, vous aurez accès à tous les périphériques.

Pour ajouter un périphérique iSCSI dans un support de démarrage basé sur Linux

1. Cliquez sur **Outils** > **Configurer les périphériques iSCSI/NDAS**.
2. Cliquez sur **Ajouter un hôte**.
3. Précisez l'adresse IP et le port du portail cible iSCSI, ainsi que le nom de l'initiateur iSCSI qui est autorisé à accéder au périphérique.
4. Si l'hôte nécessite une authentification, spécifiez un nom d'utilisateur et un mot de passe.
5. Cliquez sur **OK**.
6. Sélectionnez la cible iSCSI dans la liste et cliquez ensuite sur **Connexion**.
7. Si l'authentification CHAP est activée dans les paramètres de la cible iSCSI, vous serez invité à spécifier les informations d'identification pour accéder à la cible iSCSI. Spécifiez le même nom d'utilisateur et mot de passe cible que dans les paramètres de la cible iSCSI. Cliquez sur **OK**.
8. Cliquez sur **Fermer** pour fermer la fenêtre.

Pour ajouter un périphérique iSCSI dans un support de démarrage PE

1. Cliquez sur **Outils** > **Exécuter l'installation iSCSI**.
2. Cliquez sur l'onglet **Découverte**.
3. Dans **Portails cibles**, cliquez sur **Ajouter**, puis précisez l'adresse IP et le port du portail cible iSCSI. Cliquez sur **OK**.
4. Cliquez sur l'onglet **Général**, puis sur **Modifier**, et indiquez le nom d'un initiateur iSCSI qui est autorisé à accéder au périphérique.
5. Cliquez sur l'onglet **Cibles**, puis sur **Actualiser**, sélectionnez la cible iSCSI dans la liste et cliquez ensuite sur **Connexion**. Cliquez sur **OK** pour vous connecter à la cible iSCSI.
6. Si l'authentification CHAP est activée dans les paramètres de la cible iSCSI, vous verrez l'erreur **Échec de l'authentification**. Dans ce cas, cliquez sur **Connexion**, cliquez sur **Avancés**, sélectionnez **Activer la connexion CHAP**, puis spécifiez le même nom d'utilisateur et mot de passe cible que dans les paramètres de la cible iSCSI. Cliquez sur **OK** pour fermer la fenêtre, puis cliquez sur **OK** pour vous connecter à la cible iSCSI.
7. Cliquez sur **OK** pour fermer la fenêtre.

Startup Recovery Manager

Startup Recovery Manager est un composant de démarrage qui se trouve sur votre disque dur. Avec Startup Recovery Manager, vous pouvez démarrer l'utilitaire de démarrage de secours sans utiliser de support de démarrage séparé.

Startup Recovery Manager est particulièrement utile pour les utilisateurs en déplacement. En cas de défaillance, redémarrez l'ordinateur, attendez que l'invitation **Appuyez sur F11 pour Acronis Startup Recovery Manager...** apparaisse, puis appuyez sur F11. Le programme démarre et vous pouvez effectuer une restauration. Sur les ordinateurs sur lesquels le chargeur de démarrage GRUB est installé, sélectionnez Startup Recovery Manager à partir du menu de démarrage au lieu d'appuyer sur F11.

Vous pouvez également effectuer une sauvegarde à l'aide de Startup Recovery Manager, alors que vous êtes en déplacement.

Pour utiliser Startup Recovery Manager, vous devez l'activer. Ensuite, vous activez l'invite de démarrage **Appuyez sur F11 pour Acronis Startup Recovery Manager** (ou ajoutez l'élément « **Gestionnaire de restauration de démarrage** au menu GRUB si vous utilisez le chargeur de démarrage GRUB).

Remarque
Pour activer le Startup Recovery Manager sur un ordinateur avec volume système non chiffré, cet ordinateur doit disposer d'au moins 100 Mo d'espace libre. Les opérations de récupération nécessitant le redémarrage de la machine ont besoin de 100 Mo supplémentaires.

Vous pouvez activer Startup Recovery Manager sur un ordinateur disposant d'un volume chiffré par BitLocker si cet ordinateur comprend au moins un autre volume non chiffré. Le volume non chiffré doit avoir au moins 500 Mo d'espace libre. Pour les opérations de récupération nécessitant le redémarrage de l'appareil, l'ordinateur doit disposer de 500 Mo d'espace libre supplémentaires.

Important
S'il est impossible d'activer Startup Recovery Manager, les opérations de sauvegarde qui créent les sauvegardes de reprise en un clic échouent.

À moins d'utiliser le chargeur de démarrage GRUB et qu'il soit installé dans le secteur de démarrage principal (MBR), l'activation de Startup Recovery Manager écrase le MBR avec son propre code de démarrage. Ainsi, il se peut que vous deviez réactiver des chargeurs de démarrage tiers si de tels chargeurs de démarrage sont installés.

Sous Linux, lorsque vous utilisez un chargeur de démarrage autre que GRUB (tel que LILO, par exemple), envisagez de l'installer sur la zone d'amorce d'une partition racine (ou d'amorçage) Linux plutôt que sur le secteur de démarrage principal (MBR) avant d'activer Startup Recovery Manager. Sinon, reconfigurez manuellement le chargeur de démarrage après l'activation.

Activation de Startup Recovery Manager

Sur un ordinateur exécutant un agent pour Windows ou un agent pour Linux, vous pouvez activer Startup Recovery Manager dans la console Web Cyber Protect.

Activer Startup Recovery Manager dans la console Web Cyber Protect

1. Sélectionnez la machine sur laquelle vous voulez activer Startup Recovery Manager.
2. Cliquez sur **Détails**.
3. Activez le commutateur **Startup Recovery Manager** .
4. Patientez pendant que le logiciel active Startup Recovery Manager.

Pour activer Startup Recovery Manager sur une machine sans agent

1. Démarrez la machine à partir du support de démarrage.
2. Cliquez sur **Outils** > **Activer Startup Recovery Manager** .
3. Patientez pendant que le logiciel active Startup Recovery Manager.

Désactivation de Startup Recovery Manager

Pour désactiver Startup Recovery Manager, répétez la procédure d'activation, puis sélectionnez les actions opposées respectives. La désactivation désactive l'invite de démarrage **Appuyer sur F11 pour Acronis Startup Recovery Manager** (ou l'élément de menu dans GRUB).

Si Startup Recovery Manager n'est pas activé, vous aurez besoin d'effectuer une des suggestions suivantes pour restaurer le système quand le démarrage échoue :

- démarrer la machine à partir d'un support de démarrage séparé
- utiliser le démarrage réseau à partir du serveur PXE ou de Microsoft Remote Installation Services (RIS)

Serveur PXE Acronis

Le serveur PXE Acronis permet de démarrer des ordinateurs sur des composants de démarrage Acronis grâce au réseau.

Démarrage réseau :

- Élimine la nécessité d'avoir un technicien sur place pour installer le support de démarrage dans le système devant être démarré.
- Pendant les opérations de groupes, il réduit le temps requis pour démarrer plusieurs machines, comparativement à l'utilisation d'un support de démarrage physique.

Les composants de démarrage sont transférés vers le serveur PXE Acronis à l'aide de l'outil Acronis Bootable Media Builder. Pour transférer les composants de démarrage, lancez le support de démarrage et suivez les instructions pas-à-pas décrites dans la section « Support de démarrage basé sur un environnement Linux ».

Le démarrage de plusieurs ordinateurs à partir du serveur PXE Acronis est utile si un serveur DHCP existe sur votre réseau. Ensuite, les interfaces réseau des machines démarrées obtiendront automatiquement des adresses IP.

Limites :

Le serveur PXE Acronis ne prend pas en charge le chargeur de démarrage UEFI.

Installation du serveur Acronis PXE

Installer le serveur PXE Acronis

1. Connectez-vous comme administrateur et lancez le programme d'installation d'Acronis Cyber Protect.

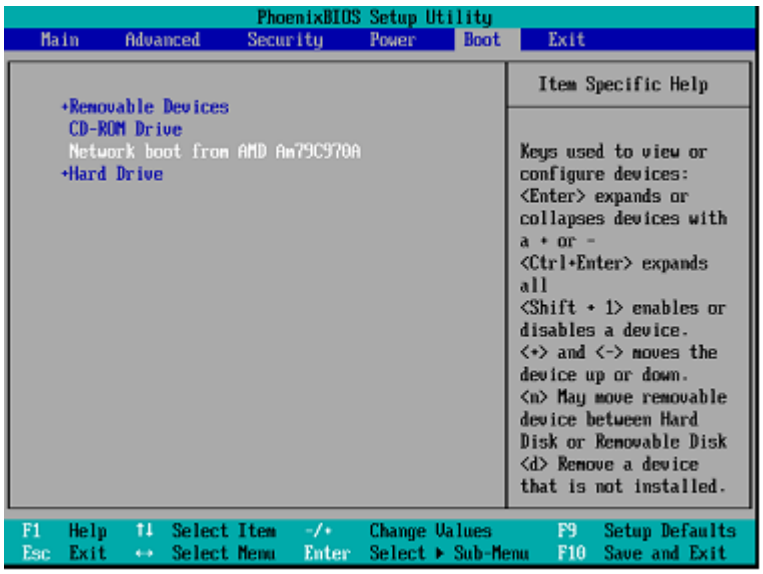
2. [Facultatif] Pour changer la langue du programme d'installation, cliquez sur **Configurer la langue**.
3. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
4. Cliquez sur **Personnaliser les paramètres d'installation**.
5. En regard de **Éléments à installer**, cliquez sur **Modifier**.
6. Cochez la case **serveur PXE**. Si vous ne souhaitez pas installer d'autre composants sur cette machine, décochez les cases correspondantes. Cliquez sur **Terminé** pour continuer.
7. [Facultatif] Modifiez d'autres paramètres d'installation.
8. Cliquez sur **Installer** pour procéder à l'installation.
9. Une fois l'installation terminée, cliquez sur **Fermer**.

Le serveur PXE Acronis est immédiatement opérationnel après installation. Après cela, il se lancera automatiquement à chaque redémarrage du système. Vous pouvez arrêter et démarrer le serveur Acronis PXE de la même manière que d'autres services Windows.

Configuration d'une machine pour démarrer à partir de PXE

Sur un matériel sans SE (« bare metal »), il suffit que le BIOS de la machine prenne en charge le démarrage sur réseau.

Sur une machine dont le disque dur contient un système d'exploitation, le BIOS doit être configuré de façon à ce que la carte d'interface réseau constitue le premier périphérique de démarrage, ou au moins qu'elle précède le périphérique de disque dur. L'exemple ci-dessous représente l'une des configurations BIOS possibles. Si vous n'insérez pas de support amorçable, la machine démarrera à partir du réseau.



Dans certaines versions BIOS, vous devez enregistrer les modifications dans le BIOS après avoir activé la carte d'interface réseau afin que cette dernière apparaisse dans la liste des périphériques de démarrage.

Si le matériel possède plusieurs cartes d'interface réseau, vérifiez que le câble réseau est bien branché sur la carte prise en charge par le BIOS.

Travailler à travers les sous-réseaux

Pour permettre au serveur PXE Acronis de travailler dans un autre sous-réseau (à travers le commutateur), configurez le commutateur pour relayer le trafic PXE. Les adresses IP du serveur PXE sont configurées sur une base par interface en utilisant la fonctionnalité d'assistance IP de la même façon que les adresses du serveur DHCP. Pour plus d'informations, reportez-vous à https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server (en anglais).

Protection des terminaux mobiles

L'application de sauvegarde 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 de sauvegarde sur un appareil mobile fonctionnant sous n'importe lequel des systèmes d'exploitation suivants :

- iOS 10.3 ou version ultérieure (iPhone, iPod et iPad)
- Android 5.0 ou version ultérieure

Ce que vous pouvez sauvegarder

- Contacts
- Photos
- 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 en continu** est activée par défaut. Si ce paramètre est activé :
  - Pour Android 7.0 ou version ultérieure, l'application de sauvegarde détecte automatiquement les nouvelles données à la volée et les charge sur le Cloud.
  - Pour Android 5 et 6, elle recherche les modifications toutes les trois heures. Vous pouvez désactiver la sauvegarde en continu dans les paramètres de l'application.
- L'option **Utiliser le Wi-Fi uniquement** est activée par défaut dans les paramètres de l'application. Si ce paramètre est activé, l'application sauvegarde vos données uniquement si une connexion Wi-Fi est disponible. Si la connexion est perdue, le processus de sauvegarde ne se lance pas. Si vous souhaitez que l'application utilise également les données cellulaires, désactivez cette option.
- Vous pouvez économiser de l'énergie de deux façons :
  - La fonctionnalité **Sauvegarder pendant la charge**, qui est désactivée par défaut. Si ce paramètre est activé, l'application sauvegarde vos données uniquement lorsque votre appareil

est connecté à une source d'alimentation. Si l'appareil n'est pas connecté à une source d'alimentation lors du processus de sauvegarde continu, la sauvegarde est mise en pause.
    - L'option **Mode d'économie d'énergie**, qui est activée par défaut. Si ce paramètre est activé, l'application sauvegarde vos données uniquement lorsque la batterie de votre appareil est suffisamment chargée. Lorsque le niveau de charge de la batterie baisse, la sauvegarde continue est mise en pause. Cette option est disponible sur Android 8 ou version ultérieure.
- 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 appareil Android peuvent être récupérés sur un appareil 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 Web 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 de sauvegarde, vous pouvez restaurer uniquement la version des données la plus récente. Si vous souhaitez effectuer une restauration à partir d'une version de sauvegarde en particulier, utilisez la console Web Cyber Protect sur une tablette ou sur un ordinateur.
- [Pour les appareils 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 obtenir l'application de sauvegarde

1. Sur le terminal mobile, ouvrez un navigateur et accédez à https://backup.acronis.com/.
2. Connectez-vous à votre compte.
3. Cliquez sur **Tous les périphériques** > **Ajouter**.
4. Sous **Terminaux mobiles**, sélectionnez le type de terminal.
   En fonction du type d'appareil, vous serez redirigé vers l'App Store ou le Play Store de Google.
5. [Sur appareils iOS uniquement] Cliquez sur **Obtenir**.
6. Cliquez sur **Installer** pour installer l'application de sauvegarde.

Comment commencer à sauvegarde vos données

1. Ouvrez l'application.
2. Connectez-vous à votre compte.

Appuyez sur **Configurer** pour créer votre première sauvegarde.

1. Sélectionnez les catégories de données que vous voulez sauvegarder. Par défaut, toutes les catégories sont sélectionnées.

2. [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**.
3. Sélectionnez **Sauvegarder**.
4. 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 appareil mobile

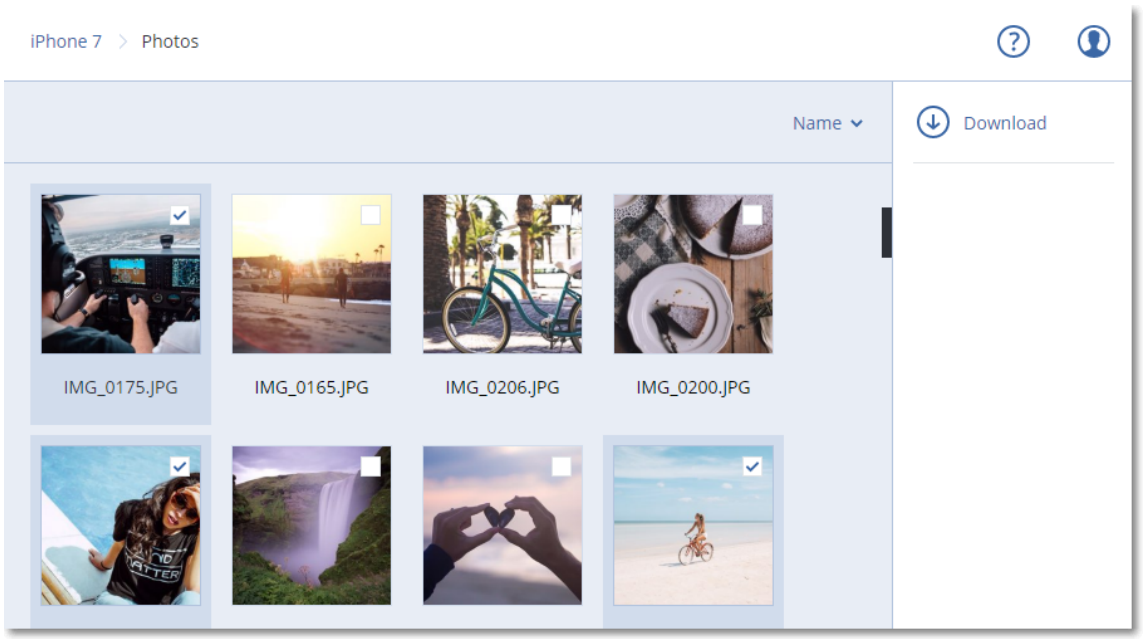
1. Ouvrez l'application de sauvegarde.
2. Appuyez sur **Parcourir**.
3. Entrez le nom du terminal.
4. Effectuez l'une des actions suivantes :
   - Pour restaurer toutes les données sauvegardées, appuyez sur **Tout restaurer**. Aucune autre action n'est requise.
   - Pour restaurer une ou plusieurs catégories 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 Web Cyber Protect

1. Sur un ordinateur, ouvrez un navigateur et saisissez l'URL de la console Web Cyber Protect.
2. Connectez-vous à votre compte.
3. Dans **Tous les périphériques**, cliquez sur **Restaurer** sous le nom de votre appareil 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 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 d'applications Microsoft

Important
Certaines des fonctionnalités décrites dans cette section sont disponibles uniquement pour les déploiements sur site.

Protection du serveur Microsoft SQL Server et Microsoft Exchange Server

Il existe deux méthodes de protection pour ces applications :

- **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 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 Bases de données en tant que fichiers	Toute la machine Bases de données sur une instance SQL Server distante active Bases de données en tant que fichiers	Toute la machine
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.

Prérequis

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 :

- 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 https://kb.acronis.com/content/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, 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 **Toute la machine** est sélectionnée pour la sauvegarde. L'option de sauvegarde **secteur par secteur** sera désactivée dans un plan de protection. Dans le cas contraire, il sera impossible d'exécuter une 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 :

- La machine virtuelle sauvegardée répond aux exigences de sauvegarde et de restauration cohérentes avec l'application qui sont répertoriées dans l'article Windows Backup Implementations de la documentation VMware : https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.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 informations d'identification d'un administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

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 2008/2008R2/2012.
- 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 informations d'identification d'un administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.
- 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.
- 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 **Périphériques** > **Microsoft SQL**.
   Le logiciel affiche l'arborescence des groupes de disponibilité AlwaysOn 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 AlwaysOn (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.
- 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 **Périphériques** > **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 aux lettres », les boîtes aux lettres s'affichent également dans cette arborescence.
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.
   - 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, consultez la section « Protection des groupes de disponibilité de la base de données (DAG) ».
   - 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 aux lettres », vous pouvez sélectionner les boîtes aux lettres pour la sauvegarde.
4. Le cas échéant, spécifiez les identifiants donnant accès aux données.
5. Cliquez sur **Protection**.

Protection des groupes de disponibilité AlwaysOn (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.

Configurations de cluster prises en charge

Le logiciel de sauvegarde prend *uniquement* en charge les groupes de disponibilité AlwaysOn (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.

   Remarque
   Après avoir installé l'agent sur l'un des nœuds, le logiciel affiche l'AAG et ses nœuds sous **Périphériques** > **Microsoft SQL** > **Bases de données**. Pour installer Agents pour SQL sur les autres nœuds, sélectionnez l'AAG, cliquez sur **Détails**, puis sur **Installer un agent** en regard de chaque nœud.

2. Sélectionnez l'AAG ou la base de données 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 récupération à partir duquel vous voulez les restaurer.

   Quand vous sélectionnez une base de données en cluster sous **Périphériques** > **Microsoft SQL** > **Bases de données** et que vous cliquez sur **Restaurer**, le logiciel n'affiche que les points de

récupération 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 récupération 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 : `<nom AAG> - <nom plan protection>` 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.

   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 AlwaysOn 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'AGG 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

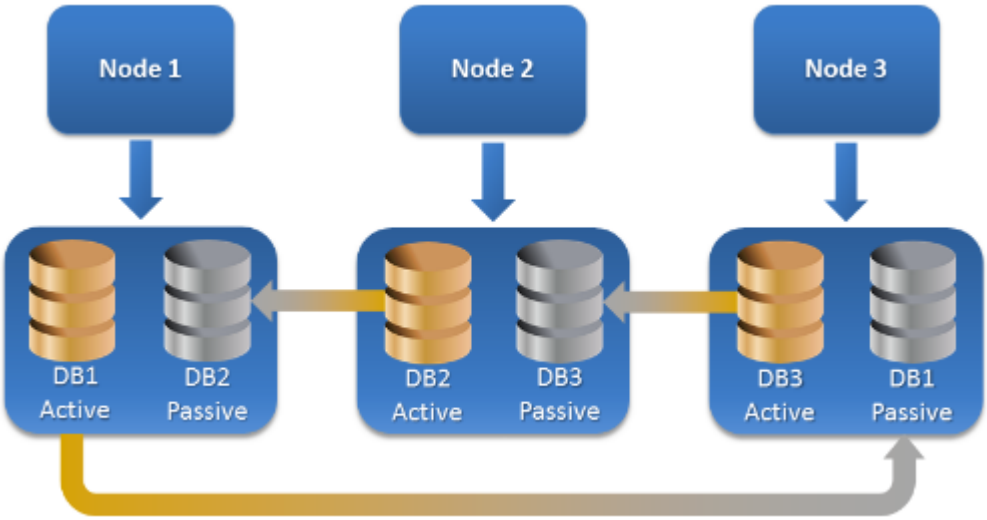
Grâce à la sauvegarde prenant en charge les clusters, vous sauvegardez seulement une copie des données du cluster. Si les données changent d'emplacement au sein du cluster (en raison d'un

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.

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
Après avoir installé l'agent sur l'un des nœuds, la console Web 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 ».

2. Configurez l'option de sauvegarde « Mode de sauvegarde de cluster ».
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.

Restauration des données du cluster Exchange

1. Sélectionnez le point de récupération 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 **Périphériques** > **Microsoft Exchange** > **Bases de données** > `<nom du cluster>` > `<nom du nœud` et cliquez sur **Restaurer**, le logiciel n'affiche que les points de récupération correspondant aux fois où la copie a été sauvegardée.
   La façon la plus simple d'afficher tous les points de récupération 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 » 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 de niveau disque reconnaissant les applications est disponible pour les machines physiques, les machines virtuelles ESXi et les machines virtuelles Hyper-V.

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 :

1. Les applications sont sauvegardées dans un état cohérent et sont donc immédiatement disponibles après la restauration de la machine.

2. 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.
3. 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.
4. 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, aucun agent d'installation n'est nécessaire ; on suppose que la machine est sauvegardée par l'agent pour VMware (Windows) ou l'agent pour Hyper-V.

Remarque
Pour les machines virtuelles Hyper-V exécutant Windows Server 2022, la sauvegarde reconnaissant les applications n'est pas prise en charge en mode sans agent, c'est-à-dire lorsque la sauvegarde est effectuée par l'agent pour Hyper-V. Pour protéger les applications Microsoft sur ces machines, installez l'agent pour Windows dans le système d'exploitation invité.

L'agent pour VMware (matériel virtuel) et l'agent pour VMware (Windows) peuvent créer des sauvegardes reconnaissant l'application, mais ne peuvent pas restaurer de données d'application provenant de ces sauvegardes. Pour restaurer des données d'application à partir de sauvegardes créées par ces agents, 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 récupération sur l'onglet **Stockage de sauvegarde**, puis sélectionnez cette machine dans **Machine à parcourir**.

Les autres critères sont répertoriés dans les sections "Prérequis" (p. 454) et "Droits utilisateur requis pour la sauvegarde reconnaissant les applications" (p. 463).

Droits utilisateur requis pour la sauvegarde 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 :

  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.
- Pour Exchange Server :

  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 informations d'identification d'un administrateur de domaine intégré (DOMAIN\Administrator) lors de l'activation d'une sauvegarde d'application.

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 les politiques de CCU, vous devez fournir les identifiants d'un administrateur de domaine intégré (DOMAIN\Administrator) lors de la configuration des sauvegardes reconnaissant les applications.

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.

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**.

Pour connecter l'agent pour Exchange au CAS

1. Cliquez sur **Périphériques** > **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 **Périphériques** > **Microsoft Exchange** > **Boîtes aux lettres**.

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 **Périphériques** > **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 **Sauvegarder**.

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 en savoir plus sur la configuration du rôle de gestion **ApplicationImpersonation**, consultez l'article suivant de base de connaissances Microsoft : https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

Restauration de bases de données SQL

Cette section décrit la restauration depuis des sauvegardes de base de données et des sauvegardes reconnaissant les applications.

Vous pouvez restaurer les bases de données SQL sur une instance SQL Server, à condition que l'agent pour SQL soit installé sur la machine de l'instance.

Si vous utilisez l'authentification Windows, vous devrez fournir les identifiants d'un compte membre du groupe **Opérateurs de sauvegarde** ou **Administrateurs** sur la machine, et membre du rôle **sysadmin** sur l'instance cible. Si vous utilisez l'authentification SQL Server, vous devrez fournir les identifiants d'un compte membre du rôle **sysadmin** sur l'instance cible.

Parallèlement, vous pouvez restaurer les bases de données en tant que fichiers. Cela 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. Vous pouvez attacher les fichiers de base de données SQL à une instance SQL Server, comme décrit dans « Attacher des bases de données SQL Server ».

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 (matériel virtuel) n'est pas possible.

Les bases de données système sont généralement restaurées de la même façon que les bases de données utilisateurs. Les particularités de la restauration des bases de données système sont présentées à la section « Restauration de bases de données système ».

Pour restaurer des bases de données SQL vers une instance SQL Server

1. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, sous **Périphériques**, 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 **Périphériques** > **Microsoft SQL**, 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 SQL, puis choisissez un point de récupération.
   - Sélectionnez un point de récupération 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 bases de données SQL.
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 SQL**, sélectionnez la base de données que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
   - Lors d'une restauration depuis une sauvegarde de base de données, cliquez sur **Restaurer** > **Bases de données vers une instance**.
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. Vous pouvez sélectionner une autre instance SQL Server (fonctionnant sur la même machine) pour effectuer la restauration des bases de données.

   Pour restaurer une base de données en tant que base de données différente vers la même instance :

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. [Facultatif] [Non disponible pour une base de données restaurée à son instance d'origine en tant que nouvelle base de données] Pour changer le statut d'une base de données après restauration, cliquez sur le nom de la base de données, puis choisissez l'un des statuts suivants :
   - **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.
7. Cliquez sur **Démarrer la restauration**.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour restaurer des bases de données SQL sous forme de fichiers

1. Effectuez l'une des actions suivantes :
   - Lors d'une restauration à partir d'une sauvegarde reconnaissant les applications, sous **Périphériques**, 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 **Périphériques** > **Microsoft SQL**, 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 SQL ou Agent pour VMware, puis choisissez un point de récupération
- Sélectionnez un point de récupération 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 bases de données SQL.

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 SQL**, sélectionnez les bases de données que vous souhaitez restaurer, puis cliquez sur **Restaurer en tant que fichiers**.
   - 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**.

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.

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
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 (matériel virtuel) 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 **Périphériques**, 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 **Périphériques** > **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 récupération.
   - Sélectionnez un point de récupération 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 récupération 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**.
   - 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 **Périphériques**, 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 **Périphériques** > **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 récupération.
   - Sélectionnez un point de récupération 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 récupération 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**.

- 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

Cette section décrit comment restaurer des boîtes aux lettres et des éléments de boîtes aux lettres Exchange depuis des sauvegardes reconnaissant les applications et des sauvegardes de boîte aux lettres. La ou les boîtes aux lettres peuvent être restaurée(s) sur Exchange Server en temps réel ou sur Microsoft 365.

Les éléments suivants peuvent être restaurés :

- Boîtes aux lettres (à l'exception des boîtes aux lettres archivées)
- Dossiers publics

Remarque
Disponible uniquement depuis les sauvegardes de base de données. Voir "Sélection de données Exchange Server" (p. 457)

- 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.

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*.

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 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 de Microsoft 365, consultez la section "Protection des boîtes aux lettres Microsoft 365" (p. 482).

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 Office 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 Office 365 au sein de votre organisation, installez un agent pour Office 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 Office 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 Office 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 **Périphériques**, 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 **Périphériques** > **Microsoft Exchange** > **Bases de données**, puis sélectionnez la base de données qui contenait à l'origine les données que vous voulez restaurer.

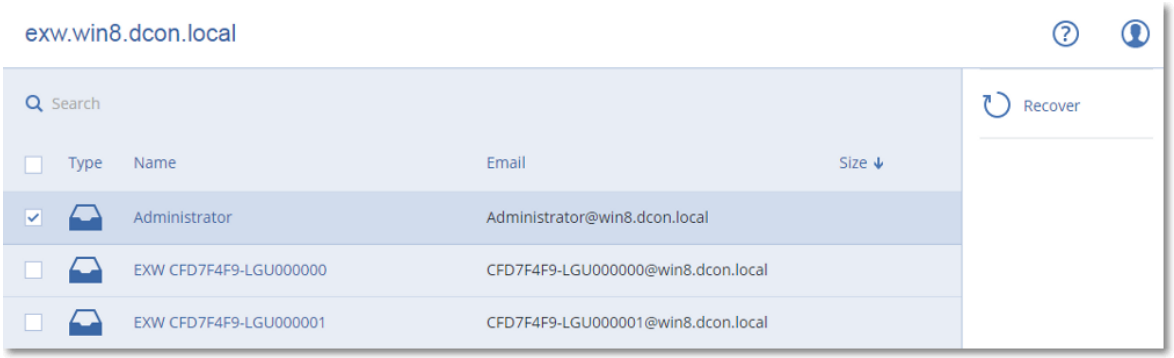
3. Cliquez sur **Restauration**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

   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 récupération.
   - Sélectionnez un point de récupération 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 Office 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. 466).

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**.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour restaurer une boîte aux lettres à partir d'une sauvegarde de boîte aux lettres

1. Cliquez sur **Périphériques** > **Microsoft Exchange** > **Boîtes aux lettres**.
2. Sélectionnez la boîte aux lettres à restaurer, puis cliquez sur **Restaurer**.

   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 Office 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 Office 365 au sein de votre organisation, installez un agent pour Office 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 Office 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 Office 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 **Périphériques**, 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 **Périphériques** > **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 récupération.
   - Sélectionnez un point de récupération 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.

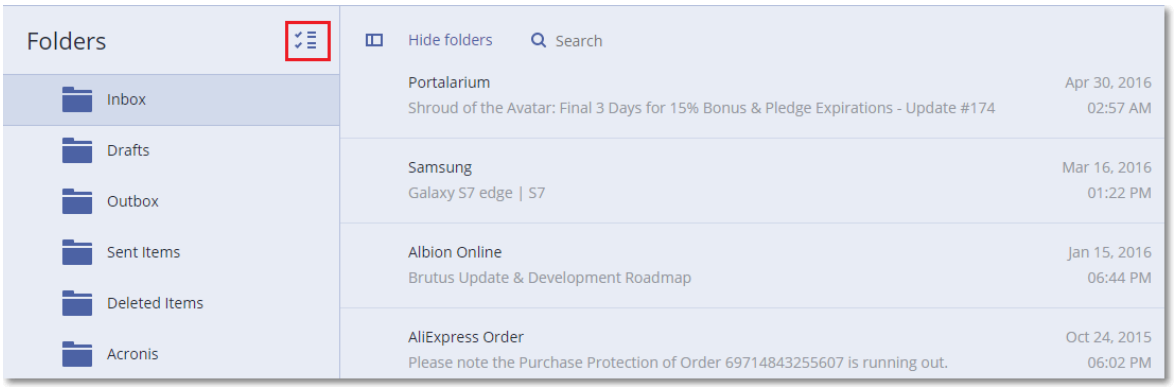
   Les options de recherche suivantes sont disponibles. Les caractères génériques ne sont pas pris en charge.

   - 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.



8. Cliquez sur **Restaurer**.
9. Pour restaurer Microsoft 365, sélectionnez **Microsoft Office 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 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. 466).
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**.

La progression de la restauration sont affichées dans l'onglet **Activités**.

Pour restaurer un élément de boîte aux lettres à partir d'une sauvegarde de boîte aux lettres

1. Cliquez sur **Périphériques** > **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.

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 Office 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.

Pour modifier les informations d'identification de SQL Server ou Exchange Server

1. Cliquez sur **Périphériques**, puis sur **Microsoft SQL** ou **Microsoft Exchange**.
2. Sélectionnez le groupe de disponibilité AlwaysOn, 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 **Périphériques** > **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 boîtes aux lettres Microsoft 365

Important
Cette section est valable pour des déploiements sur site de Acronis Cyber Protect. Si vous utilisez un déploiement dans le Cloud, veuillez consulter le site https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html.

Pour en savoir plus sur les options de licence, consultez Acronis Cyber Backup pour les licences Microsoft 365.

Pourquoi sauvegarder les boîtes aux lettres Microsoft 365 ?

Bien que Microsoft 365 soit un service de Cloud, l'exécution de sauvegardes régulières offre une couche de protection supplémentaire contre les erreurs des utilisateurs et les actions malveillantes intentionnelles. Il est possible de restaurer les éléments supprimés d'une sauvegarde même après expiration de la période de rétention de Microsoft 365. De la même manière, pour des raisons de conformité à d'éventuelles réglementations, il est possible de conserver une copie locale des boîtes aux lettres Microsoft 365.

Restauration

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.

La restauration peut être réalisée sur Microsoft 365 ou sur Exchange Server en temps réel.

Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres Microsoft 365 existante, les éléments existants dont les identifiants sont identiques sont écrasés. Lorsqu'une boîte aux lettres est restaurée sur une boîte aux lettres existante sur un serveur Exchange, les éléments existants sont conservés tels quels. Les éléments restaurés sont placés à leurs côtés.

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.

Limites

- L'application d'un plan de protection à plus de 500 boîtes aux lettres peut dégrader les performances de sauvegarde. Pour protéger davantage de boîtes aux lettres, créez plusieurs plans de protection et planifiez leur exécution à des horaires différents.
- Les boîtes aux lettres archivées (**Archives permanentes**) ne peuvent pas être sauvegardées.
- 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 restauration vers une nouvelle boîte aux lettres Microsoft 365 n'est pas possible. Vous devez d'abord créer un nouvel utilisateur Microsoft 365 manuellement, puis restaurer les éléments vers la boîte aux lettres de cet utilisateur.
- La restauration vers une autre organisation Microsoft 365 n'est pas prise en charge.
- Certains types ou propriétés d'éléments pris en charge par Microsoft 365 peuvent ne pas être pris en charge par Exchange Server. Ils seront ignorés pendant la restauration sur Exchange Server.

Ajout d'une organisation Microsoft 365

Pour ajouter une organisation Microsoft, vous devez connaître l'identifiant et le code 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.

Pour ajouter une organisation Microsoft 365

1. Installez l'agent pour Office 365 sur une machine Windows connectée à Internet. Il ne peut y avoir qu'un seul agent pour Office 365 au sein d'une organisation.
2. Dans la console Web Cyber Protect, cliquez sur **Microsoft Office 365**.
3. Dans la fenêtre qui s'ouvre, saisissez l'identifiant et le secret de l'application, ainsi que l'identifiant du tenant Microsoft 365.
4. Cliquez sur **Connexion**.

Les éléments de données de votre organisation apparaissent ensuite dans la console Web Cyber Protect de l'onglet **Microsoft Office 365**.

Obtention de l'identifiant et du secret d'application

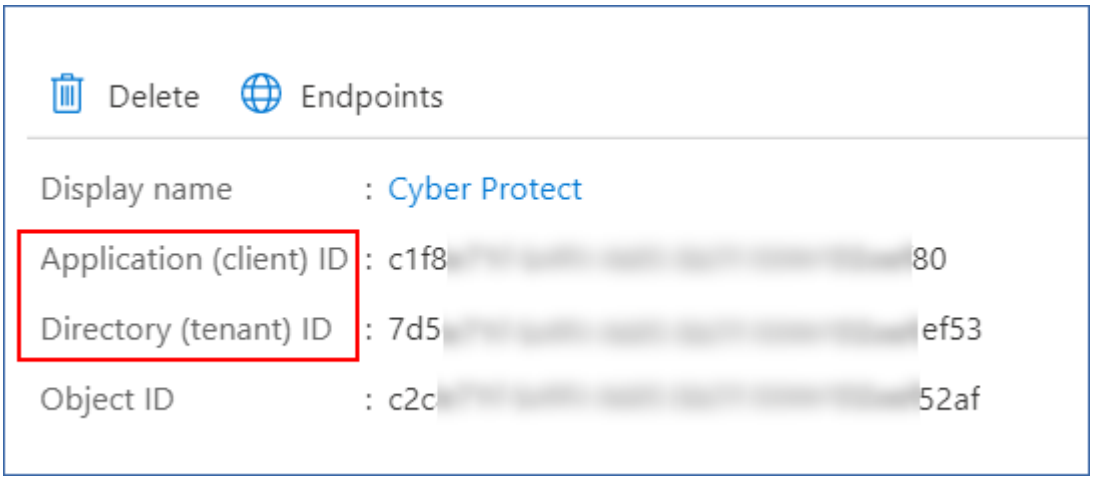
Pour utiliser l'authentification moderne pour Microsoft 365, vous devez créer une application personnalisée dans Azure Active Directory et lui attribuer une permission d'API spécifique. Vous

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 Web Cyber Protect.

Pour créer une application dans Azure Active Directory

1. Connectez-vous au portail Azure 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 Protect.
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 portail Azure, accédez à la page **Vue d'ensemble** de l'application, puis vérifiez l'identifiant de votre application (client) et le répertoire (identifiant du tenant).



Pour plus d'informations sur la création d'une application dans le portail Azure, reportez-vous à la documentation Microsoft.

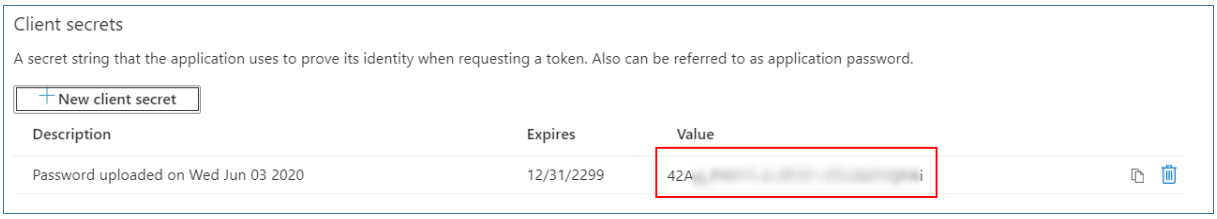
Pour accorder à l'application les permissions d'API nécessaires

1. Sur le portail Azure, accédez aux **permissions d'API** de l'application, puis cliquez sur **Ajouter une permission**.
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**.
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 <nom de votre application>**.
10. Confirmez votre choix en cliquant sur **Oui**.

Pour créer un secret d'application

1. Sur le portail Azure, accédez à **Certificat et secrets** > **New secret du client** de votre application.
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. Dans la console Web Cyber Protect, accédez à **Périphériques** > **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.
5. Cliquez sur **Connexion**.

Sélection de boîtes aux lettres

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. Dans la console Web Cyber Protect, accédez à **Périphériques** > **Microsoft Office 365**.
2. Sélectionnez les boîtes aux lettres que vous voulez sauvegarder.
3. Cliquez sur **Sauvegarder**.

Restauration de boîtes aux lettres et d'éléments de boîte aux lettres

Restauration de boîtes aux lettres

1. [Uniquement lors d'une restauration vers Exchange Server] Assurez-vous qu'il existe un utilisateur Exchange avec le même identifiant de connexion que le nom d'utilisateur de l'utilisateur pour lequel la boîte aux lettres est restaurée. Dans le cas contraire, créez l'utilisateur. Voir la liste complète des conditions requises pour cet utilisateur dans "Exigences sur les comptes d'utilisateur" (p. 474).
2. Dans la console Web Cyber Protect, accédez à **Périphériques** > **Microsoft Office 365**.
3. Sélectionnez la boîte aux lettres à restaurer, puis cliquez sur **Restaurer**.

   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**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
5. Cliquez sur **Restaurer** > **Boîte aux lettres**.
6. Pour effectuer une restauration vers Exchange Server, dans **Restaurer vers** sélectionnez **Microsoft Exchange**. Poursuivez la restauration comme décrit dans "Restauration de boîtes aux lettres" (p. 475), en commençant par l'étape 9. Les étapes suivantes de cette procédure ne sont pas nécessaires.

   Pour restaurer Microsoft 365, dans **Restaurer vers**, conservez la valeur **Microsoft Office 365** par défaut.
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**.

Restauration d'éléments de boîte aux lettres

1. [Uniquement lors d'une restauration vers Exchange Server] Assurez-vous qu'il existe un utilisateur Exchange avec le même identifiant de connexion que le nom d'utilisateur de l'utilisateur pour lequel la boîte aux lettres est restaurée. Dans le cas contraire, créez l'utilisateur. Voir la liste complète des conditions requises pour cet utilisateur dans "Exigences sur les comptes d'utilisateur" (p. 474).
2. Dans la console Web Cyber Protect, accédez à **Périphériques** > **Microsoft Office 365**.

3. 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**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.
5. Cliquez sur **Restaurer** > **Messages électroniques**.
6. 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.

   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 : 
7. Cliquez sur **Restaurer**.
8. Pour effectuer une restauration vers Exchange Server, dans **Restaurer vers** sélectionnez **Microsoft Exchange**.

   Pour restaurer Microsoft 365, dans **Restaurer vers**, conservez la valeur **Microsoft Office 365** par défaut.
9. [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** de Microsoft Exchange Server 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. 466).

10. 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.
11. [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.
12. Cliquez sur **Démarrer la restauration**.

Protéger des données Google Workspace

Cette fonctionnalité est disponible uniquement dans les déploiements dans le Cloud de Acronis Cyber Protect. Pour une description détaillée de cette fonctionnalité, veuillez consulter le site https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html.

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/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf.

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 d'exécuter cette machine virtuelle temporaire pour 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.

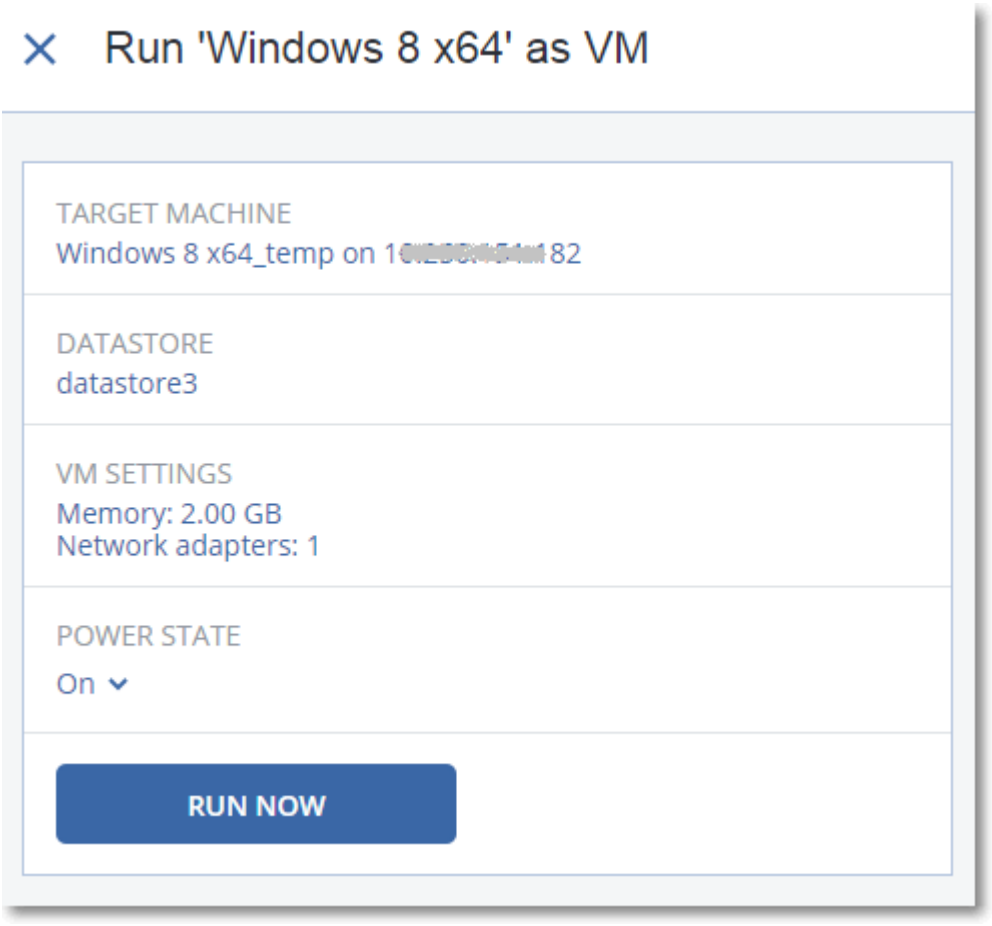
Prérequis

- Au moins un agent pour VMware ou Hyper-V doit être enregistré dans le service de cyber protection.
- La sauvegarde peut être stockée dans un dossier réseau, dans un nœud de stockage ou dans un dossier 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. Il n'est pas possible d'exécuter une machine virtuelle à partir d'une sauvegarde stockée sur un serveur SFTP, un périphérique à bandes ou Secure Zone.

- 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 récupération 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.

Suppression de la machine

Nous ne recommandons pas de supprimer une machine virtuelle temporaire directement dans vSphere/Hyper-V. 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 périphériques**, 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.

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 périphériques**, 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. récupération normale

Le processus de finalisation est plus lent qu'une récupération 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 récupération 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 recommandons d'exécuter des machines virtuelles à partir de sauvegardes locales si vous prévoyez d'effectuer la finalisation et que vous avez le choix.

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 Changed Block Tracking, 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.
- **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 charge de travail 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.

Restrictions

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

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.
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 périphériques** 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

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.

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**.

Suivi des blocs modifiés (CBT)

Cette option est identique à l'option de sauvegarde « Changed Block Tracking (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.

Important
Pour réaliser l'amorçage d'un réplica, l'agent pour VMware (matériel virtuel) 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.

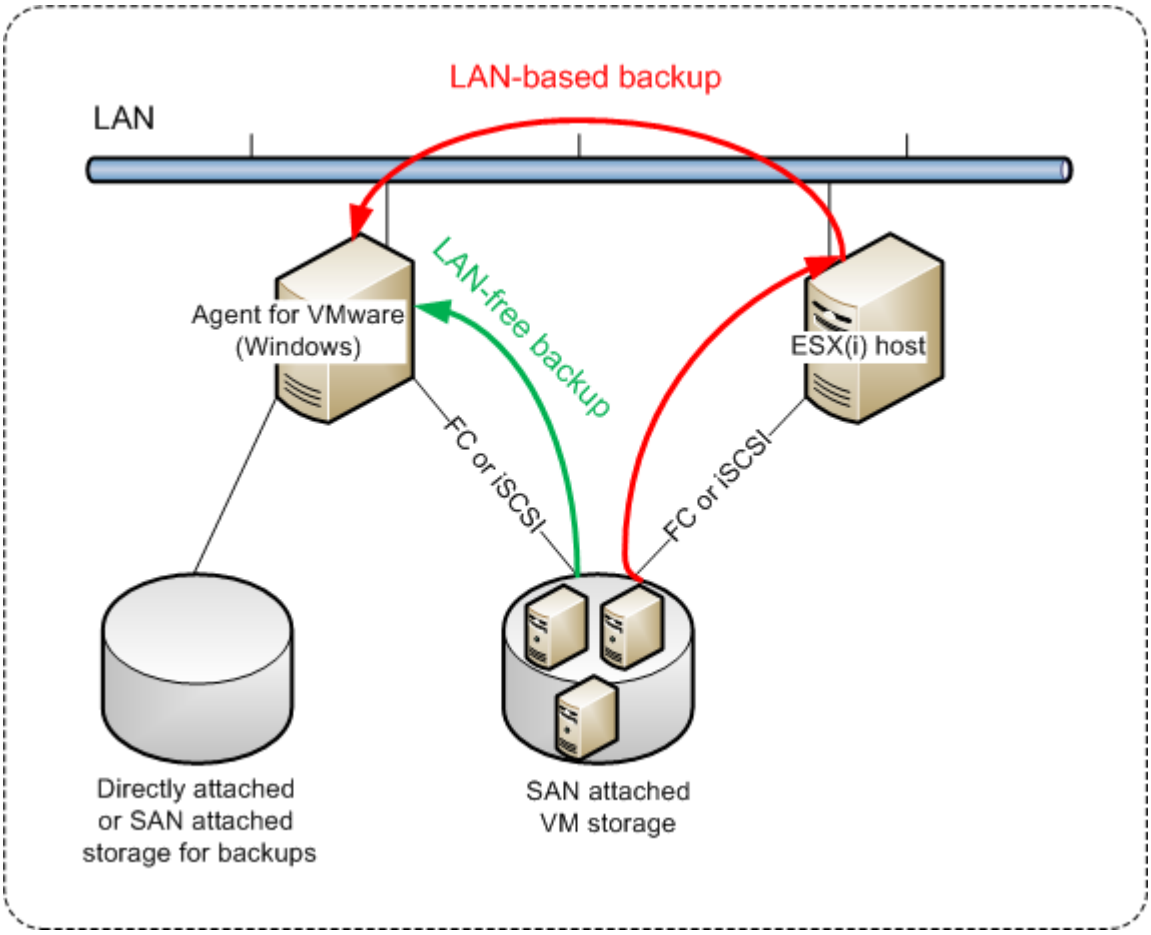
En conséquence, le logiciel continuera à mettre à jour le réplica. Toutes les réplications seront incrémentielles.

Sauvegarde sans LAN

Si vos hôtes de production ESXi sont si lourdement chargés qu'il n'est pas souhaitable d'exécuter les matériels virtuels, pensez à installer l'agent pour VMware (Windows) sur une machine physique ne faisant pas partie de l'infrastructure ESXi.

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 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.

     Pour éviter l'initialisation du LUN, la **stratégie SAN** est automatiquement définie sur **Tout hors ligne** pendant l'installation de l'agent pour VMware (Windows).

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.

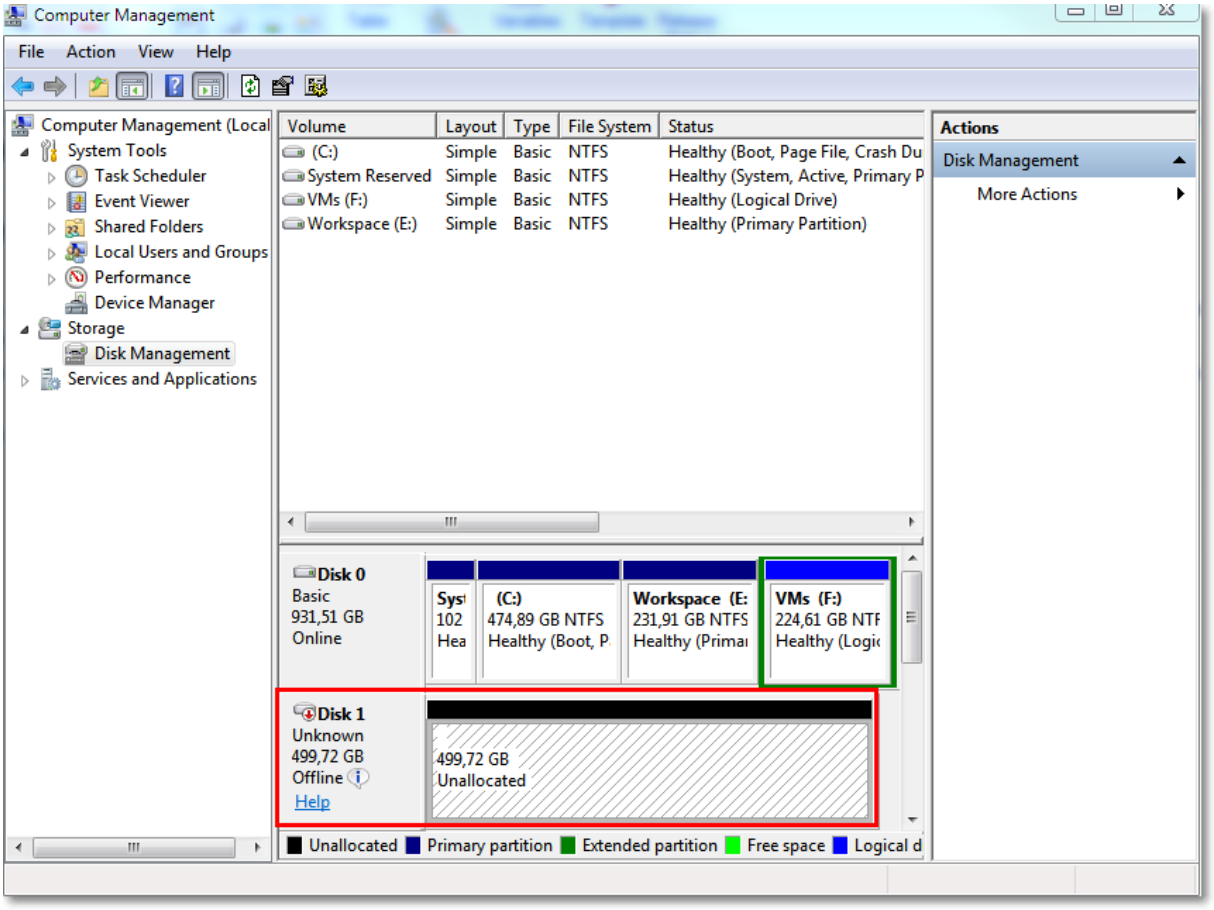
Pour configurer un initiateur iSCSI

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 **Connecter**.
   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'instantanés matériels SAN

Si votre VMware vSphere utilise un système de stockage de réseau de zone de stockage (SAN) en tant que magasin de données, vous pouvez activer l'Agent pour VMware (Windows) pour utiliser des instantanés matériels lorsque vous effectuez une sauvegarde.

Important
Seul le stockage SAN de NetApp est pris en charge.

Pourquoi utiliser des instantanés matériels SAN ?

L'Agent pour VMware a besoin d'un instantané de machine virtuelle pour créer une sauvegarde cohérente. Étant donné que l'agent lit le contenu du disque virtuel depuis l'instantané, ce dernier doit être conservé pendant toute la durée du processus de sauvegarde.

Par défaut, l'agent utilise des instantanés VMware natifs créés par l'hôte ESXi. Alors que l'instantané est conservé, les fichiers du disque virtuel sont en lecture seule, et l'hôte inscrit tous les changements apportés aux disques pour séparer les fichiers delta. Une fois le processus de

sauvegarde terminé, l'hôte supprime l'instantané, c'est-à-dire qu'il fusionne les fichiers delta avec les fichiers du disque virtuel.

Conserver aussi bien que supprimer l'instantané affecte la performance de la machine virtuelle. Avec des disques virtuels de grande capacité et des changements rapides de données, ces opérations prennent du temps, pendant lequel la performance peut se détériorer. Dans des cas extrêmes, lorsque plusieurs machines sont sauvegardées en même temps, les fichiers delta croissants peuvent presque entièrement remplir le magasin de données et provoquer l'arrêt de toutes les machines virtuelles.

Vous pouvez réduire l'utilisation de la ressource hyperviseur en déchargeant les instantanés vers le SAN. Dans ce cas, la séquence d'opérations est comme suit :

1. L'ESXi prend un instantané VMware au début du processus de sauvegarde, pour que l'état des disques virtuels soit cohérent.
2. Le SAN crée un instantané matériel du volume ou LUN qui contient la machine virtuelle et son instantané VMware. Cette opération prend généralement quelques secondes.
3. L'ESXi supprime l'instantané VMware. L'Agent pour VMware lit le contenu du disque virtuel à partir de l'instantané matériel SAN.

Étant donné que l'instantané VMware est conservé uniquement pendant quelques secondes, la détérioration de la performance de la machine virtuelle est minimisée.

De quoi ai-je besoin pour utiliser les instantanés matériels SAN ?

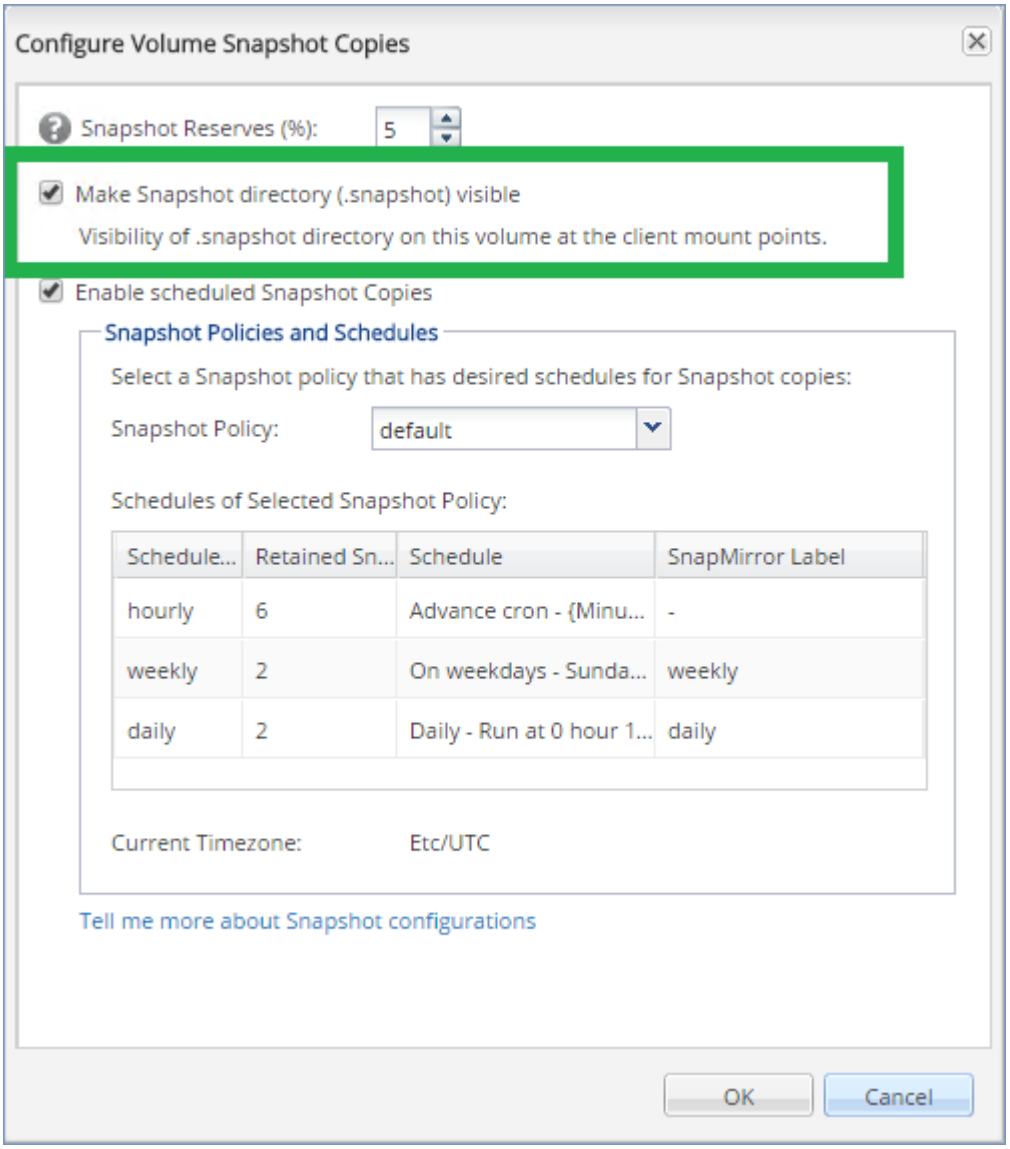
Si sous souhaitez utiliser les instantanés matériels SAN lors de la sauvegarde des machines virtuelles, assurez-vous que toutes les conditions suivantes sont remplies :

- Le stockage SAN NetApp remplit les conditions requises décrites dans la section « Configuration requise pour le stockage SAN de NetApp ».
- La machine exécutant l'Agent pour VMware (Windows) est configurée comme décrit dans la section « Configuration de la machine sur laquelle s'exécute l'Agent pour VMware ».
- Le stockage SAN est enregistré sur le serveur de gestion.
- [S'il existe des Agents pour VMware qui n'ont pas pris part à l'enregistrement ci-dessus] Les machines virtuelles qui résident dans le stockage SAN sont affectées à des agents compatibles avec un SAN, tel que décrit dans la section « Liaisons des machines virtuelles ».
- L'option de sauvegarde Instantanés matériels SAN est activée dans les options du plan de protection.

Configuration requise pour le stockage SAN de NetApp

- Le stockage SAN doit être utilisé comme magasin de données NFS ou iSCSI.
- Le SAN doit exécuter Data ONTAP 8.1 ou version ultérieure dans le mode **Clustered Data ONTAP (cDOT)**. Le mode **7-Mode** n'est pas pris en charge.
- Dans NetApp OnCommand System Manager, la case à cocher **Snapshot copies** > **Configure** > **Make Snapshot directory (.snapshot) visible** doit être sélectionnée pour le volume où le

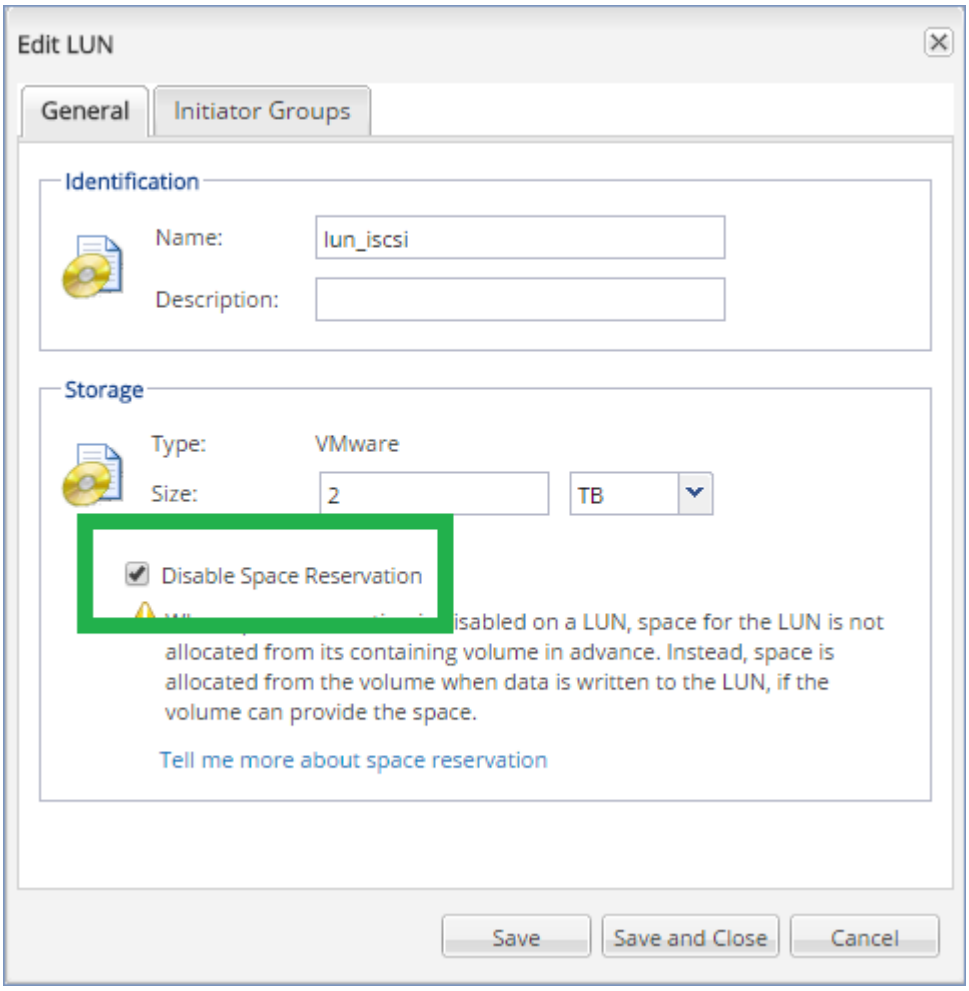
magasin de données se trouve.



- [Pour les magasins de données NFS] L'accès aux partages NFS depuis les clients Windows NFSv3 doit être activé sur la machine virtuelle de stockage spécifiée lors de la création du magasin de données. L'accès peut être activé grâce à la commande suivante :

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  Pour plus d'informations, consultez le document NetApp Best Practices : https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [Pour les magasins de données iSCSI] Dans NetApp OnCommand System Manager, la case à cocher **Disable Space Reservation** doit être sélectionnée pour le LUN iSCSI où le magasin de données se trouve.



Configuration de la machine sur laquelle s'exécute l'agent pour VMware

Selon si le stockage SAN est utilisé comme magasin de données NFS ou iSCSI, consultez la section correspondante ci-dessous.

Configuration de l'initiateur iSCSI

Assurez-vous que toutes les conditions suivantes sont remplies :

- L'initiateur Microsoft iSCSI est installé.
- Le type de démarrage du service Initiateur iSCSI de Microsoft est paramétré sur **Automatique** ou **Manuel**. Ceci peut être fait dans le composant logiciel **Services**.
- L'initiateur iSCSI est configuré comme décrit dans la section d'exemples de « Sauvegarde sans LAN ».

Configuration du client NFS

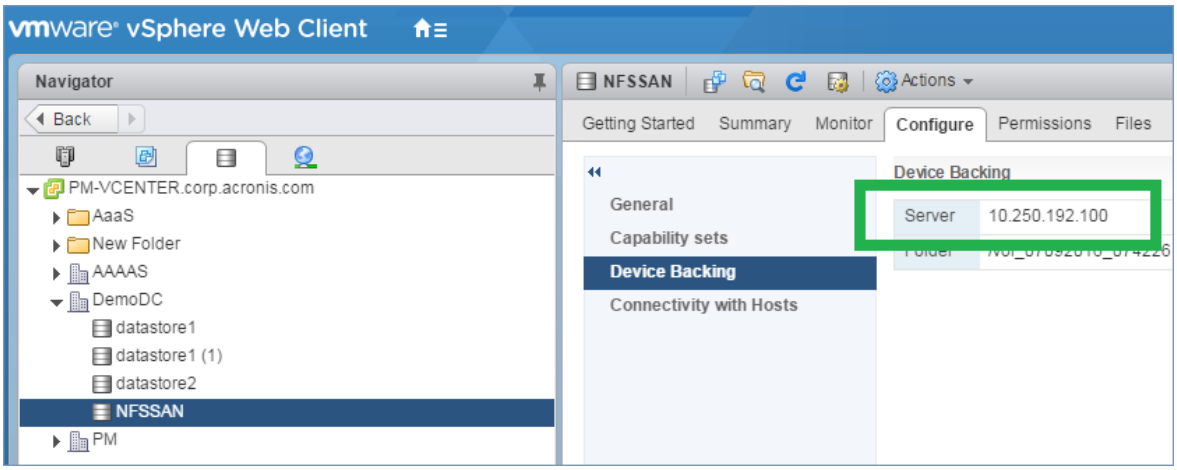
Assurez-vous que toutes les conditions suivantes sont remplies :

- **Services Microsoft pour NFS** (dans Windows Server 2008) ou **Client pour NFS** (dans Windows Server 2012 et ultérieur) sont installés.

- Le client NFS est configuré pour un accès anonyme. Cela peut être fait comme suit :
  a. Ouvrez l'Éditeur du Registre
  b. Localisez la clé de registre suivante : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
  c. Dans cette clé, créez une nouvelle valeur **DWORD** nommée **AnonymousUID** et définissez sa valeur sur 0.
  d. Dans la même clé, créez une nouvelle valeur **DWORD** nommée **AnonymousGID** et définissez sa valeur sur 0.
  e. Redémarrez la machine.

Enregistrement du stockage SAN sur le serveur de gestion

1. Cliquez sur **Paramètres** > **Stockage SAN**.
2. Cliquez sur **Ajouter stockage**.
3. [Facultatif] Dans **Nom**, modifiez le nom du stockage.
   Ce nom s'affichera dans l'onglet **Stockage SAN**.
4. Dans **Nom d'hôte ou adresse IP**, indiquez la machine virtuelle de stockage NetApp (SVM, également appelée serveur de fichiers) spécifiée lors de la création du magasin de données.
   Pour trouver les informations requises dans VMware vSphere Web Client, sélectionnez le magasin de données, puis cliquez sur **Configure** (Configurer) > **Device backing** (Sauvegarde du périphérique). Le nom de l'hôtel ou l'adresse IP s'affichent dans le champ **Serveur**.



5. Dans **User name** (Nom d'utilisateur) et **Password** (Mot de passe), saisissez les accréditations de l'administrateur SVM.

   Important
   Le compte spécifié doit être celui d'un administrateur local sur le SVM, plutôt que celui de l'administrateur de gestion du système NetApp.

   Vous pouvez spécifier un utilisateur existant ou en créer un nouveau. Pour créer un nouvel utilisateur, dans NetApp OnCommand System Manager, allez dans **Configuration** > **Security** (Sécurité) > **Users** (Utilisateurs), puis créez un nouvel utilisateur.

6. Sélectionnez un ou plusieurs agent(s) pour VMware (Windows) qui bénéficieront d'une autorisation de lecture pour ce périphérique SAN.
7. Cliquez sur **Ajouter**.

Utilisation d'un stockage attaché localement

Vous pouvez connecter un disque supplémentaire à un agent pour VMware (matériel virtuel) pour que l'agent puisse effectuer des sauvegardes sur ce stockage connecté localement. Cette approche élimine le trafic réseau entre l'agent et l'emplacement de sauvegarde.

Un matériel virtuel en cours d'exécution sur le même hôte ou cluster avec les machines virtuelles ont un accès direct au(x) magasin(s) de données où se trouvent les machines. Cela signifie que 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. Si le magasin de données est connecté comme **Disque/LUN** plutôt que **NFS**, la sauvegarde sera entièrement sans réseau local. Dans le cas d'un magasin de données NFS, il y aura du trafic réseau entre le magasin de données et l'hôte.

L'utilisation d'un stockage attaché localement présume que l'agent sauvegarde toujours les mêmes machines. Si plusieurs agents travaillent au sein de vSphere, et qu'un ou plusieurs d'entre eux utilisent des stockages attachés localement, vous devez manuellement lier chaque agent à toutes les machines qu'ils doivent sauvegarder. Autrement, si les machines sont redistribuées parmi les agents par serveur de gestion, les sauvegardes d'une machine pourraient être dispersées dans plusieurs stockages.

Vous pouvez ajouter le stockage à un agent qui fonctionne déjà ou lorsque vous déployez l'agent à partir d'un modèle OVF.

Pour connecter un stockage à un agent qui fonctionne déjà

1. Dans l'inventaire de VMware vSphere, faites un clic droit sur l'agent pour VMware (matériel virtuel).
2. Ajoutez le disque en modifiant les paramètres de la machine virtuelle. La taille du disque doit être d'au moins 10 Go.

   Avertissement !
   Faites bien attention lorsque vous ajoutez un disque déjà existant. Dès que le stockage est créé, toutes les données précédemment contenues sur ce disque sont perdues.

3. Allez à la console de l'appareil virtuel. Le lien **Créer un stockage** est disponible au bas de l'écran. S'il ne l'est pas, cliquez sur **Actualiser**.
4. Cliquez sur le lien **Créer un stockage**, sélectionnez le disque et donnez-lui un nom. La longueur du nom est limitée à 16 caractères à cause des limites du système de fichiers.

Pour sélectionner un stockage attaché localement comme une destination de sauvegarde

Lors de la création d'un plan de protection, dans **Où sauvegarder**, sélectionnez **Dossiers locaux**, puis tapez la lettre correspondant au stockage attaché localement, par exemple, **D:**.

Liaison de machine virtuelle

Cette section vous donne un aperçu de la façon dont le serveur de gestion organise l'opération de plusieurs agents dans VMware vCenter.

L'algorithme de distribution ci-dessous fonctionne à la fois pour les appareils virtuels 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 serveur de gestion 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 un appareil virtuel supplémentaires au 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 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.

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 périphériques**
- 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

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 appareils virtuels.
- La liaison manuelle est nécessaire si vous utilisez des instantanés matériels SAN. Liez l'Agent pour VMware (Windows) pour lequel les instantanés matériels SAN sont configurés avec les machines résidant dans le magasin de données SAN.
- Il est nécessaire de lier les MV à un agent si l'agent possède un stockage attaché localement.
- 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.

Prise en charge de la migration de MV

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

vMotion déplace l'état et la configuration d'une machine virtuelle vers un autre hôte alors que les disques de la machine demeurent dans le même emplacement dans le stockage partagé.

- La fonction vMotion de l'agent pour VMware (application virtuelle) n'est pas prise en charge et est désactivée.
- La fonction vMotion d'une machine virtuelle est désactivée lors d'une sauvegarde. Les sauvegardes continueront à être effectuées après la fin de la migration.

Stockage VMotion

La fonction Storage vMotion déplace les disques de machine virtuelle d'un magasin de données vers un autre.

- La fonction Storage vMotion de l'agent pour VMware (application virtuelle) n'est pas prise en charge et est désactivée.
- La fonction Storage vMotion d'une machine virtuelle est désactivée lors d'une sauvegarde. Les sauvegardes continueront à être effectuées après la migration.

Gestion des environnements de virtualisation

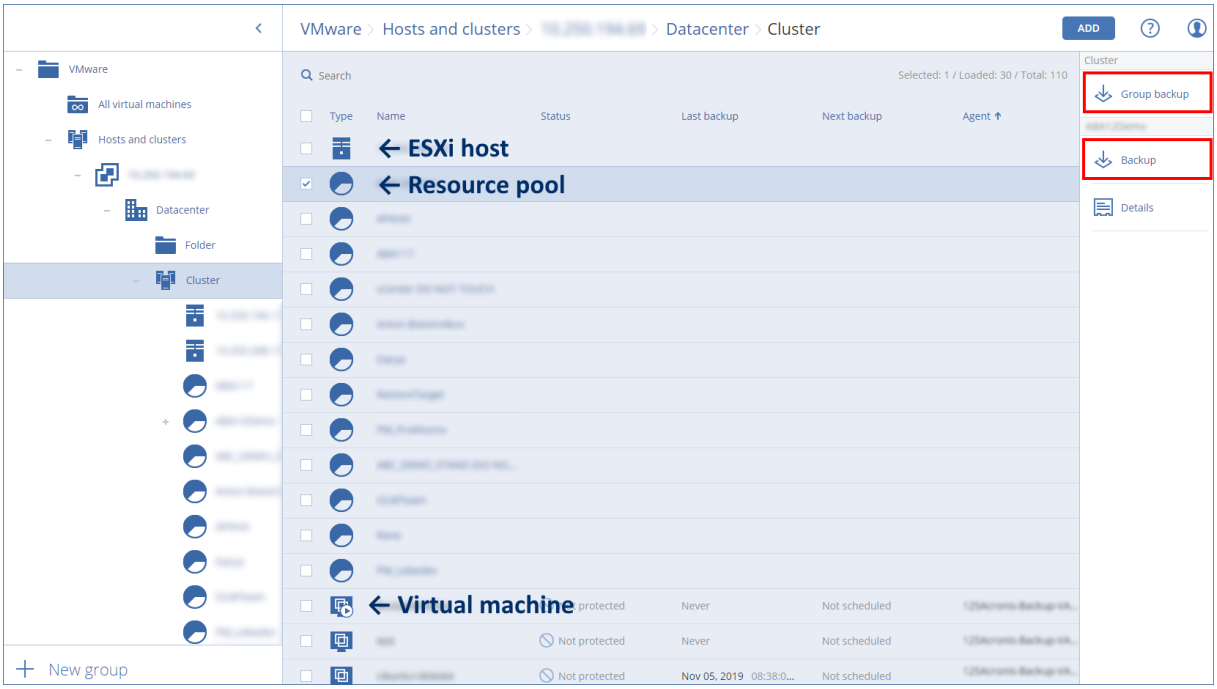
Vous pouvez afficher les environnements vSphere, Hyper-V et Virtuozzo dans leur présentation native. Une fois l'agent correspondant installé et enregistré, l'onglet **VMware**, **Hyper-V** ou **Virtuozzo** apparaît sous **Périphériques**.

Dans l'onglet **VMware**, vous pouvez sauvegarder les objets d'infrastructure VMware suivants :

- Centre de données
- Dossier
- Cluster
- Hôte ESXi
- Liste des ressources

Chacun de ces objets d'infrastructure fonctionne comme un objet de groupe pour les machines virtuelles. Lorsque vous appliquez un plan de protection à l'un de ces objets de groupe, toutes les machines virtuelles qui y sont incluses seront sauvegardées. Vous pouvez sauvegarder soit les machines de groupes sélectionnées en cliquant sur **Sauvegarder**, soit les machines de groupe parentes dans lesquelles le groupe sélectionné est inclus en cliquant sur **Sauvegarde de groupe**.

Par exemple, vous avez sélectionné le cluster, puis le pool de ressources qui s'y trouve. Si vous cliquez sur **Sauvegarder**, toutes les machines virtuelles incluses dans le pool de ressources sélectionné seront sauvegardées. Si vous cliquez sur **Sauvegarde groupe**, toutes les machines virtuelles incluses dans le cluster seront sauvegardées.



Vous pouvez modifier les informations d'identification pour le vCenter Server ou l'hôte ESXi autonome sans réinstaller l'agent.

Modification des informations d'identification d'accès au vCenter Server ou à l'hôte ESXi

1. Dans **Périphériques**, cliquez sur **VMware**.
2. Cliquez sur **Hôtes et clusters**.
3. Dans la liste **Hôtes et clusters** (à droite de l'arborescence **Hôtes et clusters**), sélectionnez le vCenter Server ou l'hôte ESXi autonome indiqué lors de l'installation de l'agent pour VMware.
4. Cliquez sur **Détails**.
5. Dans **Accréditations**, cliquez sur le nom d'utilisateur.
6. Indiquez les nouvelles informations d'identification, puis cliquez sur **OK**.

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 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**

Agent pour VMware – privilèges nécessaires

Cette section décrit les droits requis pour les opérations de machines virtuelles ESXi ainsi que pour le déploiement de matériels virtuels.

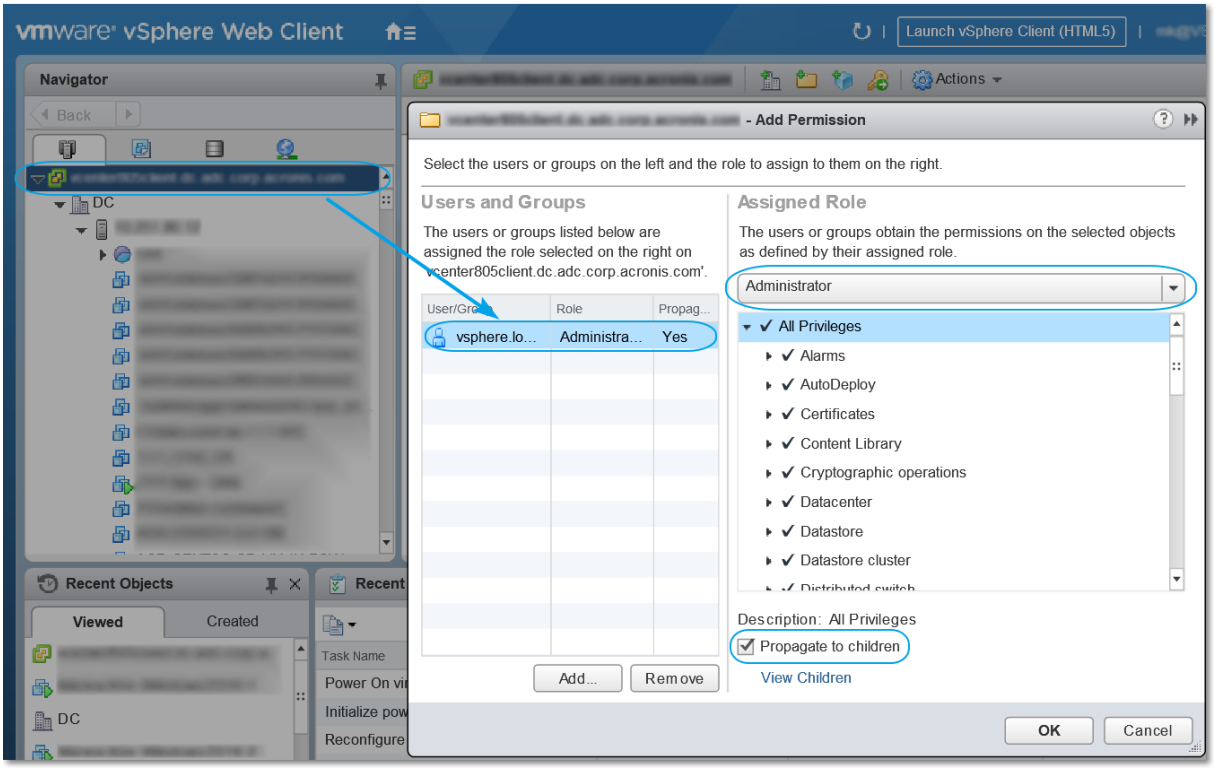
Remarque
Les API vStorage doivent être installées sur l'hôte ESXi pour autoriser la sauvegarde de machines virtuelles. Voir https://kb.acronis.com/content/14931.

Pour exécuter une opération avec des objets vCenter, comme les machines virtuelles, les hôtes ESXi, les clusters, vCenter et plus encore, l'agent pour VMware s'authentifie sur vCenter ou l'hôte ESXi à l'aide des identifiants vSphere fournis par un utilisateur. Le compte vSphere utilisé par l'agent pour VMware pour se connecter à vSphere doit disposer des privilèges nécessaires à tous les niveaux de l'infrastructure vSphere, à commencer par le niveau vCenter.

Précisez le compte vSphere disposant des privilèges nécessaires pendant l'installation ou la configuration de l'agent pour VMware. Si vous devez changer le compte ultérieurement, reportez-vous à la section « Gestion des environnements de virtualisation ».

Pour attribuer des autorisations à un utilisateur vSphere au niveau de vCenter, procédez comme suit :

1. Connectez-vous au client Web vSphere.
2. Faites un clic droit sur vCenter, puis cliquez sur **Ajouter une autorisation**.
3. Sélectionnez ou ajoutez un nouvel utilisateur ayant le rôle nécessaire (ce rôle doit inclure toutes les autorisations requises du tableau ci-dessous).
4. Sélectionnez l'option **Propager vers les enfants**.



Objet	Droit	Opération				
		Sauvegarder une MV	**Restaurer sur une nouvelle MV**	**Restaurer sur une MV existante**	**Exécuter une MV à partir d'une sauvegarde**	**Déploiement d'un appareil virtuel**
Opérations de chiffrement (à partir de vSphere 6.5)	**Ajouter un disque**	+*				
	Accès direct	+*				
Magasin de	**Allouer de**		+	+	+	+

données	**l'espace**					
	Parcourir le magasin de données				+	+
	Configurer un magasin de données	+	+	+	+	+
	Opérations de bas niveau sur les fichiers				+	+
Global	**Licences**	+	+	+	+	
	Désactiver les méthodes	+	+	+		
	Activer les méthodes	+	+	+		
	Gérer les rapports personnalisés	+	+	+		
	Définir un attribut personnalisé	+	+	+		
Hôte > **Configuration**	**Configuration du démarrage automatique de MV**					+
	Configuration de la partition de stockage				+	
Hôte - >**Inventaire**	**Modifier le cluster**					+
Hôte > **Opérations locales**	**Créer une MV**				+	+
	Supprimer une MV				+	+
	Reconfigurer une MV				+	+

Réseau	**Attribuer un réseau**		+	+	+	+
Ressource	**Attribuer une MV à un pool de ressources**		+	+	+	+
	Importer					+
Machine virtuelle > **Configuration**	**Ajouter un disque existant**	+	+		+	
	Ajouter un nouveau disque		+	+	+	+
	Ajouter ou supprimer un périphérique		+		+	+
	Advanced	+	+	+		+
	Modifier le nombre de processeurs		+			
	Suivi de changement de disque	+		+		
	Location de disque	+		+		
	Mémoire		+			
	Supprimer un disque	+	+	+	+	
	Renommer		+			
	Définir une annotation				+	
	Param.		+	+	+	
Machine virtuelle > **Opérations invité**	**Exécution de programme d'opération invité**	+**				+
	Requêtes	+**				+

	d'opération invité					
	Modifications des opérations invité	+**				
Machine virtuelle > **Interaction**	**Obtenir le ticket de contrôle invité** (dans vSphere 4.1 et 5.0)				+	+
	Configurer le support CD		+	+		
	Interaction de la console					+
	Gestion du système d'exploitation invité par VIX API (dans vSphere 5.1 et versions ultérieures)				+	+
	Mettre hors tension			+	+	+
	Mettre sous tension		+	+	+	+
Machine virtuelle > **Inventaire**	**Créer à partir d'une machine existante**		+	+	+	
	Créer une nouvelle		+	+	+	+
	Déplacement					+
	Inscrire				+	
	Supprimer		+	+	+	+
	Désinscrire				+	
Machine virtuelle >	**Autoriser l'accès au**		+	+	+	

Allocation	**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 instantané**	+		+	+	+
	Supprimer l'instantané	+		+	+	+
vApp	**Ajouter une machine virtuelle**				+	

* Ce droit est uniquement obligatoire pour les sauvegardes de machines chiffrées.

** Ce droit est uniquement obligatoire pour les sauvegardes reconnaissant les applications.

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 sur le serveur de gestion.

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, ou que vous effectuez une conversion vers une machine virtuelle Hyper-V dans le cadre d'un plan de protection, 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**.

Limite le nombre total de machines virtuelles sauvegardées simultanément.

L'option de sauvegarde **Planification** définit le nombre de machines virtuelles qu'un agent peut sauvegarder simultanément lors de l'exécution d'un plan de protection donné.

Lorsque plusieurs plans de protection se chevauchent dans le temps, les nombres spécifiés dans leurs options de sauvegarde sont additionnés. Même si le nombre total résultant est limité de manière programmée à 10, les plans qui se chevauchent affectent les performances de sauvegarde et surchargent aussi bien l'hébergeur que le stockage de la machine virtuelle.

Vous pouvez réduire davantage le nombre total de machines virtuelles qu'un agent pour VMware ou un agent pour Hyper-V peut sauvegarder simultanément.

Pour limiter le nombre total de machines virtuelles qu'un agent pour VMware (Windows) ou un agent pour Hyper-V peut sauvegarder :

1. Sur la machine exécutant l'agent, 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\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. Procédez comme suit pour redémarrer l'agent :
   a. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis entrez : **cmd**.
   b. Cliquez sur **OK**.
   c. Exécutez les commandes suivantes :

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

Pour limiter le nombre total de machines virtuelles qu'un agent pour VMware (matériel virtuel) ou un agent pour Hyper-V (Linux) peut sauvegarder :

1. Sur la machine exécutant l'agent, démarrez l'interface de commande :
   - **Agent pour VMware (matériel virtuel) :** appuyez sur CTRL+SHIFT+F2 lorsque vous vous trouvez dans l'interface utilisateur du matériel virtuel.
   - **Agent pour VMware (Linux) :** connectez-vous en tant qu'utilisateur root (superutilisateur) à l'ordinateur exécutant l'appliance Acronis Cyber Protect. Le mot de passe est le même que pour la console Web Cyber Protect.
2. Ouvrez le fichier **/etc/Acronis/MMS.config** avec un éditeur de texte, tel que **vi**.
3. Localisez la section suivante :

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Remplacez `10` par la valeur décimale de la limite que vous souhaitez définir.
5. Enregistrez le fichier.
6. Redémarrez l'agent :
   - **Agent pour VMware (appliance virtuelle) :** exécutez la `reboot` commande.
   - **Agent pour VMware (Linux) :** exécutez la commande suivante :

```
sudo service acronis_mms restart
```

Migration de machine

Vous pouvez effectuer une migration de machine en restaurant sa sauvegarde sur une machine autre que celle d'origine.

Le tableau suivant résume les options de migration disponibles.

Type de machine sauvegardée	Destinations de restauration disponibles							
	Machine physique	Machine virtuelle ESXi	Machine virtuelle Hyper-V	Machine virtuelle Virtuozzo*	Conteneur Virtuozzo*	Machine virtuelle Virtuozzo Hybrid Infrastructure*	Machine virtuelle HC3 de Scale Computing	Machine virtuelle RHV/oVirt*
Machine physique	+	+	+	-	-	+	+	+
Machine virtuelle VMware ESXi	+	+	+	-	-	+	+	+
Machine virtuelle Hyper-V	+	+	+	-	-	+	+	+
Machine virtuelle Virtuozzo*	+	+	+	+	-	+	+	+
Conteneur Virtuozzo*	-	-	-	-	+	-	-	-
Machine virtuelle Virtuozzo Hybrid Infrastructure*	+	+	+	-	-	+	+	+
Machine virtuelle HC3 de Scale Computing	+	+	+	-	-	+	+	+
Machine virtuelle Red Hat Virtualization/oVirt*	+	+	+	-	-	+	+	+

* Disponible uniquement avec le déploiement dans le cloud.

Pour obtenir des directives relatives à la migration, consultez les sections suivantes :

- Physique vers virtuelle (P2V) – "Restauration d'une machine physique sur une machine virtuelle" (p. 323)
- Virtuelle vers virtuelle (V2V) – "Restauration d'une machine virtuelle" (p. 326)
- Virtuelle vers physique (V2P) – "Restauration d'une machine virtuelle" (p. 326) ou "Restaurer des disques et des volumes via un support de démarrage" (p. 329)

Même s'il est possible d'effectuer une migration V2P dans l'interface Web, nous vous recommandons d'utiliser un support de démarrage dans des cas spécifiques. Le support peut parfois être utile pour la migration sur ESXi ou Hyper-V.

Le support vous permet de :

- Exécutez la migration P2V et V2P d'une machine Linux contenant des volumes logiques (LVM). Utilisez l'agent pour Linux ou un support de démarrage pour créer la sauvegarde et le support de démarrage à restaurer.
- fournir des pilotes pour du matériel spécifique, primordial pour la capacité de démarrage du système.

Machines virtuelles Windows Azure et Amazon EC2

Pour sauvegarder une machine virtuelle Windows Azure ou Amazon EC2, installez un agent de protection sur la machine. Les opérations de sauvegarde et de restauration sont les mêmes que pour une machine physique. La machine est toutefois considérée comme une machine virtuelle lorsque vous définissez les quotas pour le nombre de machines dans un déploiement Cloud.

La différence avec une machine physique est que les machines virtuelles Windows Azure et Amazon EC2 ne peuvent pas être démarrées à partir de supports de démarrage. Si vous souhaitez effectuer une restauration vers une nouvelle machine virtuelle Windows Azure ou Amazon EC2, suivez la procédure ci-dessous.

Pour restaurer une machine en tant que machine virtuelle Windows Azure ou Amazon EC2

1. Créez une nouvelle machine virtuelle à partir d'une image/d'un modèle dans Windows Azure ou Amazon EC2. La nouvelle machine doit avoir la même configuration de disque que la machine que vous souhaitez restaurer.
2. Installez l'agent pour Windows ou l'agent pour Linux sur la nouvelle machine.
3. Restaurez la machine sauvegardée, comme décrit dans « Machine physique ». Lorsque vous configurez la restauration, sélectionnez la nouvelle machine en tant que machine cible.

Configuration réseau requise

Les agents installés sur les machines sauvegardées doivent pouvoir communiquer avec le serveur de gestion sur le réseau.

Déploiement sur site

- Si les agents et le serveur de gestion sont installés dans le Cloud Azure/EC2, toutes les machines se trouvent déjà sur le même réseau. Aucune autre action n'est requise.
- Si le serveur de gestion est situé hors du Cloud Azure/EC2, les machines situées dans le Cloud ne disposeront pas d'un accès réseau au réseau local où le serveur de gestion est installé. Pour permettre aux agents installés sur ces machines de communiquer avec le serveur de gestion, une connexion de réseau virtuel privé (VPN) entre le réseau local et le réseau sur le Cloud (Azure/EC2) doit être établie. Pour obtenir des directives relatives à la création d'une connexion VPN, consultez les articles suivants :

  Amazon EC2 : http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure : https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Déploiement Cloud

Dans un déploiement dans le Cloud, le serveur de gestion est situé dans un des centres de données Acronis, ce qui signifie que les agents peuvent y accéder. Aucune autre action n'est requise.

Protection de SAP HANA

La protection de SAP HANA est décrite dans un document distinct disponible à l'adresse https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf.

Protection contre les malwares et protection Web

La protection contre les malwares dans Cyber Protect vous offre les avantages suivants :

- Protection optimale à toutes les étapes : proactive, active et réactive.
- Quatre technologies antimalware intégrées pour vous offrir la meilleure protection à plusieurs niveaux.
- Gestion du service Microsoft Security Essentials et de l'antivirus Windows Defender.

Protection contre les virus et les malwares

Le module de protection contre les virus et les malwares vous permet de protéger vos machines Windows et macOS contre toutes les menaces de malwares récentes. Notez que la fonctionnalité Active Protection, qui fait partie de la protection contre les malwares, n'est pas prise en charge sur les machines macOS. Voir la liste complète des fonctionnalités anti-malware prises en charge : Fonctionnalités prises en charge par système d'exploitation.

Acronis Cyber Protect est pris en charge et enregistré dans le Centre de sécurité Windows.

Si votre ordinateur est déjà protégé par un antivirus tiers au moment de l'application du module de protection contre les virus et les malwares sur l'ordinateur, le système générera une alerte et arrêtera la protection en temps réel afin d'éviter d'éventuels problèmes de compatibilité ou de performances. Vous aurez besoin de désactiver ou de désinstaller la solution antivirus tierce pour permettre à la protection antivirus et antimalware Acronis Cyber Protect d'être parfaitement fonctionnelle.

Les capacités anti-malware suivantes sont à votre disposition :

- Détection des malware dans les fichiers en mode temps réel et à la demande (pour Windows et macOS)
- Détection des comportements malveillants dans les processus (Windows)
- Blocage de l'accès aux URL malveillantes (Windows)
- Placement de fichiers dangereux en quarantaine
- Ajout des applications d'entreprise de confiance à la liste blanche

Le module de protection contre les virus et les malwares vous offre deux types d'analyse :

- Analyse de protection en temps réel
- Analyse des malwares à la demande

Analyse de protection en temps réel

La protection en temps réel vérifie tous les fichiers ouverts ou en cours d'exécution sur une machine afin de prévenir les menaces de malwares.

Vous pouvez choisir parmi les types d'analyse suivants :

- La détection lors de l'accès signifie que le programme anti-malware s'exécute en arrière-plan et analyse le système de votre machine de manière active et constante, à la recherche de virus et d'autres menaces malveillantes, pendant tout le temps où votre système est allumé. 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 le lire/le modifier.
- 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 des malwares à la demande

L'analyse anti-malware est réalisée de façon planifiée.

Vous pouvez suivre les résultats de l'analyse anti-malware dans le widget **Tableau de bord** > **Présentation** > Affectés récemment.

Paramètres de protection contre les virus et les malwares

Pour apprendre à créer un plan de protection avec le module de protection contre les virus et les malwares, reportez-vous à la section « Création d'un plan de protection ».

Vous pouvez définir les paramètres suivants pour le module de protection contre les virus et les malwares.

Active Protection

Active Protection protège un système des ransomware et des malware d'extraction de cryptomonnaie. Un ransomware chiffre les fichiers et exige une rançon en échange de la clé de chiffrement. Un malware de cryptomining effectue des calculs mathématiques en arrière-plan et monopolise ainsi la puissance de traitement ainsi que le trafic réseau.

Dans les éditions Cyber Backup de Acronis Cyber Protect, Active Protection est un module distinct du plan de protection. Par conséquent, il peut être configuré différemment et appliqué à différents périphériques ou groupes de périphériques. Dans les éditions Protect de Acronis Cyber Protect, Active Protection fait partie du module de protection contre les virus et les malwares.

Active Protection est disponible pour les ordinateurs exécutant les systèmes d'exploitation suivants :

- Systèmes d'exploitation de bureau : Windows 7 Service Pack 1 et versions ultérieures
  Sur les machines fonctionnant sous Windows 7, assurez-vous que la Mise à jour pour Windows 7 (KB2533623) est installée.
- Systèmes d'exploitation serveurs : Windows Server 2008 R2 et versions ultérieures.

L'agent pour Windows doit être installé sur la machine.

Fonctionnement

Active Protection surveille les processus en cours d'exécution sur la machine protégée. Lorsqu'un processus tiers essaye de chiffrer des fichiers ou d'extraire de la cryptomonnaie, Active Protection génère une alerte et exécute des actions supplémentaires, si ces dernières sont précisées par la configuration.

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.

Paramètre par défaut : **Activé**.

Paramètres d'Active Protection

Dans **Action lors de la détection**, sélectionnez l'action que le logiciel exécutera lors de la détection d'une activité de ransomware, puis cliquez sur **Terminé**.

Vous pouvez sélectionner l'une des options suivantes :

- **Notifier uniquement**
  Le logiciel générera une alerte au sujet du processus.
- **Arrêter le processus**
  Le logiciel générera une alerte et arrêtera le processus.
- **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**.

Protection du dossier réseau

L'option **Protéger vos dossiers réseau mappés en tant que lecteurs locaux** définit si la protection contre les virus et les malwares protège les dossiers réseau qui sont mappés en tant que lecteurs locaux contre les processus malveillants locaux.

Cette option 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 les paramètres de cette option. Le dossier par défaut est le suivant : **C:\ProgramData\Acronis\Restored Network Files**. 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 option définit si la protection contre les virus et les malwares protège les dossiers réseau que vous partagez des connexions entrantes extérieures en provenance d'autres serveurs du réseau, qui pourraient potentiellement amener des menaces.

Paramètre par défaut : **Désactivé**.

Définir des connexions fiables et bloquées

Dans l'onglet **Fiable**, vous pouvez spécifier les connexions autorisées à modifier des données. Vous devez définir le nom d'utilisateur et l'adresse IP.

Dans l'onglet **Bloqué**, vous pouvez spécifier les connexions qui ne sont pas autorisées à modifier des données. Vous devez définir le nom d'utilisateur et l'adresse IP.

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, Secure Zone, ainsi que des sauvegardes contenues dans les dossiers locaux. Nous ne recommandons pas la désactivation de cette fonctionnalité.

Paramètre par défaut : **Activé**.

Autoriser les processus à modifier des sauvegardes

L'option **Autoriser des processus particuliers à modifier des sauvegardes** prend effet lorsque l'option **Autoprotection** est activée.

Elle s'applique aux fichiers qui disposent d'une extension .tibx, .tib ou .tia et qui sont situés dans des dossiers locaux.

Cette option vous permet de préciser les processus qui sont autorisés à modifier les fichiers de sauvegarde, même si ces fichiers sont protégés par l'autoprotection. Elle est très utile, par exemple, si vous supprimez des fichiers de sauvegarde ou les déplacez vers un emplacement différent à l'aide d'un script.

Si cette option est désactivée, 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 cette option est activée, vous pouvez autoriser d'autres processus à modifier les sauvegardes. Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur.

Paramètre par défaut : **Désactivé**.

Détection d'un processus de cryptominage

Cette option définit si la protection contre les virus et les malwares détecte les malwares de cryptomining potentiels.

Un malware de cryptomining réduit la performance des applications utiles, accroît la facture d'électricité, peut causer des plantages système et même endommager le matériel à cause d'un usage abusif. Nous vous recommandons d'ajouter les malwares de cryptominage à la liste des processus **nuisibles** pour les empêcher de s'exécuter.

Paramètre par défaut : **Activé**.

Paramètres de détection d'un processus de cryptominage

Sélectionnez l'action que le logiciel exécutera lors de la détection d'une activité de cryptominage, puis cliquez sur **Terminé**. Vous pouvez sélectionner l'une des options suivantes :

- **Notifier uniquement**
  Le logiciel génère une alerte au sujet du processus suspecté d'activité de cryptominage.
- **Arrêter le processus**
  Le logiciel génère une alerte et arrête le processus suspecté d'activité de cryptominage.

Paramètre par défaut : **Arrêter le processus**.

Quarantaine

La zone de quarantaine est un dossier destiné à isoler les fichiers suspects (probablement infectés) ou potentiellement dangereux.

Supprimer les fichiers mis en quarantaine après : définit la période, en jours, après laquelle les fichiers en quarantaine seront supprimés.

Paramètre par défaut : **30 jours**.

Détection des comportements

Acronis Cyber Protect protège votre système au moyen d'heuristiques comportementales lui permettant d'identifier les processus malveillants : le logiciel 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. Par conséquent, un nouveau malware est détecté grâce à son comportement typique.

Paramètre par défaut : **Activé**.

Paramètres de détection des comportements

Dans **Action lors de la détection**, sélectionnez l'action que le logiciel exécutera lors de la détection d'une activité de malware, puis cliquez sur **Terminé**.

Vous pouvez sélectionner l'une des options suivantes :

- **Notifier uniquement**
  Le logiciel générera une alerte au sujet du processus suspecté d'activité de malware.
- **Arrêter le processus**
  Le logiciel générera une alerte et arrêtera le processus suspecté d'activité de malware.
- **Quarantaine**
  Le système générera une alerte, arrêtera le processus et placera l'élément exécutable dans le dossier de quarantaine.

Paramètre par défaut : **Quarantaine**.

Protection en temps réel

La **protection en temps réel** recherche constamment des virus et autres menaces dans votre système informatique pendant tout le temps où votre système est allumé.

Paramètre par défaut : **Activé**.

Configurer l'action lors de la détection pour une protection en temps réel

Dans **Action lors de la détection**, sélectionnez l'action que le logiciel exécutera lors de la détection d'un virus ou d'une activité de malware, puis cliquez sur **Terminé**.

Vous pouvez sélectionner l'une des options suivantes :

- **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.

Paramètre par défaut : **Quarantaine**.

Configurer le mode d'analyse pour une protection en temps réel

En **mode d'analyse**, sélectionnez l'action que le logiciel exécutera lors de la détection d'une activité de malware, puis cliquez sur **Terminé**.

Vous pouvez sélectionner l'une des options suivantes :

- **Mode sur accès intelligent :** surveille toutes les activités du système et analyse automatiquement les fichiers lorsque quelqu'un y accède pour lecture ou écriture, ou chaque fois qu'un programme est lancé.
- **Lors de l'exécution :** analyse automatiquement 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.

Paramètre par défaut : **Mode sur accès intelligent**.

Planifier l'analyse

Vous pouvez définir une planification selon laquelle votre machine sera analysée à la recherche de malwares, en activant le paramètre **Planifier l'analyse**.

Action lors de la détection :

- **Quarantaine**
  Le logiciel génère une alerte et place le fichier exécutable dans le dossier de quarantaine.
- **Notifier uniquement**
  Le logiciel génère une alerte au sujet du processus suspecté d'être un malware.

Paramètre par défaut : **Quarantaine**.

Type d'analyse :

- **Complète**
  L'analyse complète est bien plus longue que l'analyse rapide, car chaque fichier est vérifié.
- **Rapide**
  L'analyse rapide analyse uniquement les emplacements courants où se trouvent habituellement les malwares sur la machine.
- **Personnalisée**
  L'analyse personnalisée analyse les fichiers/dossiers sélectionnés par l'administrateur et ajoutés au plan de protection.

Vous pouvez planifier les trois analyses **rapide**, **complète** et **personnalisée** dans un seul plan de protection.

Paramètres par défaut :

- Des analyses **rapides** et **complètes** sont planifiées.
- L'analyse **personnalisée** est désactivée par défaut.

Planifiez l'exécution de la tâche à l'aide des événements suivants :

- **Planifier selon l'horaire :** 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.
- **Lorsque l'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.

Paramètre par défaut : **Planifier selon l'horaire**.

Type de planification :

- **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée.
- **Quotidienne :** sélectionnez les jours de la semaine pendant lesquels la tâche sera exécutée.
- **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.

Paramètre par défaut : **Quotidien**.

Démarrage à : sélectionnez l'heure exacte à laquelle la tâche sera exécutée.

Exécuter sur une plage de date : configurez une plage pendant laquelle le programme configuré sera effectif.

Conditions de démarrage : définissez toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée.

Les conditions de démarrage pour les analyses anti-malwares sont similaires aux conditions de démarrage du module Sauvegarde, décrites dans "Conditions de démarrage" (p. 247). 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.

Analyser uniquement les fichiers nouveaux ou modifiés : seuls les fichiers nouveaux ou modifiés seront analysés.

Paramètre par défaut : **Activé**.

Lors de la planification d'une **Analyse complète**, vous avez deux options supplémentaires :

- **Analyser les fichiers d'archive**
  Paramètre par défaut : **Activé**.
  - **Profondeur de réapparition maximum**
    Le nombre de niveaux d'archive incorporées qui peuvent être analysés. Par exemple, Document MIME > archive ZIP > archive Office > contenu du document.
    Paramètre par défaut : **16**.
  - **Taille maximale**
    Taille maximale d'un fichier d'archive à analyser.
    Paramètre par défaut : **Illimitée**.
- **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**

Exclusions

Pour minimiser les ressources utilisées par l'analyse heuristique et éliminer les faux positifs lorsqu'un programme de confiance est considéré comme un ransomware, vous pouvez définir les paramètres suivants :

Dans l'onglet **Fiable**, vous pouvez spécifier les éléments suivants :

- Les processus à ne jamais considérer comme malwares. Les processus signés par Microsoft sont toujours fiables.
- Les dossiers dans lesquels les modifications des fichiers ne seront pas surveillées.
- Les fichiers et les dossiers pour lesquels l'analyse planifiée ne sera pas exécutée.

Dans l'onglet **Bloqué**, vous pouvez spécifier les éléments suivants :

- Les processus qui seront toujours bloqués. Ces processus ne pourront pas démarrer tant qu'Active Protection sera activé sur la machine.
- Les dossiers dans lesquels n'importe quel processus sera bloqué.

Spécifiez le chemin d'accès complet au processus exécutable, en commençant par la lettre du lecteur. Par exemple : `C:\Windows\Temp\er76s7sdkh.exe`.

Pour spécifier des dossiers, vous pouvez utiliser les caractères génériques * et ?. L'astérisque (*) remplace zéro ou plusieurs caractères. Le point d'interrogation (?) remplace exactement un seul caractère. Il n'est pas possible d'utiliser des variables d'environnement telles que `%AppData%`.

Paramètre par défaut : Aucune exclusion n'est définie par défaut.

Filtrage d'URL

Pour obtenir une description détaillées, consultez la rubrique Filtrage des URL.

Active Protection

Dans les éditions Cyber Backup de Acronis Cyber Protect, Active Protection est un module distinct du plan de protection. Ce module dispose des paramètres suivants :

- Action sur la détection
- Autoprotection
- Protection du dossier réseau
- Protection côté serveur
- Détection d'un processus de cryptominage
- Exclusions

Dans les éditions Protect de Acronis Cyber Protect, Active Protection fait partie du module de protection contre les virus et les malwares.

Active Protection est disponible pour les ordinateurs exécutant les systèmes d'exploitation suivants :

- Systèmes d'exploitation de bureau : Windows 7 Service Pack 1 et versions ultérieures
  Sur les machines fonctionnant sous Windows 7, assurez-vous que la Mise à jour pour Windows 7 (KB2533623) est installée.
- Systèmes d'exploitation serveurs : Windows Server 2008 R2 et versions ultérieures.

L'agent pour Windows doit être installé sur la machine.

Pour en savoir plus sur Active Protection et ses paramètres, consultez la section "Paramètres de protection contre les virus et les malwares" (p. 527).

Antivirus Windows Defender

L'antivirus Windows Defender est un composant anti-malwareintégré àMicrosoft Windows, qui est fourni à partir de Windows 8.

Le module Antivirus de Windows Defender vous permet de configurer les règles de sécurité de l'antivirus Windows Defender et de suivre son état par l'intermédiaire de la console Web Cyber Protect.

Ce module s'applique à toutes les machines sur lesquelles l'antivirus Windows Defender est installé.

Planifier l'analyse

Spécifiez la planification pour l'analyse planifiée.

Mode d'analyse :

- **Complète :** vérification complète de tous les fichiers et dossiers, outre les éléments analysés lors de l'analyse rapide. Elle requiert plus de ressources machine comparativement à l'analyse rapide.
- **Rapide :** une vérification rapide des processus et dossiers en mémoire, dans lesquels se trouvent généralement les malwares. Elle 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 :

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 plus d'informations sur les paramètres de planification de l'antivirus Windows 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 machine.
- **Quarantaine :** placer le malware détecté en quarantaine, mais ne pas le supprimer.
- **Supprimer ;** supprimer le malware détecté d'une machine.
- **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 plus d'informations sur les paramètres des actions par défaut de l'antivirus Windows 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 machines.

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.

Pour plus d'informations sur les paramètres de protection en temps réel de l'antivirus Windows 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 dans l'analyse les fichiers archivés tels que les fichiers .zip ou .rar.
- **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'interface 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 Web 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 plus d'informations sur les paramètres avancés de l'antivirus Windows Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

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 plus d'informations sur les paramètres d'exclusion de l'antivirus Windows Defender, reportez-vous à l'article https://docs.microsoft.com/fr-fr/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

Microsoft Security Essentials

Microsoft Security Essentials est un composantanti-malwareintégré àMicrosoft Windows, qui est fourni avec les versions antérieures à Windows 8.

Le module Microsoft Security Essentials vous permet de configurer les règles de sécurité de Microsoft Security Essentials et de suivre son état via la console Web Cyber Protect.

Ce module s'applique à tous les ordinateurs sur lesquels Microsoft Security Essentials est installé.

Les paramètres de Microsoft Security Essentials sont globalement identiques à ceux de l'antivirus Microsoft Windows Defender, à l'exception du fait qu'il n'existe aucun paramètre de protection en temps réel et qu'il est impossible de définir des exclusions via la console Web Cyber Protect.

Filtrage d'URL

Les malwares sont souvent distribués par des sites malveillants ou infectés et font appel à une méthode d'infection appelée « téléchargement furtif ». La fonctionnalité de filtrage d'URL vous permet de protéger vos ordinateurs des menaces Internet telles que les malwares ou le hameçonnage. Vous pouvez bloquer l'accès aux sites Web dont le contenu peut être malveillant.

La fonctionnalité de filtrage d'URL vous permet aussi de contrôler l'utilisation d'Internet afin de respecter les réglementations externes ou les règles internes de l'entreprise. Vous pouvez configurer différentes règles d'accès pour plus de 40 catégories de site Web.

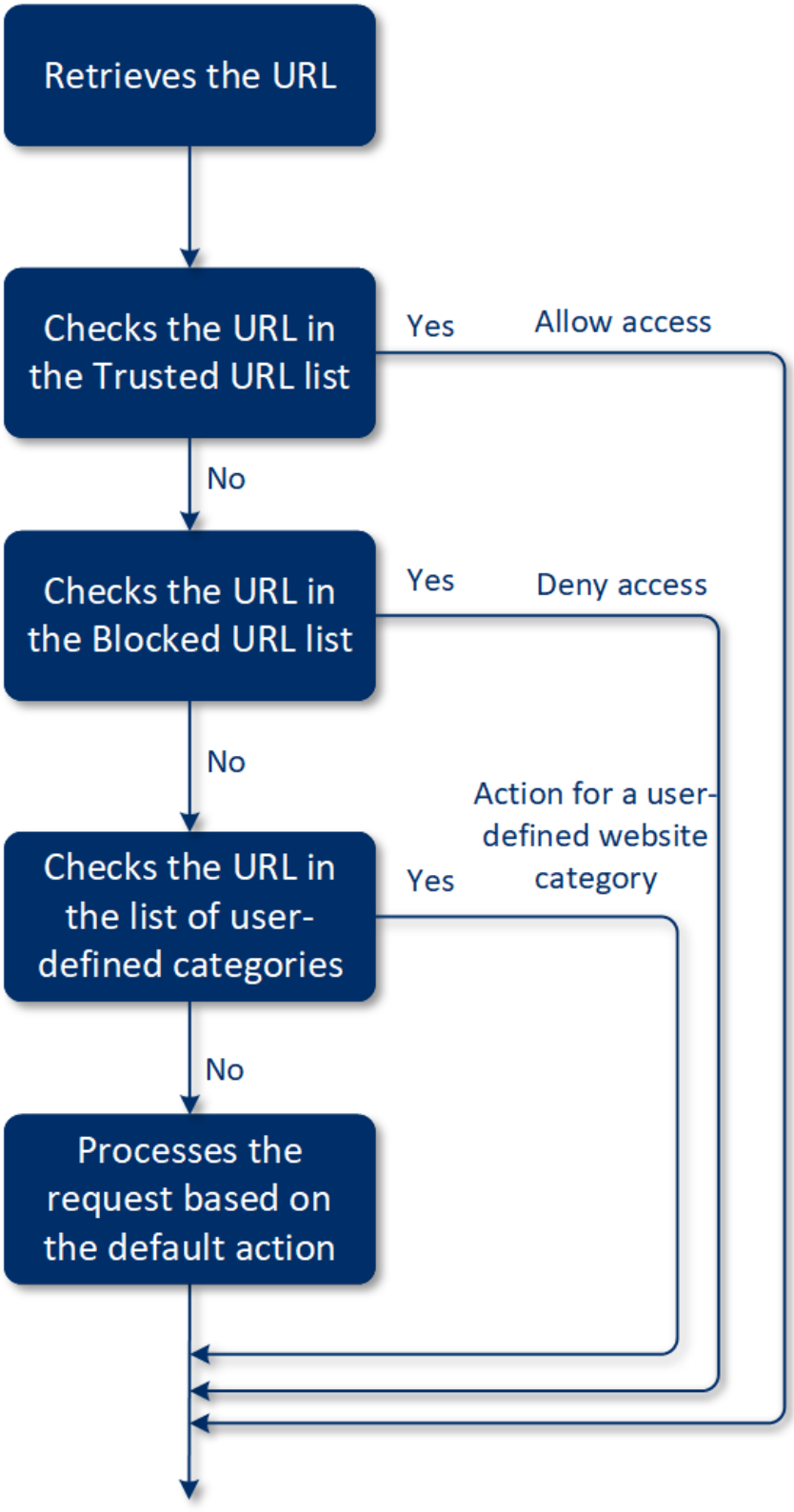
Pour le moment, les connexions HTTP et HTTPS sur les ordinateurs Windows sont vérifiées par l'agent de protection.

La fonctionnalité de filtrage des URL nécessite une connexion Internet.

Remarque
Des conflits peuvent se produire si le filtrage d'URL est utilisé en parallèle de solutions antivirus tierces qui possèdent également des fonctionnalités de filtrage d'URL. Vous pouvez déterminer l'état des autres solutions antivirus installées via le centre de sécurité Windows.
Si un problème de compatibilité ou de performances se produit, désinstallez la solution tierce ou désactivez le module de filtrage d'URL dans vos plans de protection.

Fonctionnement

Un utilisateur suit un lien ou saisit une URL dans la barre d'adresse d'un navigateur. L'intercepteur récupère l'URL et l'envoie à l'agent de protection. L'agent de protection analyse l'URL, vérifie la base de données, puis renvoie un verdict à l'intercepteur. Si l'URL est interdite, l'intercepteur bloque son accès et informe l'utilisateur qu'il n'est pas autorisé à voir ce contenu.



Pour configurer le filtrage d'URL

1. Créez un plan de protection avec le module de filtrage d'URL activé.
2. Configurez les paramètres de filtrage d'URL (voir ci-dessous).

3. Attribuez le plan de protection aux ordinateurs souhaités.

Pour consulter les URL qui ont été bloquées, accédez à **Tableau de bord** > **Alertes**.

Paramètres du filtrage d'URL

Vous pouvez configurer les paramètres suivants pour le module de filtrage d'URL.

Accès à un site Web malveillant

Spécifiez l'action à exécuter lorsqu'un utilisateur essaie d'ouvrir un site Web malveillant :

- **Bloquer** : l'accès au site Web malveillant est bloqué et une alerte est générée.
- **Toujours demander à l'utilisateur** : l'utilisateur reçoit un message lui demandant de choisir s'il souhaite accéder au site Web ou revenir à la page précédente.

Catégories à filtrer

Il existe 44 catégories de sites Web pour lesquelles vous pouvez configurer des règles d'accès. Par défaut, l'accès aux sites Web de toutes les catégories est autorisé.

	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 catégorieDrogues.
7	**Éducation**	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 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 catégorieJeux 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 catégorieActivités illégales) • Les jeux qui nécessitent qu'un utilisateur télécharge et exécute un fichier exécutable, comme World ofWarcraft ; 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 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 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. Il est recommandé 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.
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.
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 demandes vers le serveur Web de destination se font depuis le serveur de proxy Web, seule son adresse IP est visible, et si les administrateurs du serveur identifient l'utilisateur, la trace s'arrêtera au niveau du proxy Web, ce qui peut ou non conserver les journaux nécessaires pour localiser l'utilisateur d'origine. • Pour l'usurpation de l'emplacement. Les adresses IP des utilisateurs sont souvent utilisées pour établir le profil du service par emplacement de la source (il se peut que certains sites Web gouvernementaux nationaux soient disponibles uniquement depuis des adresses IP locales), et il se peut que l'utilisation de ces services aide l'utilisateur à masquer 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.

Si vous cochez la case **Afficher toutes les notifications pour les URL bloquées par catégorie**, les notifications concernant les URL bloquées par catégorie s'affichent dans la zone de notification. Si un site Web possède plusieurs sous-domaines, les notifications sont également générées pour ces sous-domaines, ce qui peut augmenter considérablement le nombre de notifications.

Exclusions

Les URL considérées comme fiables peuvent être ajoutées à la liste des URL de confiance. Les URL considérées comme une menace peuvent être ajoutées à la liste des URL bloquées.

Pour ajouter une URL à une liste

1. Dans le module de filtrage d'URL d'un plan de protection, cliquez sur **Exclusions**.
2. Sélectionnez la liste souhaitée : **Fiable** ou **Bloqué**.
3. Cliquez sur **Ajouter**.
4. Indiquez l'URL ou l'adresse IP, puis cochez la case.

Exemples d'exclusions d'URL :

- Si vous ajoutez xyz.com comme étant une adresse fiable/non fiable, toutes les adresses du domaine xyz.com seront traitées comme étant fiables ou non fiables, selon l'endroit où vous les ajoutez.
- Si vous souhaitez ajouter un sous-domaine spécifique, vous pouvez ajouter l'adresse **mail.xyz.com** comme étant fiable/non fiable. De cette manière, toutes les adresses **xyz.com** ne seront pas considérées comme étant fiables ou non fiables.
- Si vous souhaitez ajouter l'adresse IPv4 comme étant fiable/non fiable, vous devez utiliser le format suivant : **20.53.203.50**.
- Si vous souhaitez ajouter plusieurs exclusions d'URL simultanément, veillez à ajouter chaque entrée sur une nouvelle ligne :

  acronis.com

  mail.xyz.com

  20.53.203.50

Quarantaine

La zone de **quarantaine** est un dossier isolé spécial, présent sur le disque dur d'une machine, dans lequel sont placés les fichiers suspects détectés par la protection contre les virus et les malwares afin d'éviter de propager davantage les menaces.

La zone de quarantaine vous permet de consulter les fichiers suspects et potentiellement dangereux présents sur toutes les machines, et de décider s'ils doivent être supprimés ou restaurés. Les fichiers en quarantaine sont automatiquement supprimés si la machine est supprimée du système.

Comment les fichiers arrivent-ils dans le dossier de quarantaine ?

1. Vous configurez le plan de protection et indiquez que par défaut, les fichiers infectés doivent être mis en quarantaine.
2. Lors d'une analyse lors de l'accès ou lors d'une analyse planifiée, le système détecte des fichiers malveillants et les place dans le dossier sécurisé Quarantaine.
3. Le système met à jour la liste de quarantaine sur les machines.
4. Les fichiers sont automatiquement nettoyés du dossier de quarantaine après la période définie pour le paramètre **Supprimer les fichiers mis en quarantaine après** dans le plan de protection.

Gestion des fichiers mis en quarantaine

Pour gérer les fichiers mis en quarantaine, accédez à **Protection contre les malwares** > **Quarantaine**. Vous verrez la liste des fichiers mis en quarantaine sur toutes les machines.

Nom	Description
Fichier	Le nom du fichier.
Date de début de la mise en quarantaine	La date et l'heure auxquelles le fichier a été mis en quarantaine.
Périphérique	Le périphérique 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 mis en quarantaine.

Pour les fichiers mis en quarantaine, deux actions sont possibles :

- **Supprimer :** supprimer définitivement un fichier mis en quarantaine de toutes les machines.
- **Restaurer :** restaurer un fichier mis en quarantaine à son emplacement d'origine, sans aucune modification. Si un fichier avec le même nom existe dans l'emplacement d'origine, il sera écrasé par le fichier restauré.

Emplacement de quarantaine sur les machines

L'emplacement par défaut pour les fichiers mis en quarantaine est le suivant :

Pour une machine Windows : `%ProgramData%\%product_name%\Quarantine`

Pour une machine Mac/Linux : `/usr/local/share/%product_name%/quarantine`

Liste blanche d'entreprise

Important
La liste blanche d'entreprise nécessite que le service d'analyse soit installé sur le serveur de gestion.

Une solution antivirus pourrait identifier des applications légitimes spécifiques à une entreprise comment étant suspectes. Afin d'éviter les faux positifs, les applications de confiance sont ajoutées manuellement à une liste blanche, ce qui est chronophage.

Cyber Protect peut automatiser ce processus : les sauvegardes sont analysées par le module de protection contre les virus et les malwares, et les données analysées sont examinées pour placer ces applications sur la liste blanche, et les détections de faux positifs sont évitées. La liste blanche à l'échelle de l'entreprise améliore également les performances d'analyse ultérieures.

La liste blanche peut être activée et désactivée. Lorsqu'elle est désactivée, les fichiers qui y sont ajoutés sont temporairement masqués.

Ajout automatique à la liste blanche

1. Exécutez l'analyse Cloud des sauvegardes sur au moins deux ordinateurs. Pour cela, utilisez "Plan d'analyse de la sauvegarde" (p. 360).
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 Web Cyber Protect, accédez à **Protection contre les malwares** > **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 Web Cyber Protect, accédez à **Protection contre les malwares** > **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 au terme d'un délai long et après un nombre important de vérifications. Ces applications sont plus fiables. Toutefois, cette approche augmente la possibilité de faux positifs. Les critères pour considérer qu'un fichier est propre et fiable sont stricts.
- **Par défaut**

  Les applications d'entreprise seront ajoutées à la liste blanche en fonction du niveau de protection recommandé, afin de réduire la possibilité de faux positifs. Les critères pour considérer qu'un fichier est propre et fiable sont moyens.
- **Élevée**

  Les applications d'entreprise seront ajoutées à la liste blanche plus rapidement, afin de réduire la possibilité de faux positifs. Toutefois, cela ne garantit pas que le logiciel soit propre et il peut, par la suite, être identifié comme suspect ou malware. Les critères pour considérer qu'un fichier est 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 anti-malware des sauvegardes

Pour prévenir la restauration de fichiers infectés à partir de sauvegardes, vous pouvez analyser les sauvegardes à la recherche de malwares. L'analyse des sauvegardes n'est prise en charge que pour les systèmes d'exploitation Windows. Cette fonctionnalité est uniquement disponible si le service d'analyse est installé sur le serveur de gestion Cyber Protect.

Pour analyser des sauvegardes à la recherche de malwares, créez un plan d'analyse de sauvegarde.

Remarque
Pour des raisons de sécurité et de performances, nous vous recommandons d'utiliser un ordinateur dédié aux analyses. Cette machine aura accès à toutes les sauvegardes qui sont analysées.

Vous pouvez consulter les résultats de l'analyse dans le widget « Détails de l'analyse de la sauvegarde » sur le tableau de bord. Vous pouvez également consulter l'état d'une sauvegarde dans **Stockage de sauvegarde** > **Emplacements** > **<nom de la sauvegarde>**. Si une analyse de sauvegarde n'a pas été réalisée, les sauvegardes restent à l'état **Non analysé**. Une fois une analyse de sauvegarde réalisée, l'état des sauvegardes change et l'un des états suivants s'affiche :

- **Aucun malware**
- **Malware détecté**

Limites

- Seules les sauvegardes de type **Toute la machine** ou **Disques/volumes** peuvent être analysées à la recherche de malwares.
- Seuls les volumes avec système de fichiers NTFS et partitionnement GPT et MBR seront analysés.
- Les emplacements de sauvegarde pris en charge sont les suivants : **Stockage dans le Cloud**, **dossier local** et **dossier réseau**.

- Les sauvegardes disposant de points de récupération CDP (Protection continue des données) peuvent être sélectionnées pour analyse, mais ces points de récupération seront exclus de l'analyse. Seuls les points de récupération normaux seront analysés.
- Lorsqu'une sauvegarde CDP est sélectionnée pour la restauration sûre d'une machine complète, la machine sera restaurée sans les données du point de récupération CDP. Pour restaurer les données CDP, exécutez une restauration de **Fichiers/dossiers**.

Protection des applications de collaboration et de communication

Zoom, Cisco Webex Meetings et Microsoft Teams sont désormais largement utilisés pour les communications et conférences Web et vidéo. Cyber Protect vous permet de protéger vos outils de collaboration.

La configuration de la protection pour Zoom, Cisco Webex Meetings et Microsoft Teams est similaire. Dans l'exemple ci-dessous, nous évoquerons la configuration de Zoom.

Pour configurer la protection pour Zoom

1. Installez un agent de protection sur la machine sur laquelle l'application de collaboration est installée.
2. Connectez-vous à la console Web 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

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. En utilisant le module d'évaluation des vulnérabilités dans un plan de protection, vous pouvez analyser vos ordinateurs à la recherche de vulnérabilités, et vérifier que 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 ordinateurs exécutant les systèmes d'exploitation suivants :

- Windows. Pour plus d'informations, voir "Produits Microsoft et tiers pris en charge" (p. 555).
- Ordinateurs Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastucture). Pour plus d'informations, voir "Produits Linux pris en charge" (p. 556).

Utilisez la fonctionnalité de **gestion des correctifs** pour gérer les correctifs (mises à jour) des applications et systèmes d'exploitation installés sur vos machines, et garder vos systèmes à jour. Dans le module de gestion des correctifs, vous pouvez approuver automatiquement ou manuellement l'installation de mises à jour sur vos ordinateurs.

La gestion des correctifs est prise en charge pour les ordinateurs exécutant Windows. Pour plus d'informations, voir "Produits Microsoft et tiers pris en charge" (p. 555).

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 ordinateurs.
2. Le système, de façon planifiée ou à la demande, envoie une commande aux agents de protection afin qu'ils exécutent l'analyse d'évaluation des vulnérabilités.
3. Les agents reçoivent la commande, commencent à analyser les ordinateurs 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, ainsi qu'une liste des vulnérabilités trouvées.
6. En utilisant ces informations, vous pouvez décider des vulnérabilités trouvées à corriger.

Vous pouvez suivre les résultats de l'analyse d'évaluation des vulnérabilités dans les widgets **Tableau de bord** > **Présentation** > **Vulnérabilités/Vulnérabilités existantes**.

Produits Microsoft et tiers pris en charge

Les produits Microsoft et tiers suivants pour les systèmes d'exploitation Windows sont pris en charge pour l'évaluation des vulnérabilités :

Produits Microsoft pris en charge

Systèmes d'exploitation de bureau

- Windows 7 (Entreprise, Professionnel, Intégrale)
- Windows 8
- Windows 8.1
- Windows 10

Systèmes d'exploitation des serveurs

- 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 2008 R2
- Microsoft SQL Server 2012

- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Produits tiers pris en charge pour Windows

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.

Pour obtenir la liste complète des produits tiers pris en charge pour Windows, reportez-vous à l'article https://kb.acronis.com/content/62853.

Produits Linux pris en charge

Les distributions Linux suivantes sont prises en charge pour l'évaluation des vulnérabilités :

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Stockage 2.4.0
- Acronis Stockage 2.2.0

Paramètres d'évaluation des vulnérabilités

Pour apprendre à créer un plan de protection avec le module d'évaluation des vulnérabilités, reportez-vous à la section "Création d'un plan de protection" (p. 208). Vous pouvez effectuer une analyse d'évaluation des vulnérabilités de façon planifiée ou à la demande (à l'aide de l'action **Exécuter maintenant** d'un plan de protection).

Vous pouvez spécifier les paramètres suivants dans le module d'évaluation des vulnérabilités.

Éléments à analyser

Définir les produits logiciels que vous souhaitez analyser à la recherche de vulnérabilités :

- Ordinateurs Windows :
  - **Produits Microsoft**
  - **Produits Windows tiers**
    Pour plus d'informations sur les produits tiers pris en charge pour Windows, reportez-vous à l'article https://kb.acronis.com/content/62853.
- Ordinateurs Linux :
  - **Analyser les packages Linux**

Planification

Définissez le planning selon lequel l'analyse d'évaluation des vulnérabilités sera effectuée sur les machines sélectionnées :

Planifiez l'exécution de la tâche à l'aide des événements suivants :

- **Planifier selon l'horaire :** 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.
- **Lorsque l'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.

Paramètre par défaut : **Planifier selon l'horaire**.

Type de planification :

- **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée.
- **Quotidienne :** sélectionnez les jours de la semaine pendant lesquels la tâche sera exécutée.
- **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.

Paramètre par défaut : **Quotidien**.

Démarrage à : sélectionnez l'heure exacte à laquelle la tâche sera exécutée.

Exécuter sur une plage de date : configurez une plage pendant laquelle le programme configuré sera effectif.

Conditions de démarrage : définissez toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée.

Les conditions de démarrage pour les analyses anti-malwares sont similaires aux conditions de démarrage du module Sauvegarde, décrites dans "Conditions de démarrage" (p. 247). 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.

Évaluation des vulnérabilités pour les machines Windows

Vous pouvez analyser les ordinateurs Windows et les produits tiers pour Windows à la recherche de vulnérabilités.

1. Dans la console Web 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 Microsoft**, les **produits Windows tiers**, ou les deux.
   - **Planification :** définir le calendrier de réalisation de l'évaluation des vulnérabilités.
     Pour en savoir plus sur les options de **Planification**, reportez-vous à "Paramètres d'évaluation des vulnérabilités" (p. 556).
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 suivre les résultats de l'évaluation des vulnérabilités, consultez les widgets **Tableau de bord** > **Présentation** > **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 Web 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**, reportez-vous à "Paramètres d'évaluation des vulnérabilités" (p. 556).
3. Appliquez le plan aux machines Linux.

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 suivre les résultats de l'évaluation des vulnérabilités, consultez les widgets **Tableau de bord** > **Présentation** > **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 pour lesquelles des correctifs sont disponibles et celles pour lesquelles aucun correctif n'a été suggéré. Vous pouvez vous servir du filtre pour afficher uniquement les vulnérabilités pour lesquelles un correctif est disponible.

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 attribués, d'après le système d'évaluation des vulnérabilités (CVSS) : • **Critique :** 9 à 10 CVSS • **Élevé :** 7 à 9 CVSS • **Moyen :** 3 à 7 CVSS

	• **Faible :** 0 à 3 CVSS • **Aucun**
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 d'une vulnérabilité trouvée en cliquant sur son nom dans la liste.

Démarrer le processus de réparation des vulnérabilités

1. Dans la console Web Cyber Protect, accédez à **Gestion de logiciel** > **Vulnérabilités**.
2. Sélectionnez les vulnérabilités dans la liste, puis cliquez sur **Installer les correctifs**. L'assistant de réparation des vulnérabilités apparaît.
3. Sélectionnez les correctifs à installer. Cliquez sur **Suivant**.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez installer des correctifs.
5. Choisissez si vous souhaitez redémarrer l'ordinateur après l'installation d'un correctif :
   - **Non :** l'ordinateur ne sera jamais redémarré après l'installation de correctifs.
   - **Si nécessaire :** l'ordinateur sera redémarré uniquement si cela est nécessaire à l'application des mises à jour.
   - **Oui :** l'ordinateur sera toujours redémarré après l'installation de correctifs. Toutefois, vous pouvez spécifier un délai.

   Ne redémarrez pas avant la fin de la sauvegarde : si un processus de sauvegarde est en cours d'exécution, le redémarrage de l'ordinateur sera retardé jusqu'à la fin de la sauvegarde.
6. Cliquez sur **Installer les correctifs**.

Les correctifs choisis sont alors installés sur les machines sélectionnées.

Gestion des correctifs

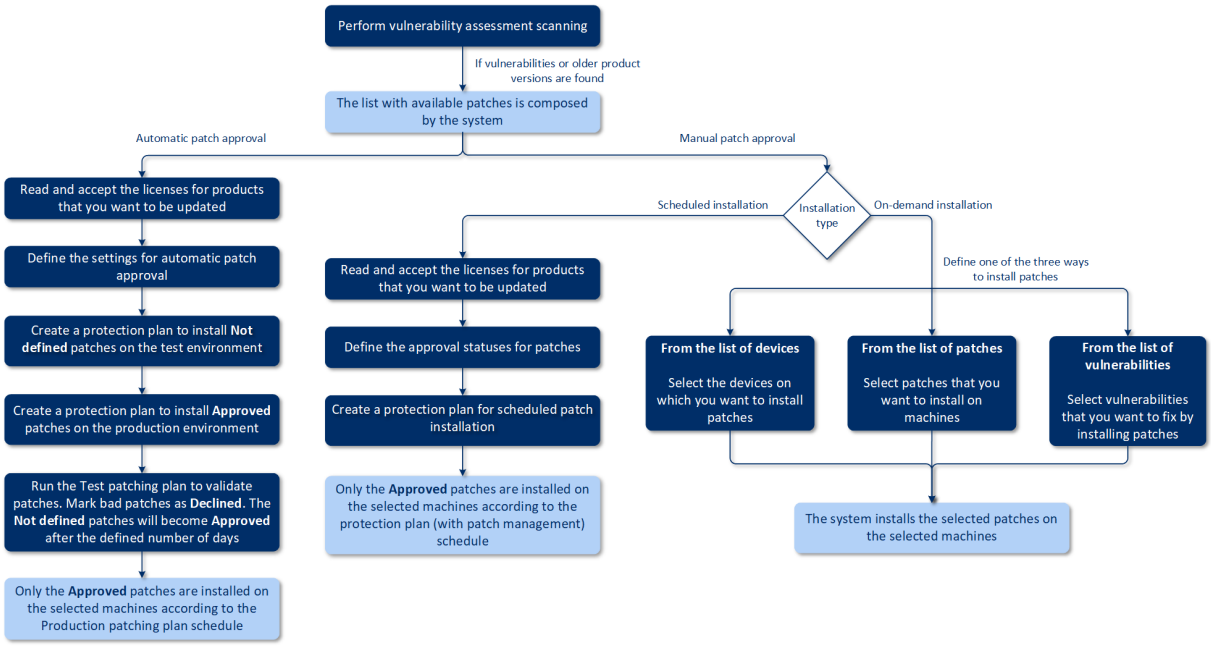
Servez-vous de la fonctionnalité de gestion des correctifs pour effectuer les tâches suivantes :

- Installer les mises à jour du système d'exploitation ou des applications
- Approuver manuellement ou automatiquement les correctifs
- Installer des correctifs à la demande ou de façon planifiée
- Définir précisément quels correctifs appliquer selon différents critères : gravité, catégorie et statut d'approbation
- Effectuer une sauvegarde pré mise à jour afin de prévenir les éventuelles mises à jour ratées
- Définir l'option de redémarrage à appliquer après l'installation des correctifs

pour réduire le trafic sur la bande passante, Cyber Protect utilise une technologie de pair à pair. 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.

Fonctionnement

Vous pouvez configurer l'approbation automatique ou l'approbation manuelle des correctifs. Dans le schéma ci-dessous, vous pouvez voir la procédure d'approbation automatique des correctifs, ainsi que la procédure manuelle.



1. En premier lieu, vous devez effectuer au moins une analyse d'évaluation des vulnérabilités à l'aide du plan de protection avec module d'**évaluation des vulnérabilités** activé. Une fois l'analyse effectuée, la liste des vulnérabilités trouvées et celle des correctifs disponibles sont élaborées par le système.
2. Ensuite, vous pouvez configurer l'approbation automatique des correctifs ou opter pour l'approche d'approbation manuelle des correctifs.
3. Définissez de quelle manière installer les correctifs : de façon planifiée, ou à la demande. L'installation de correctifs à la demande peut être effectuée de trois manières différentes, selon vos préférences :
   - Accédez à la liste des correctifs (**Gestion de logiciel** > **Correctifs**) et installez les correctifs nécessaires.
   - Accédez à la liste des vulnérabilités (**Gestion de logiciel** > **Vulnérabilités**) et démarrez le processus de réparation, qui inclut aussi l'installation de correctifs.
   - Accédez à liste des périphériques (**Périphériques** > **Tous les périphériques**), sélectionnez les machines que vous souhaitez mettre à jour, puis installez-y les correctifs.

Vous pouvez suivre les résultats de l'installation des correctifs dans le widget **Tableau de bord** > **Présentation** > **Historique d'installation des correctifs**.

Paramètres de gestion des correctifs

Pour apprendre à créer un plan de protection avec le module de gestion des correctifs, reportez-vous à la section Création d'un plan de protection. En utilisant le plan de protection, vous pouvez indiquer les mises à jour de produits Microsoft ou tiers pour les systèmes d'exploitation Windows qui doivent être installées automatiquement sur les ordinateurs définis.

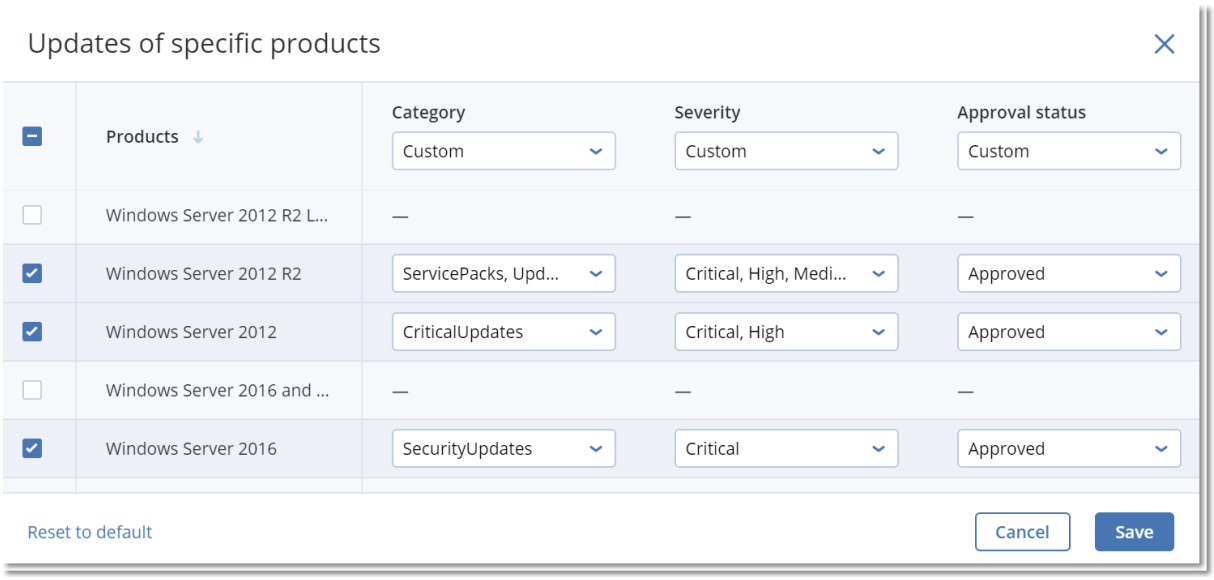
Vous pouvez définir les paramètres suivants pour le module de gestion des correctifs.

Produits Microsoft

Pour installer les mises à jour Microsoft sur les machines sélectionnées, activez l'option **Mettre les produits Microsoft à jour**.

Sélectionnez les mises à jour que vous souhaitez installer :

- **Toutes les mises à jour**
- **Uniquement les mises à jour critiques et de sécurité**
- **Mises à jour de produits spécifiques :** vous pouvez 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, par catégorie, gravité ou statut d'approbation.

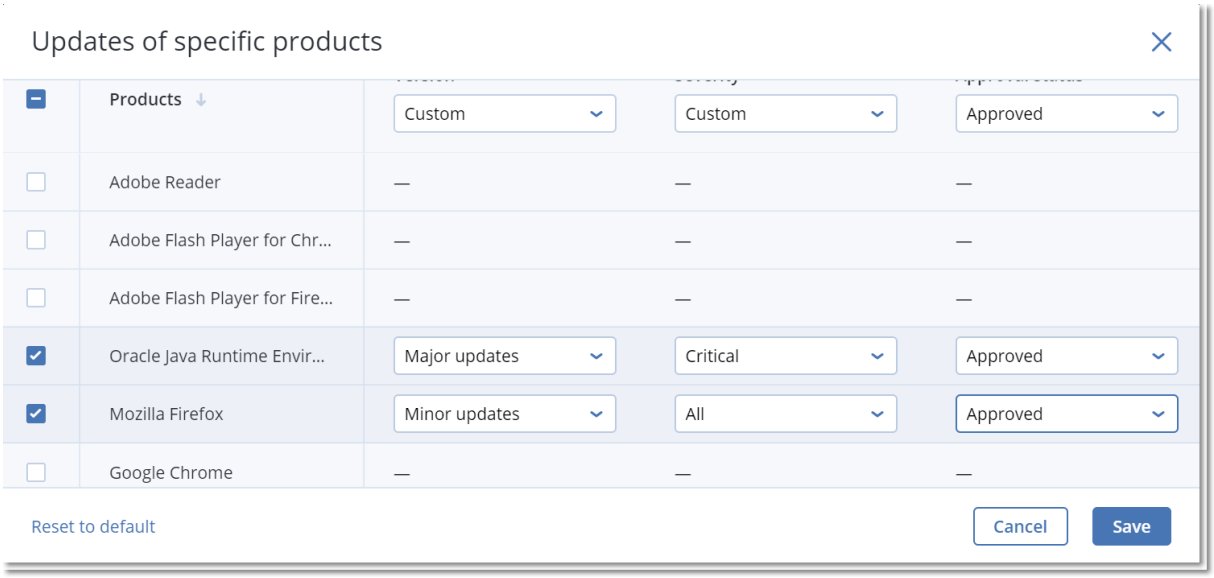


Produits Windows tiers

Pour installer les mises à jour tierces pour les systèmes d'exploitation Windows sur les machines sélectionnées, activez l'option **Produits Windows tiers**.

Sélectionnez les mises à jour que vous souhaitez installer :

- L'option **Mises à jour majeures uniquement** vous permet d'installer la dernière version disponible de la mise à jour.
- L'option **Mises à jour mineures uniquement** vous permet d'installer la version mineure de la mise à jour.
- **Mises à jour de produits spécifiques :** vous pouvez 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, par catégorie, gravité ou statut d'approbation.



Planification

Définissez le planning selon lequel les mises à jour seront installées sur les machines sélectionnées.

Planifiez l'exécution de la tâche à l'aide des événements suivants :

- **Planifier selon l'horaire :** 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.
- **Lorsque l'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.

Paramètre par défaut : **Planifier selon l'horaire**.

Type de planification :

- **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée.
- **Quotidienne :** sélectionnez les jours de la semaine pendant lesquels la tâche sera exécutée.
- **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.

Paramètre par défaut : **Quotidien**.

Démarrage à : sélectionnez l'heure exacte à laquelle la tâche sera exécutée.

Exécuter sur une plage de date : configurez une plage pendant laquelle le programme configuré sera effectif.

Conditions de démarrage : définissez toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée.

Les conditions de démarrage pour les analyses anti-malwares sont similaires aux conditions de démarrage du module Sauvegarde, décrites dans "Conditions de démarrage" (p. 247). 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.

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. Vous pourrez ainsi rétablir l'état antérieur en cas d'échec de l'installation du correctif. Pour que l'option **Sauvegarde pré-mise à jour** fonctionne, le module Gestion des correctifs et le module Sauvegarde doivent tous les deux être activés sur les ordinateurs correspondants 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**.

Gestion de la liste des correctifs

Une fois l'évaluation des vulnérabilités effectuée, vous trouverez les correctifs disponibles dans **Gestion de logiciel** > **Correctifs**.

Nom	Description
Nom	Le nom du correctif.
La gravité	La gravité du correctif : • **Critique** • **Élevée** • **Moyenne** • **Faible** • **Aucun**
Fournisseur	Le fournisseur du correctif.
Produit	Le produit auquel s'applique le correctif.
Versions installées	Les versions du produit qui sont déjà installées.
Version	La version du correctif.
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 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, l'identifiant de l'article de la base de connaissances est fourni.
Date de publication	La date à laquelle le correctif a été publié.
Machines	Le nombre de machines affectées.
Statut d'approbation	Le statut d'approbation est principalement nécessaire pour les scénarios d'approbation automatique et pour être en mesure de définir, dans le plan de protection, les mises à jour à installer par statut. 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. • **Non défini :** le statut du correctif n'est pas clair et doit être validé.
Contrat de licence	• Lire et accepter • Refusé. Si vous refusez le contrat de licence, le statut du correctif devient **Refusé** et le correctif ne sera pas installé.
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.

Approbation automatique des correctifs

L'approbation automatique des correctifs vous permet de faciliter le processus d'installation des mises à jour sur les machines. Voici un exemple de son fonctionnement.

Fonctionnement

Vous devez disposer de deux environnements : test et production. L'environnement test permet de tester l'installation de correctifs et de vous assurer qu'ils n'introduisent pas de problèmes. Une fois que vous avez testé l'installation des correctifs dans l'environnement test, vous pouvez installer automatiquement ces correctifs sûrs dans l'environnement de production.

Configuration de l'approbation automatique des correctifs

Configurer l'approbation automatique des correctifs

1. Vous devez lire et accepter le contrat de licence de chaque fournisseur dont vous souhaitez planifier la mise à jour des produits. Dans le cas contraire, l'installation automatique des correctifs sera impossible.
2. Configurez les paramètres d'approbation automatique.
3. Préparez le plan de protection (Par exemple, « Correctifs Test ») avec le module de **gestion des correctifs** activé, puis appliquez-le aux machines dans l'environnement test. Spécifiez la condition d'installation de correctif suivante : le statut d'approbation du correctif doit être **Non défini**. Cette étape est nécessaire pour valider les correctifs et vérifier si les ordinateurs fonctionnent correctement après l'installation des correctifs.
4. Préparez le plan de protection (Par exemple, « Correctifs Production ») avec le module de **gestion des correctifs** activé, puis appliquez-le aux machines dans l'environnement de production. Spécifiez la condition d'installation de correctif suivante : le statut d'approbation du correctif doit être **Approuvé**.
5. Exécutez le plan « Correctifs Test » et vérifiez les résultats. Le statut d'approbation des machines qui ne présentent pas de problème peut être maintenu sur **Non défini**, tandis que celui des machines qui fonctionnent mal peut être défini sur **Refusé**.
6. En fonction du nombre de jours définis pour l'option **Approbation automatique**, les correctifs **Non définis** deviendront **Approuvés**.
7. Une fois le plan « Correctifs Production » lancé, seuls les correctifs **Approuvés** seront installés sur les machines de production.

Les étapes manuelles sont présentes ci-dessous.

Étape 1 : Lisez et acceptez le contrat de licence des produits que vous souhaitez mettre à jour.

1. Dans la console Web Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Sélectionnez le correctif, puis lisez et acceptez le contrat de licence.

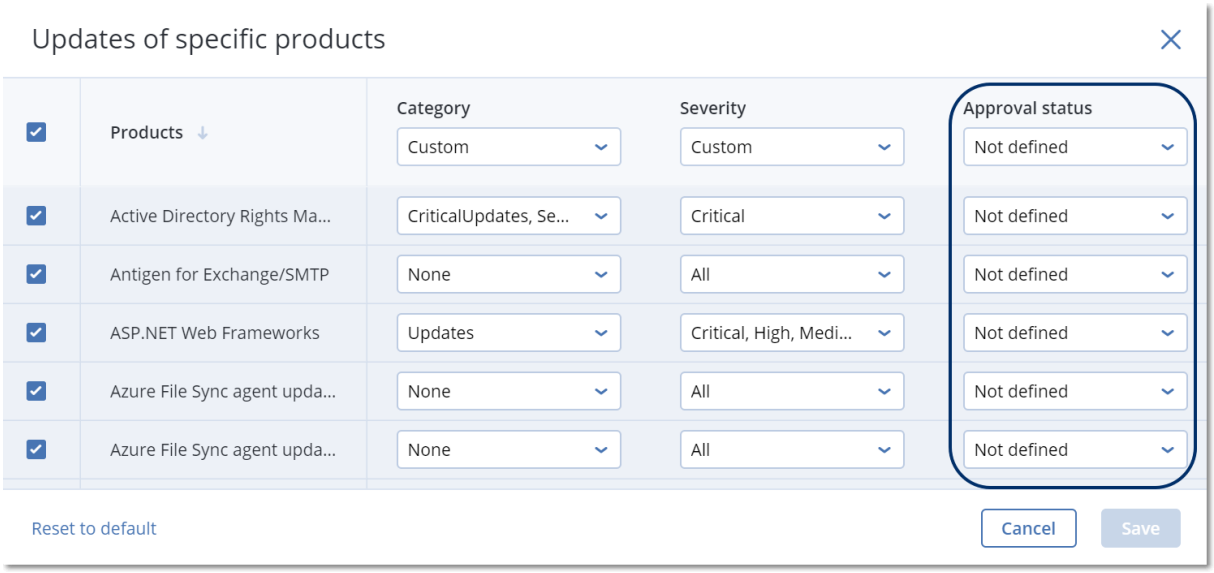
Étape 2. Configurez les paramètres d'approbation automatique.

1. Dans la console Web Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Cliquez sur **Paramètres**.
3. Activez l'option **Approbation automatique** et spécifiez le nombre de jours. Ainsi, après le nombre de jours spécifiés à compter de la première tentative d'installation des correctifs, les correctifs dont le statut est **Non défini** obtiendront automatiquement le statut **Approuvé**.
   Par exemple, vous avez spécifié 10 jours. Vous avez exécuté le plan « Correctifs Test » pour les machines de test et avez installé les correctifs. Les correctifs qui ont endommagé les machines ont été marqués comme **Refusés**, et les autres correctifs ont conservé le statut **Non défini**. Après 10 jours, les correctifs dont le statut est **Non défini** passent automatiquement au statut **Approuvé**.
4. Activez l'option **Accepter automatiquement les contrats de licence**. L'activation de cette option est nécessaire pour l'acceptation automatique des licences lors de l'installation des correctifs. Aucune confirmation de l'utilisateur n'est requise.

Étape 3. Préparez le plan de protection « Correctifs Test ».

1. Dans la console Web Cyber Protect, accédez à **Plans** > **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 en savoir plus sur ces paramètres, reportez-vous à la section « Paramètres de gestion des correctifs ».

Important
Pour tous les produits à mettre à jour, définissez le **statut d'approbation** sur **Non défini**. Lorsque le moment sera venu d'exécuter la mise à jour, l'agent installera uniquement les correctifs dont le statut est **Non défini** sur les machines sélectionnées dans l'environnement test.

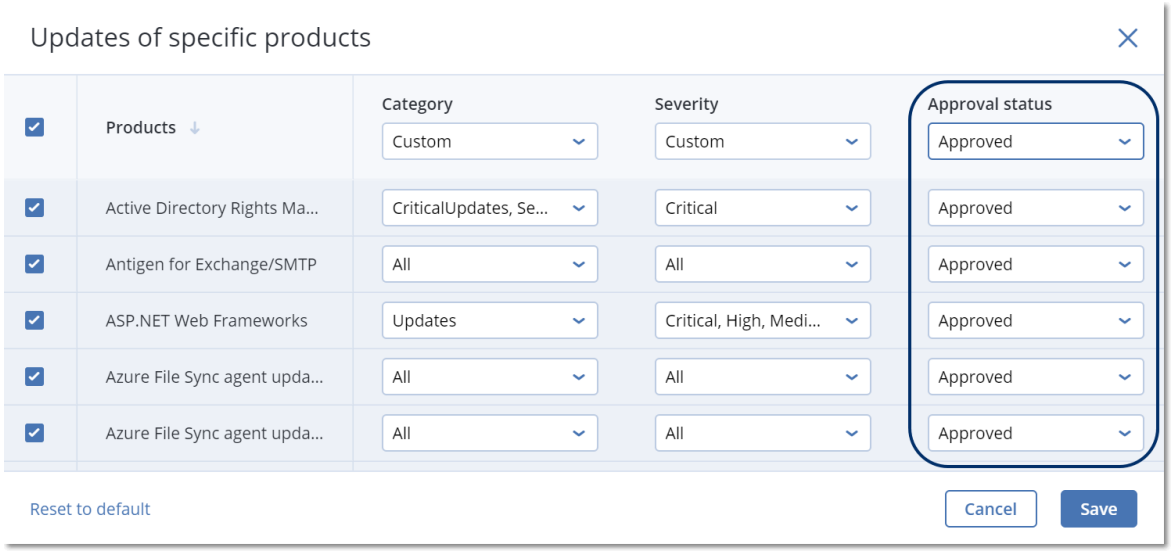


Étape 4 : Préparez le plan de protection « Correctifs Production ».

1. Dans la console Web Cyber Protect, accédez à **Plans** > **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 en savoir plus sur ces paramètres, reportez-vous à la section « Paramètres de gestion des correctifs ».

Important
Pour tous les produits à mettre à jour, définissez le **statut d'approbation** sur **Approuvé**. Lorsque le moment sera venu d'exécuter la mise à jour, l'agent installera uniquement les correctifs dont le statut est **Approuvé** sur les machines sélectionnées dans l'environnement de production.

Remarque



Etape 5. Exécutez le plan de protection « Correctifs Production » et vérifiez les résultats.

1. Exécutez le plan de protection « Correctifs Test » (de façon planifiée ou à la demande).
2. Après cela, examinez les correctifs installés et déterminez lesquels sont sûrs et lesquels ne le sont pas.
3. Accédez à **Gestion de logiciel** > **Correctifs** et définissez le **statut d'approbation** sur **Refusé** pour les correctifs qui ne sont pas sûrs.

Approbation manuelle des correctifs

Le processus d'approbation manuelle des correctifs est le suivant :

1. Dans la console Web Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Sélectionnez les correctifs que vous souhaitez installer, puis lisez et acceptez les contrats de licence.
3. Définissez le **statut d'approbation** sur **Approuvé** pour les correctifs dont vous souhaitez approuver l'installation.
4. Créez un plan de protection avec le module gestion des correctifs activé. Vous pouvez programmer le planning ou lancer le plan à la demande en cliquant sur **Exécuter maintenant** dans les paramètres du module de gestion des correctifs.

Seuls les correctifs approuvés seront alors installés sur les machines sélectionnées.

Installation des correctifs à la demande

L'installation de correctifs à la demande peut être effectuée de trois manières différentes, selon vos préférences :

- Accédez à la liste des correctifs (**Gestion de logiciel** > **Correctifs**) et installez les correctifs nécessaires.
- Accédez à la liste des vulnérabilités (**Gestion de logiciel** > **Vulnérabilités**) et démarrez le processus de réparation, qui inclut aussi l'installation de correctifs.
- Accédez à liste des périphériques (**Périphériques** > **Tous les périphériques**), sélectionnez les machines que vous souhaitez mettre à jour, puis installez-y les correctifs.

Examinons l'installation de correctifs à partir de la liste des correctifs :

1. Dans la console Web Cyber Protect, accédez à **Gestion de logiciel** > **Correctifs**.
2. Acceptez le contrat de licence des correctifs que vous souhaitez installer.
3. Sélectionnez les correctifs que vous souhaitez installer, puis cliquez sur **Installer**.
4. Sélectionnez les machines sur lesquelles les correctifs doivent être installés.
5. Définissez si la machine doit être redémarrée ou non après l'installation correctifs :
   - **Jamais :** la machine ne sera jamais redémarrée après installation correctifs.
   - **Si nécessaire :** la machine sera redémarrée uniquement si cela est nécessaire à l'application des correctifs.
   - **Toujours :** la machine sera toujours redémarrée après installation des correctifs. Vous pouvez toujours spécifier le délai de redémarrage.

   Ne redémarrez pas avant la fin de la sauvegarde : si le processus de sauvegarde est en cours d'exécution, le redémarrage de l'ordinateur sera retardé jusqu'à la fin de la sauvegarde.
6. Cliquez sur **Installer les correctifs**.

Les correctifs choisis seront installés sur les machines sélectionnées.

Durée de vie des correctifs dans la liste

Pour garder la liste des correctifs à jour, accédez à **Gestion de logiciel** > **Correctifs** > **Paramètres**, puis spécifiez l'option **Durée de vie dans la liste**.

L'option **Durée de vie dans la liste** définit la durée pendant laquelle le correctif disponible détecté sera conservé dans la liste des correctifs. En général, le correctif est retiré de la liste s'il est correctement installé sur toutes les machines où son absence a été détectée, ou lorsque le délai défini est écoulé.

- **Toujours :** le correctif reste toujours dans la liste.
- **7 jours** : le correctif est supprimé sept jours après sa première installation.
  Par exemple, vous disposez de deux machines sur lesquelles des correctifs doivent être installés. L'une d'elles est en ligne, et l'autre 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 la deuxième machine, car elle était hors ligne.
- **30 jours** : le correctif est supprimé trente jours après sa première installation.

Protection intelligente

Flux de menaces

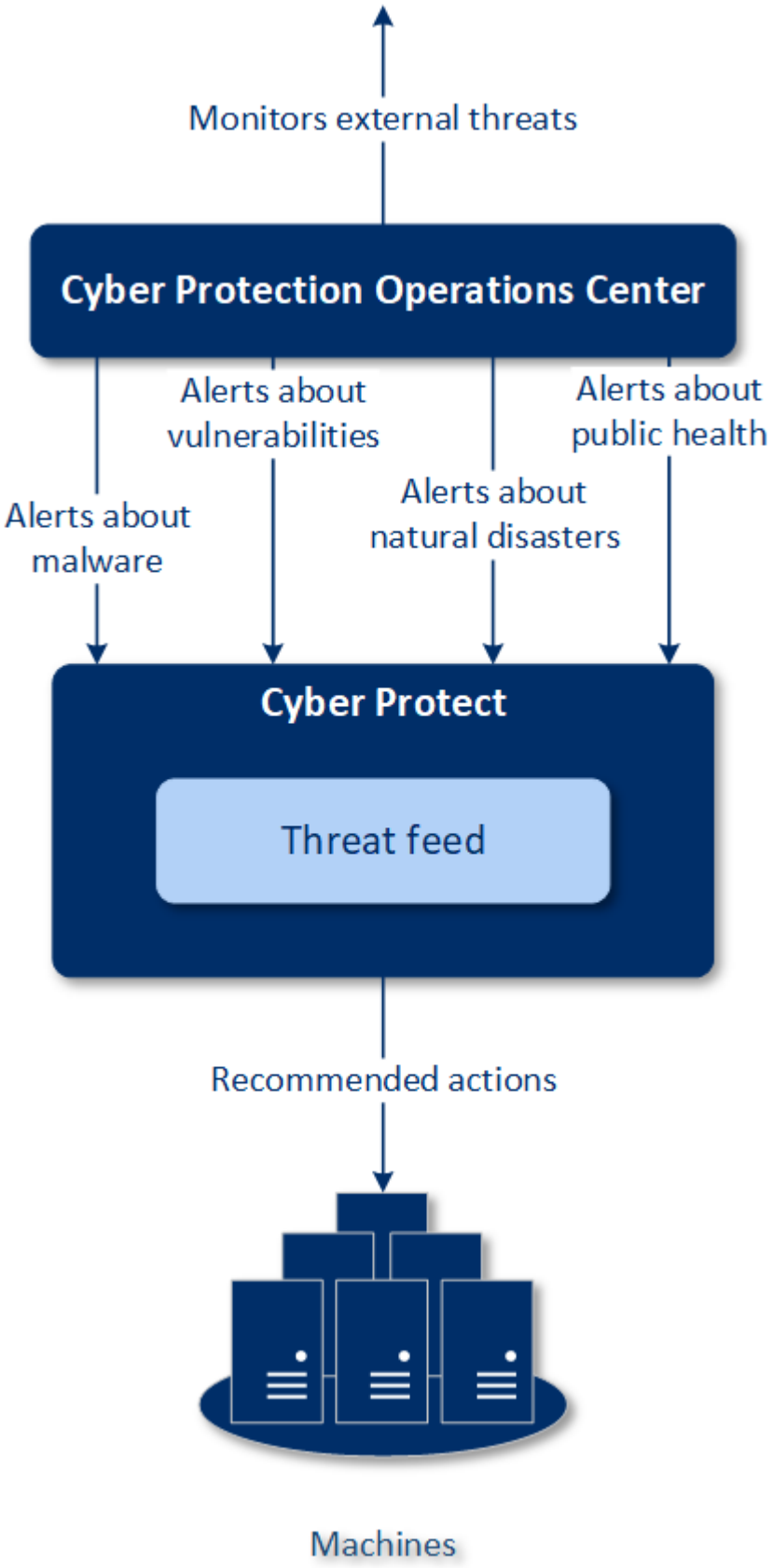
Le centre opérationnel de cyber protection Acronis (CPOC) génère des alertes de sécurité qui sont envoyées uniquement aux régions géographiques concernées. Ces alertes de sécurité fournissent des informations sur les malwares, les vulnérabilités, les catastrophes naturelles, la santé publique, et d'autres 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.

Une alerte de sécurité peut être résolue en suivant les différentes actions spécifiques fournies par les experts de la sécurité. Certaines alertes vous informent simplement de menaces à venir, mais ne vous recommandent pas d'actions de réparation.

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 Web 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.



Pour exécuter les actions recommandées suite aux alertes envoyées par le centre opérationnel de cyber protection Acronis, procédez comme suit :

1. Dans la console Web Cyber Protect, accédez à **Tableau de bord** > **Flux de menaces** pour rechercher la présence d'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 ordinateurs sur lesquels ces actions doivent être appliquées. Les actions suivantes peuvent être suggérées :

- **Évaluation des vulnérabilités** : pour analyser les ordinateurs à la recherche de vulnérabilités
- **Gestion des correctifs :** pour installer des correctifs sur les machines sélectionnées.
- **Protection contre les malwares :** pour exécuter une analyse complète des machines sélectionnées.
- **Sauvegarde de machines protégées ou non protégées :** pour sauvegarder des machines protégées/non protégées.

5. Cliquez sur **Démarrer**.

6. Sur la page **Activités**, vérifiez que l'activité a bien été effectuée.

Suppression de toutes les alertes

Les alertes de menaces sont supprimées automatiquement après les périodes suivantes :

- Catastrophes naturelles : 1 semaine
- Vulnérabilités : 1 mois
- Malwares : 1 mois
- Santé publique : 1 semaine

Carte de la protection des données

La fonctionnalité Carte de la protection des données vous permet d'effectuer les tâches suivantes :

- Obtenir des informations détaillées concernant les données stockées (classification, emplacements, statut de protection et informations supplémentaires) sur vos ordinateurs.
- Détecter si les données sont protégées. Les données sont considérées comme protégées si elles sont protégées par une sauvegarde (plan de protection avec module de sauvegarde activé).
- Effectuer des actions relatives à la protection des données.

Fonctionnement

1. En premier lieu, vous créez un plan de protection avec le module Carte de la protection des données activé.

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.
3. Vous pouvez également accéder à **Périphériques** > **Carte de la protection des données** et y trouver des informations concernant les fichiers non protégés par appareil.
4. Vous pouvez prendre des mesures pour protéger les fichiers non protégés détectés sur les appareils.

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 Web Cyber Protect, accédez à **Terminaux** > **Carte de la protection des données**.

   Dans la liste des appareils, vous trouverez des informations générales concernant le nombre de fichiers non protégés, la taille de ces fichiers par appareil, ainsi que la date de dernière découverte.

   Pour protéger les fichiers sur un ordinateur particulier, 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 l'appareil particulier qui possède des fichiers non protégés, cliquez sur **Masquer jusqu'à la prochaine découverte de données**.
2. Pour afficher des informations détaillées sur les fichiers non protégés sur un appareil en particulier, cliquez sur le nom de l'appareil.

   Vous verrez la liste des fichiers non protégés par extension de fichier et par emplacement. Vous pouvez filtrer cette liste par extension de fichier.
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 ».

Vous pouvez définir les paramètres suivants pour le module de carte de protection des données.

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.

Planifiez l'exécution de la tâche à l'aide des événements suivants :

- **Planifier selon l'horaire :** 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.
- **Lorsque l'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.

Paramètre par défaut : **Planifier selon l'horaire**.

Type de planification :

- **Mensuelle :** sélectionnez les mois et les semaines ou jours du mois pendant lesquels la tâche sera exécutée.
- **Quotidienne :** sélectionnez les jours de la semaine pendant lesquels la tâche sera exécutée.
- **Horaire :** sélectionnez les jours de la semaine, le nombre de répétitions et l'intervalle d'exécution de la tâche.

Paramètre par défaut : **Quotidien**.

Démarrage à : sélectionnez l'heure exacte à laquelle la tâche sera exécutée.

Exécuter sur une plage de date : configurez une plage pendant laquelle le programme configuré sera effectif.

Conditions de démarrage : définissez toutes les conditions qui doivent être remplies simultanément pour que la tâche soit exécutée.

Les conditions de démarrage pour les analyses anti-malwares sont similaires aux conditions de démarrage du module Sauvegarde, décrites dans "Conditions de démarrage" (p. 247). 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.

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 masqués 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.

Accès à distance au bureau

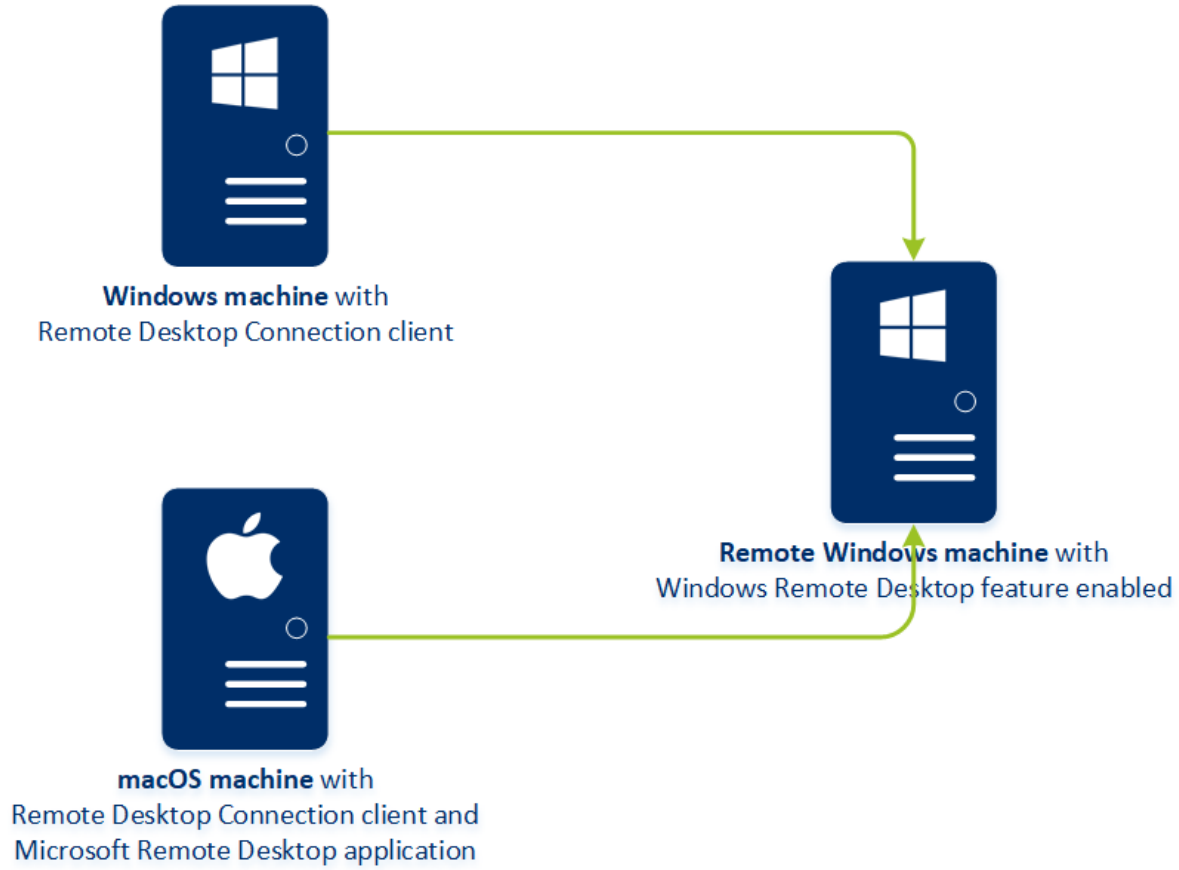
Accès distant (Clients RDP et HTML5)

Cyber Protect vous offre une capacité d'accès à distance. Vous pouvez gérer et vous connecter à distance aux machines des utilisateurs finaux directement depuis la console Web. Cela vous permet d'aider facilement les utilisateurs à résoudre les problèmes qu'ils rencontrent sur leur machine.

Pré-requis :

- Un agent de protection est installé sur la machine distance avant d'être enregistré avec le serveur de gestion.
- Une licence Cyber Protect appropriée est attribuée à l'ordinateur.
- Le client de connexion à distance au bureau est installé sur la machine depuis laquelle la connexion est démarrée.
- La machine depuis laquelle la connexion RDP est démarrée doit pouvoir accéder au serveur de gestion par son nom d'hôte. Les paramètres DNS doivent être correctement configurés ou le nom d'hôte du serveur de gestion doit être inscrit dans le fichier des hôtes.

Une connexion à distance peut être établie depuis des machines Windows et macOS.



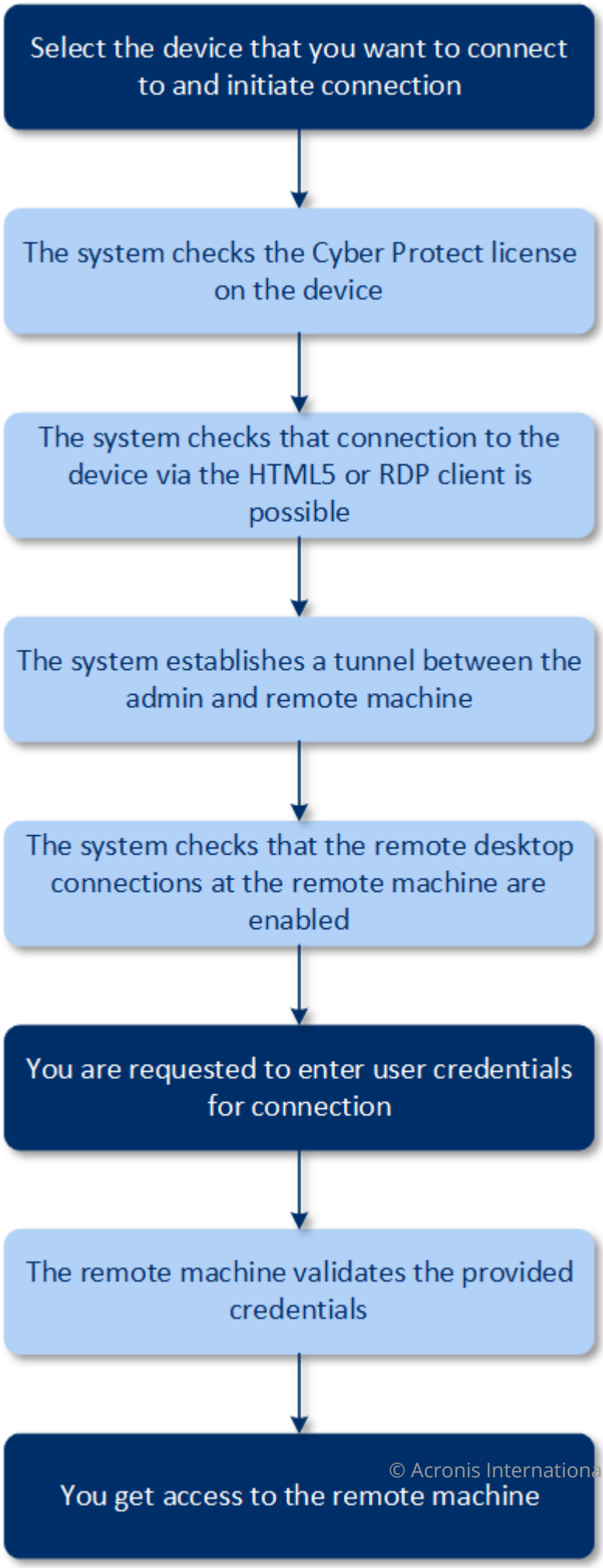
La fonctionnalité d'accès à distance peut être utilisée pour vous connecter aux machines Windows pour lesquelles la fonctionnalité Bureau à distance Windows est disponible. Pour cette raison, un accès à distance n'est pas possible pour les systèmes Windows 10 Home ou macOS par exemple.

Pour établir une connexion depuis une machine macOS vers une machine distante, assurez-vous que les applications suivantes sont installées sur la machine macOS :

- Le client de connexion à distance au bureau
- L'application Microsoft Bureau à distance

Fonctionnement

Lorsque vous essayez de vous connecter à une machine distante, le système commence par vérifier si elle dispose d'une licence Cyber Protect. Ensuite, le système vérifie si la connexion via le client HTML5 ou RDP est possible ou non. Vous démarrez une connexion via le client RDP ou HTML5. Le système établit un tunnel vers la machine distante et vérifie si les connexions de bureau à distance sont activées sur la machine distante ou non. Vous saisissez ensuite les informations d'identification et, après leur validation, pouvez accéder à la machine distante.



Se connecter à une machine distante

Pour vous connecter à une machine distante, procédez comme suit :

1. Dans la console Web Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Cliquez sur la machine à laquelle vous souhaitez vous connecter à distance, puis cliquez sur **Bureau cyber protection** > **Se connecter via un client RDP** ou sur **Se connecter via un client HTML5**.

   Remarque
   La connexion via un client HTML5 n'est disponible que si le serveur de gestion est installé sur un ordinateur Linux.

3. [Facultatif, uniquement pour la connexion via un client RDP] Téléchargez et installez le client Connexion à distance au bureau. Démarrez la connexion à la machine distante.
4. Spécifiez l'identifiant et le mot de passe requis pour accéder à la machine distante, puis cliquez sur **Connexion**.

Vous êtes alors connecté à la machine distante et pouvez la gérer.

Partage d'une connexion à distance

Il se peut que les employés en télétravail doivent accéder à leur ordinateur du bureau, mais il est possible que votre organisation n'ait pas configuré de VPN ni d'autres outils pour la connexion à distance. Le service Cyber Protect vous offre la capacité de partager un lien RDP avec les utilisateurs, leur fournissant ainsi un accès à distance à leur ordinateur.

Pour activer la fonctionnalité de partage de connexion à distance

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Protection** > **Connexion à distance**.
2. Cochez la case **Partager la connexion à distance au bureau**.

Lorsque vous sélectionnerez un terminal dans la console Web Cyber Protect, une nouvelle option **Partager la connexion à distance** apparaîtra.

Pour partager une connexion à distance avec vos utilisateurs

1. Dans la console Web Cyber Protect, accédez à **Terminaux** > **Tous les terminaux**.
2. Sélectionnez le périphérique pour lequel vous souhaitez fournir une connexion à distance.
3. Cliquez sur **Partager la connexion à distance**.
4. Cliquez sur **Obtenir le lien**. Dans la fenêtre qui s'ouvre, copiez le lien généré. Ce lien peut être partagé avec un utilisateur ayant besoin d'un accès à distance au périphérique. Il est valide pendant 10 heures.

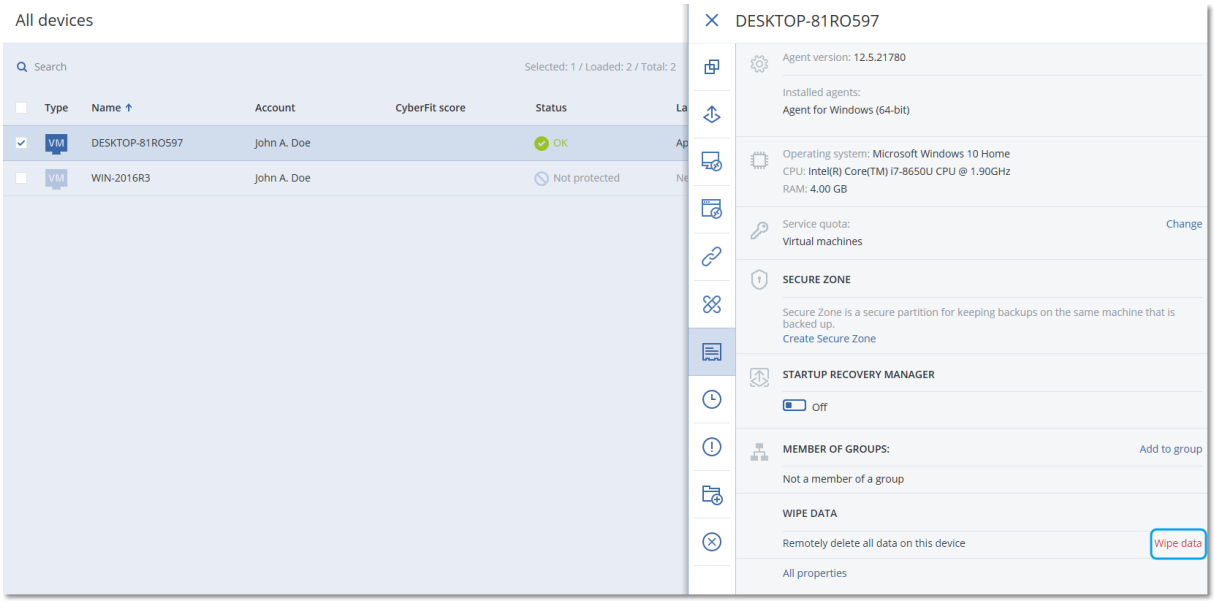
Après avoir obtenu le lien, vous pouvez le partager par e-mail ou via d'autres moyens de communication. L'utilisateur avec qui le lien a été partagé doit cliquer dessus, puis sélectionner le type de connexion :

- Se connecter via un client RDP.
  Cette connexion lancera une invite de téléchargement et d'installation du client de connexion à distance.
- Se connecter via un client HTML5.
  Cette connexion ne nécessite l'installation d'aucun client RDP sur la machine de l'utilisateur. L'utilisateur sera redirigé vers un écran de connexion et devra saisir les identifiants permettant d'accéder à la machine.

Effacement à distance

L'effacement à distance permet à un administrateur du service Cyber Protect et au propriétaire d'une machine de supprimer des données sur une machine gérée, si elle est égarée ou volée par exemple. Tout accès non autorisé à des informations sensibles sera donc évité.

L'effacement à distance est uniquement disponible pour les machines exécutant Windows 10. 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 Web 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 vérifier les détails concernant le processus d'effacement et la personne l'ayant initié dans **Tableau de bord** > **Activités**.

Groupes du périphérique

Les groupes de périphériques sont conçus pour une gestion simplifiée d'un grand nombre de périphériques enregistrés.

Vous pouvez appliquer un plan de protection à un groupe. Une fois qu'un nouveau périphérique apparaît dans le groupe, il est protégé par le plan. Si un périphérique est supprimé d'un groupe, il n'est plus protégé par le plan. Un plan appliqué à un groupe ne peut pas être supprimé uniquement chez un membre du groupe. Il sera supprimé chez tout le groupe.

Seuls les périphériques de même type peuvent être ajoutés à un groupe. Par exemple, sous **Hyper-V**, vous pouvez créer un groupe de machines virtuelles Hyper-V. Sous **Machines avec des agents**, vous pouvez créer un groupe de machines avec des agents installés. Sous **Tous les périphériques**, vous ne pouvez pas créer de groupe.

Un périphérique peut faire partie d'un ou de plusieurs groupes.

Groupes par défaut

Une fois un périphérique enregistré, il apparaît dans l'un des groupes racines intégrés dans l'onglet **Périphériques**.

Les groupes racines *ne peuvent pas* être modifiés ni supprimés. Vous *ne pouvez pas* appliquer de plan à des groupes racines.

Certains des groupes racines contiennent des sous-groupes racines intégrés. Ces groupes *ne peuvent pas* être modifiés ni supprimés. Cependant, vous *pouvez* appliquer des plans à des sous-groupes racines intégrés.

Groupes personnalisés

Le fait de protéger tous les périphériques d'un groupe par défaut avec un seul plan de protection centralisé peut ne pas être satisfaisant en raison des différents rôles des machines. Les données sauvegardées sont spécifiques pour chaque service ; certaines données doivent être sauvegardées fréquemment, d'autres données sont sauvegardées deux fois par an. Par conséquent, il se peut que vous souhaitiez créer plusieurs plans de protection applicables à différents ensembles de machines. Dans ce cas, envisagez la création de groupes personnalisés.

Un groupe personnalisé peut contenir un ou plusieurs groupes imbriqués. Tous les groupes personnalisés peuvent être modifiés ou supprimés. Il existe les groupes personnalisés suivants :

- **Groupes statiques**

  Les groupes statiques contiennent les machines ajoutées manuellement. Le contenu des groupes statiques ne change jamais à moins que vous n'ajoutiez ou supprimiez une machine explicitement.

  Exemple : Vous créez un groupe personnalisé pour le service comptable et ajoutez manuellement les machines de ce service à ce groupe. Une fois que vous appliquez le plan de

protection à ce groupe, les machines des comptables sont protégées. Si un nouveau comptable est employé, vous devrez ajouter manuellement la nouvelle machine sur le groupe.

- **Groupes dynamiques**

  Les groupes dynamiques contiennent les machines ajoutées automatiquement selon les critères de recherche spécifiés lors de la création d'un groupe. Le contenu du groupe dynamique change automatiquement. Une machine reste dans le groupe tant qu'elle répond aux critères spécifiés.

  Exemple 1 : Les noms d'hôte des machines appartenant au service comptable comportent le mot « comptabilité ». Vous spécifiez le nom de la machine partielle en tant que critère d'appartenance au groupe et appliquez un plan de protection au groupe. Si un nouveau comptable est employé, la nouvelle machine est ajoutée au groupe dès qu'elle est enregistrée. Elle est ainsi protégée automatiquement.

  Exemple 2 : Le service comptable forme une unité d'organisation (UO) Active Directory séparée. Vous spécifiez l'UO comptable en tant que critère d'appartenance au groupe et appliquez un plan de protection au groupe. Si un nouveau comptable est employé, la nouvelle machine est ajoutée au groupe dès qu'elle est enregistrée, et ajoutée à l'UO (quel que soit l'ordre d'arrivée). Elle est ainsi protégée automatiquement.

Création d'un groupe statique

1. Cliquez sur **Périphériques**, puis sélectionnez le groupe intégré contenant les périphériques pour lesquels vous souhaitez créer un groupe statique.
2. Cliquez sur l'icône en forme d'engrenage en regard du groupe dans lequel vous souhaitez créer un groupe.
3. Cliquez sur **Nouveau groupe**.
4. Indiquez le nom du groupe, puis cliquez sur **OK**.

   Le groupe nouvellement créé apparaît dans l'arbre de groupes.

Ajout de périphériques aux groupes statiques

1. Cliquez sur **Périphériques**, puis sélectionnez un ou plusieurs périphérique(s) que vous souhaitez ajouter à un groupe.
2. Cliquez sur **Ajouter au groupe**.

   Le logiciel affiche une arborescence de groupes auxquels le périphérique sélectionné peut être ajouté.
3. Si vous souhaitez créer un nouveau groupe, procédez comme suit. Sinon, ignorez cette étape.
   a. Sélectionnez le groupe dans lequel vous souhaitez créer un groupe.
   b. Cliquez sur **Nouveau groupe**.
   c. Indiquez le nom du groupe, puis cliquez sur **OK**.
4. Sélectionnez le groupe auquel vous voulez ajouter le périphérique, puis cliquez sur **Terminé**.

Pour ajouter des périphériques à un groupe statique, vous pouvez également sélectionner le groupe et cliquer sur **Ajouter des périphériques**.

Création d'un groupe dynamique

1. Cliquez sur **Périphériques**, puis sélectionnez le groupe contenant les périphériques pour lesquels vous souhaitez créer un groupe dynamique.
2. Utilisez le champ de recherche pour chercher des périphériques. Vous pouvez utiliser plusieurs attributs et opérateurs décrits ci-dessous.
3. Cliquez sur **Enregistrer sous** en regard du champ de recherche.

   Remarque
   Certains attributs ne sont pas pris en charge pour la création de groupes. Consultez le tableau de la section Requête de recherche ci-dessous.

4. Indiquez le nom du groupe, puis cliquez sur **OK**.

Requête de recherche

Le tableau suivant résume les attributs disponibles que vous pouvez utiliser dans vos requêtes de recherche.

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
`name`	• Nom d'hôte pour les machines physiques • Nom des machines virtuelles • Nom de la base de données • Adresse électronique pour les boîtes aux lettres	`name = 'en-00'`	Oui
`parameters.MacAddress`	Adresse MAC.	`parameters.MacAddress LIKE '00-22-4D-50-25-E5'`	Oui
`comment`	Commentaire pour un périphérique. Il peut être spécifié automatiquement ou manuellement. Valeur par défaut :	`comment = 'important machine'` `comment = ''` (toutes les machines sans commentaire)	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• 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 périphériques. **Remarque** Si vous ajoutez manuellement du texte dans le champ commentaire, la synchronisation automatique avec la description Windows se désactive. Pour l'activer à nouveau, effacez le commentaire que vous avez ajouté. Pour actualiser les commentaires automatiquement synchronisés pour vos terminaux, redémarrez le service de machine gérée dans **Services Windows** ou exécutez les commandes suivantes dans l'invite de commandes : `net stop mms`		

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	`net start mms` Pour afficher le commentaire, sous **Périphériques**, sélectionnez le périphérique, cliquez sur **Détails**, puis localisez la section **Commentaire**. Pour ajouter ou modifier le commentaire, 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 synchronisée toutes les 15 minutes. ◦ Vide pour d'autres périphériques.		

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	Remarque Si vous ajoutez manuellement du texte dans le champ commentaire, la synchronisation automatique avec la description Windows se désactive. Pour l'activer à nouveau, effacez le commentaire que vous avez ajouté. • 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 encore les deux peuvent		

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	être vierges. Si les deux commentaires sont spécifiés, le commentaire sur le terminal sera prioritaire. Pour afficher un commentaire sur un agent, sous **Périphériques** > **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**.		
`ip`	Adresse IP (uniquement pour les machines physiques).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Oui
`cpuArch`	Architecture du processeur. Valeurs possibles : • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Oui
`memorySize`	Taille de la mémoire RAM en mégaoctets (Mo).	`memorySize < 1024`	Oui
`cpuName`	Nom du processeur.	`cpuName LIKE '%XEON%'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
`insideVm`	Machine virtuelle avec un agent. Valeurs possibles : • `true` • `false`	`insideVm = true`	Oui
`tzOffset`	Décalage de fuseau horaire de l'ordinateur en minutes.	`tzOffset = 120`	Oui
`parameters.Architecture`	Architecture du système d'exploitation. Valeurs possibles : • `'x86'` • `'x64'`	`parameters.Architecture = 'x86'`	Oui
`osName`	Nom du système d'exploitation.	`osName LIKE '%Windows XP%'`	Oui
`osType`	Type de système d'exploitation. Valeurs possibles : • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	Oui
`osProductType`	Type de produit du système d'exploitation. Valeurs possibles : • `'dc'` Représente le contrôleur de domaine. • `'server'` • `'workstation'`	`osProductType = 'server'`	Oui
`virtualType`	Type de machine virtuelle.	`virtualType = 'vmwesx'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	Valeurs possibles : • `'vmwesx'` Machines virtuelles VMware. • `'mshyperv'` Machines virtuelles Hyper-V. • `'pcs'` Machines virtuelles Virtuozzo. • `'hci'` Machines virtuelles Virtuozzo Hybrid Infrastructure. • `'scale'` Machines virtuelles HC3 de Scale Computing. • `'ovirt'` Machines virtuelles oVirt.		
`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.	`osVersionMminor = 1`	Oui
`isOnline`	Disponibilité de machine. Valeurs possibles : • `true` • `false`	`isOnline = true`	Non
`tenant`	Nom de l'unité auquel le périphérique appartient.	`tenant = 'Unit 1'`	Oui
`tenantId`	Identificateur de l'unité	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	auquel le périphérique appartient. Pour obtenir l'identifiant de l'unité, sous **Périphériques**, sélectionnez le périphérique, puis **Détails** > **Toutes les propriétés**. L'identifiant apparaît dans le champ `ownerId`.		
`state`	État du périphérique. Valeurs possibles : • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	Non
`status`	État de ressources. Valeurs possibles : • `'notProtected'` • `'ok'` • `'warning'` • `'error'`	`status = 'ok'`	Non

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	• `'critical'`		
`protectedByPlan`	Périphériques protégés par un plan de protection avec un identifiant donné. Pour obtenir l'identifiant du plan, cliquez sur **Plans** > **Sauvegarde**. Sélectionnez ensuite le plan et cliquez sur le diagramme dans la colonne **État**, puis sur un état. Une nouvelle recherche avec l'identifiant du plan sera créée.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`okByPlan`	Périphériques protégés par un plan de protection avec un identifiant donné et un état **OK**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`errorByPlan`	Périphériques protégés par un plan de protection avec un identifiant donné et un état **Erreur**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`warningByPlan`	Périphériques protégés par un plan de protection avec un identifiant donné et un état **Avertissement**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`runningByPlan`	Périphériques protégés par un plan de protection avec un identifiant donné et un état **En cours d'exécution**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non
`interactionByPlan`	Périphériques protégés par un plan de protection avec un identifiant donné	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Non

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	et un état **Intervention requise**.		
`ou`	Machines appartenant à l'unité organisationnelle Active Directory spécifiée.	`ou IN ('RnD', 'Computers')`	Oui
`id`	Identifiant du périphérique. Pour obtenir l'identifiant du périphérique, sous **Périphériques**, sélectionnez le périphérique, puis **Détails** > **Toutes les propriétés**. L'identifiant apparaît dans le champ `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Oui

`lastBackupTime`	Date et heure de la dernière sauvegarde réussie.
	Le format est « `AAAA-MM-JJ HH:MM` ».
		`lastBackupTime > '2022-03-11'`
		`lastBackupTime <= '2022-03-11 00:15'`
		`lastBackupTime is null`
			Non

`lastBackupTryTime`	Heure de la dernière tentative de sauvegarde. Le format est « `AAAA-MM-JJ HH:MM` ».	`lastBackupTryTime >= '2022-03-11'`	Non
`nextBackupTime`	Heure de la prochaine sauvegarde. Le format est « `AAAA-MM-JJ HH:MM` ».	`nextBackupTime >= '2022-08-11'`	Non
`agentVersion`	Version de l'agent de protection installé.	`agentVersion LIKE '12.0.*'`	Oui
`hostId`	Identifiant interne de l'agent de protection. Pour obtenir l'identifiant	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Oui

Attribut	Signification	Exemples de requête de recherche	Pris en charge pour la création de groupe
	de l'agent de protection, sous **Périphériques**, sélectionnez la machine, puis **Détails** > **Toutes les propriétés**. Utilisez la valeur `"id"` de la propriété `agent`.		
`resourceType`	Type de ressource. Valeurs possibles : • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_machine.mshyperv'` • `'virtual_machine.rhev'` • `'virtual_machine.kvm'` • `'virtual_machine.xen'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Oui
`hasAsz`	Agent de protection sur une machine physique avec AcronisSecure Zone. Valeurs possibles : • `true` • `false`	`hasAsz=true`	Oui
`chassis`	Type de châssis de l'ordinateur. Valeurs possibles : • `unknown` • `laptop` • `desktop` • `server` • `other`	`chassis='laptop'`	Oui

Remarque
Si vous n'indiquez pas la valeur heure et minutes, la date et l'heure de début seront considérées comme étant AAAA-MM-JJ 00:00, et la date et l'heure de fin seront considérées comme étant AAAA-MM-JJ 23:59:59. Par exemple, dernièreHeuredeSauvegarde = 2020-02-20, signifie que les résultats de recherche incluront toutes les sauvegardes de l'intervalle dernièreHeuredeSauvegarde >= 2020-02-20 00:00 et dernièreHeuredeSauvegarde <= 2020-02-20 23:59:59

Opérateurs

Le tableau suivant résume les options disponibles.

Opérateur	Signification	Exemples
`AND`	Opérateur de conjonction logique.	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Opérateur de disjonction logique.	`state = 'backup' OR state = 'interactionRequired'`
`IN (<value1>,... <valueN>)`	Cet opérateur est utilisé pour vérifier si une expression correspond à une valeur dans une liste de valeurs.	`osType IN ('windows', 'linux')`
`NOT`	Opérateur de négation logique.	`NOT(osProductType = 'workstation')`
`NOT IN (<value1>,... <valueN>)`	Cet opérateur est l'opposé de l'opérateur `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'modèle de caractères génériques'`	Cet opérateur est utilisé pour vérifier si une expression correspond au modèle de caractères génériques.
	Les opérateurs de métacaractères suivants peuvent être utilisés :
	• * 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_'`

`RANGE(<starting_value>, <ending_value>)`	Cet opérateur est utilisé pour vérifier si une expression est comprise dans une fourchette de valeurs (inclusive).	`ip RANGE ('10.250.176.1','10.250.176.50')`
`= or ==`	Opérateur *Égal à*.	`osProductType = 'server'`
`!=` ou `<>`	Opérateur *Différent de*.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`

Opérateur	Signification	Exemples
<	Opérateur *Inférieur à*.	`memorySize < 1024`
>	Opérateur *Supérieur à*.	`diskSize > 300 Go`
<=	Opérateur *Inférieur ou égal à*.	`lastBackupTime <= '2022-05-11 00:15'`
>=	Opérateur *Supérieur ou égal à*.	`nextBackupTime >= '2022-09-11'`

Application d'un plan de protection à un groupe

1. Cliquez sur **Périphériques**, puis sélectionnez le groupe par défaut contenant le groupe auquel appliquer un plan de protection.
   Le logiciel affiche la liste des groupes enfants.
2. Sélectionnez le groupe auquel vous voulez appliquer un plan de protection.
3. Cliquez sur **Sauvegarde de groupe**.
   Le logiciel affiche la liste des plans de protection pouvant être appliqués au groupe.
4. Effectuez l'une des actions suivantes :
   - Développez un plan de protection existant, plus cliquez sur **Appliquer**.
   - Cliquez sur **Créer un nouveau**, puis créez un nouveau plan de protection, comme décrit dans « Sauvegarde ».

Surveillance et rapports

Le tableau de bord **Vue d'ensemble** vous permet de surveiller l'état de votre infrastructure protégée.

La section **Rapports** vous permet de générer des rapports planifiés ou à la demande sur l'infrastructure protégée. Cette section est disponible uniquement avec une licence Advanced.

Tableau de bord Vue d'ensemble

Le tableau de bord **Vue d'ensemble** fournit différents widgets personnalisables qui offrent une vue d'ensemble de votre infrastructure protégée. Vous pouvez faire un choix parmi plus de 20 widgets se présentant sous la forme d'un graphique en secteurs, d'un tableau, d'un graphique, d'un graphique à barres et de listes. Ils disposent d'éléments sur lesquels cliquer qui permettent de faire des recherches sur les problèmes et de les résoudre. Les informations dans les widgets sont mises à jour toutes les cinq minutes.

Avec une licence Advanced, vous pouvez également télécharger l'état actuel du tableau de bord ou l'envoyer par e-mail au format .pdf et/ou .xlsx. Pour envoyer le tableau de bord par courrier électronique, assurez-vous que les paramètres du **Serveur de messagerie** sont configurés.

Les widgets disponibles dépendent de l'édition de Cyber Protect. Les widgets par défaut sont répertoriés ci-dessous :

Widget	Disponibilité	Description
Cyberprotection	Non disponible dans les éditions Cyber Backup	Affiche les informations globales concernant la taille des sauvegardes, les malwares bloqués, les URL bloquées, les vulnérabilités trouvées et les correctifs installés.
État de protection	Disponible dans toutes les éditions	Affiche l'état de protection actuel de tous les ordinateurs.
Activités	Disponible dans toutes les éditions	Affiche un récapitulatif des activités réalisées pendant une période donnée.
Résumé des alertes actives	Disponible dans toutes les éditions	Affiche une synthèse des alertes actives par type d'alerte et par gravité.
Statut d'installation des correctifs	Non disponible dans les éditions Cyber Backup	Affiche le nombre d'ordinateurs groupés par statut d'installation des correctifs.
Mises à jour manquées, par catégorie	Non disponible dans les éditions Cyber Backup	Affiche le nombre de mises à jour manquantes, par catégorie.

Intégrité du disque	Non disponible dans les éditions Cyber Backup	Affiche le nombre de disques, par état.
Appareils	Disponible dans toutes les éditions	Affiche des informations détaillées concernant les ordinateurs de votre environnement.
Détails des alertes actives	Disponible dans toutes les éditions	Affiche des informations détaillées concernant les alertes actives.
Vulnérabilités existantes	Disponible dans toutes les éditions	Affiche les vulnérabilités existantes pour les systèmes d'exploitation et les applications dans votre environnement, ainsi que les ordinateurs affectés.
Historique d'installation des correctifs	Non disponible dans les éditions Cyber Backup	Affiche des informations détaillées concernant les correctifs installés.
Affectés récemment	Disponible dans toutes les éditions	Affiche des informations détaillées concernant les ordinateurs infectés récemment.
Résumé des emplacements	Disponible dans toutes les éditions	Affiche des informations détaillées concernant les emplacements de sauvegarde.

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 l'icône en forme de crayon lorsque le widget est sélectionné. Lorsque vous avez terminé de modifier le widget, cliquez sur **Terminé**.

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 supprimer un widget

Cliquez sur le signe X à côté du nom du widget.

Cyber Protection

Ce widget affiche les informations globales concernant la taille des sauvegardes, les malwares bloqués, les URL bloquées, les vulnérabilités trouvées et les correctifs installés.

La ligne supérieure affiche les statistiques actuelles :

- **Sauvegardé aujourd'hui :** la somme des tailles de point de récupération 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

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 :** ordinateurs sur lesquels le plan de protection est appliqué.
- **Non protégé :** ordinateurs sur lesquels 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.
- **Géré :** ordinateurs sur lesquels l'agent de protection est installé.
- **Découvert** : les ordinateurs sur lesquels 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.

Machines découvertes

Ce widget affiche la liste des machines découvertes pendant la période spécifiée.

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.
- Sur les lecteurs NVMe, la surveillance de l'intégrité du disque n'est prise en charge que pour les lecteurs qui communiquent des données SMART via l'API Windows. La surveillance de l'intégrité du disque n'est pas prise en charge pour les lecteurs NVMe qui nécessitent la lecture des données SMART directement depuis le lecteur.

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 %.
- **Calcul des données du disque**
  L'intégrité actuelle et la prévision de l'intégrité du disque sont en cours de calcul.

Fonctionnement

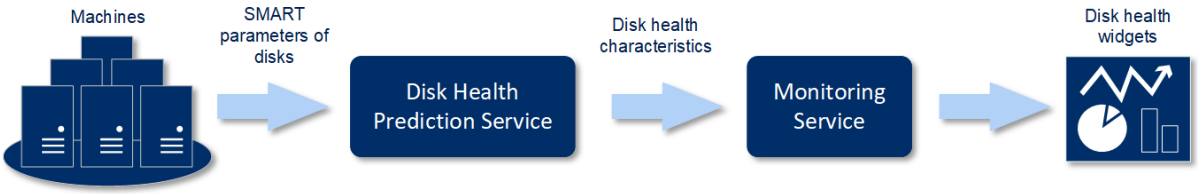
Le service Prévision de l'intégrité du disque se sert d'un modèle de prévision basé sur l'intelligence artificielle.

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'état de santé du disque traite les paramètres SMART, effectue des prévisions, et fournit les caractéristiques d'état de santé 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 toujours 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 Web Cyber Protect.



Widgets de l'état de santé du disque

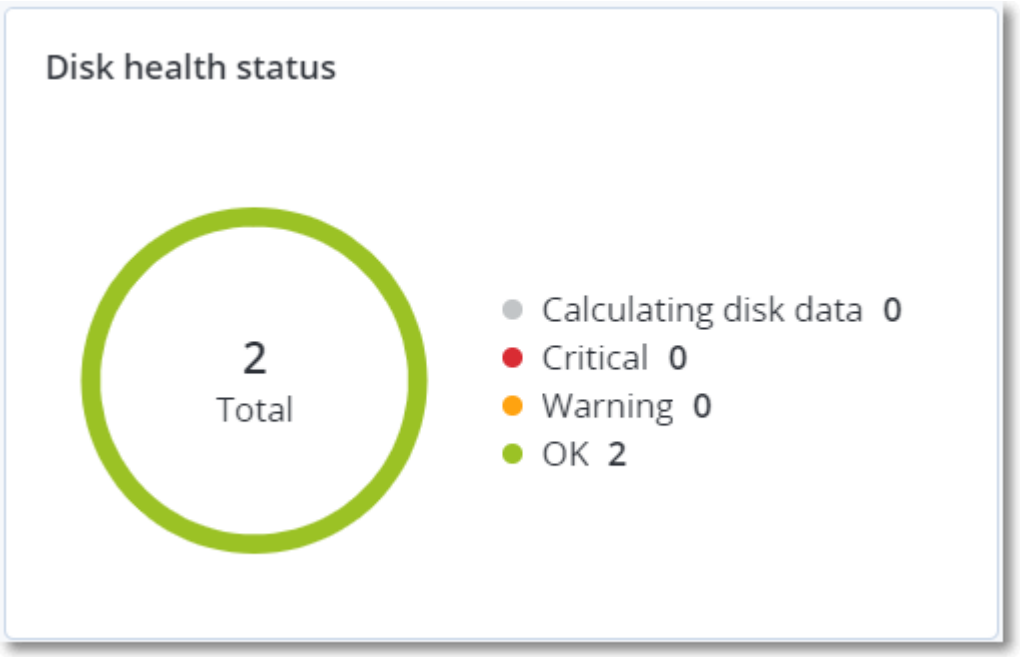
Les résultats de la surveillance de l'intégrité du disque sont présentés dans les widgets suivants, disponibles dans la console Web Cyber Protect.

- **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 machine
    Affiche des informations résumées concernant l'état du disque de tous les ordinateurs de l'unité d'organisation sélectionnée. Seul l'état de disque le plus critique est affiché. 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

- Sera amélioré

- **Intégrité du disque** est un widget de graphique circulaire qui affiche le nombre de disques pour chaque état.



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'état d'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 <nom du disque> 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 <nom du disque> sur cet ordinateur est dans un état critique, et risque fortement d'échouer très bientôt. Une sauvegarde d'image de ce disque n'est pas recommandée 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.

Carte de la protection des données

La fonctionnalité Carte de la protection des données vous permet de découvrir toutes les données qui ont une importance à vos yeux, et d'obtenir des informations détaillées concernant le nombre, la taille, l'emplacement et l'état de protection de tous les fichiers importants, le tout sous forme de carte proportionnelle dont vous pouvez faire varier l'échelle.

La taille de chaque bloc dépend du nombre total ou de la taille totale des fichiers importants qui appartiennent à une machine ou à une unité d'organisation.

Les fichiers peuvent présenter l'un des états de protection suivants :

- **Critique :** de 51 à 100 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Faible :** de 21 à 50 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Moyen :** de 1 à 20 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Élevé :** tous les fichiers présentant l'extension que vous avez spécifiée sont protégés (sauvegardés) pour la machine ou l'emplacement sélectionné.

Les résultats de l'examen de la protection des données sont disponibles sur le tableau de bord dans le widget Carte de la protection des données, un widget sous forme de carte proportionnelle, qui permet d'afficher des informations au niveau de l'ordinateur.

Passez le pointeur sur le bloc coloré pour afficher d'autres informations concernant le nombre de fichiers non protégés, ainsi que leur emplacement. Pour les protéger, cliquez sur **Protéger tous les fichiers**.

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

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.

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.

Résumé d'installation des correctifs

Ce widget affiche le résumé des correctifs par l'état de leur installation.

Historique d'installation des correctifs

Ce widget affiche des informations détaillées concernant les correctifs installés sur les ordinateurs.

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

Détails de l'analyse de la sauvegarde

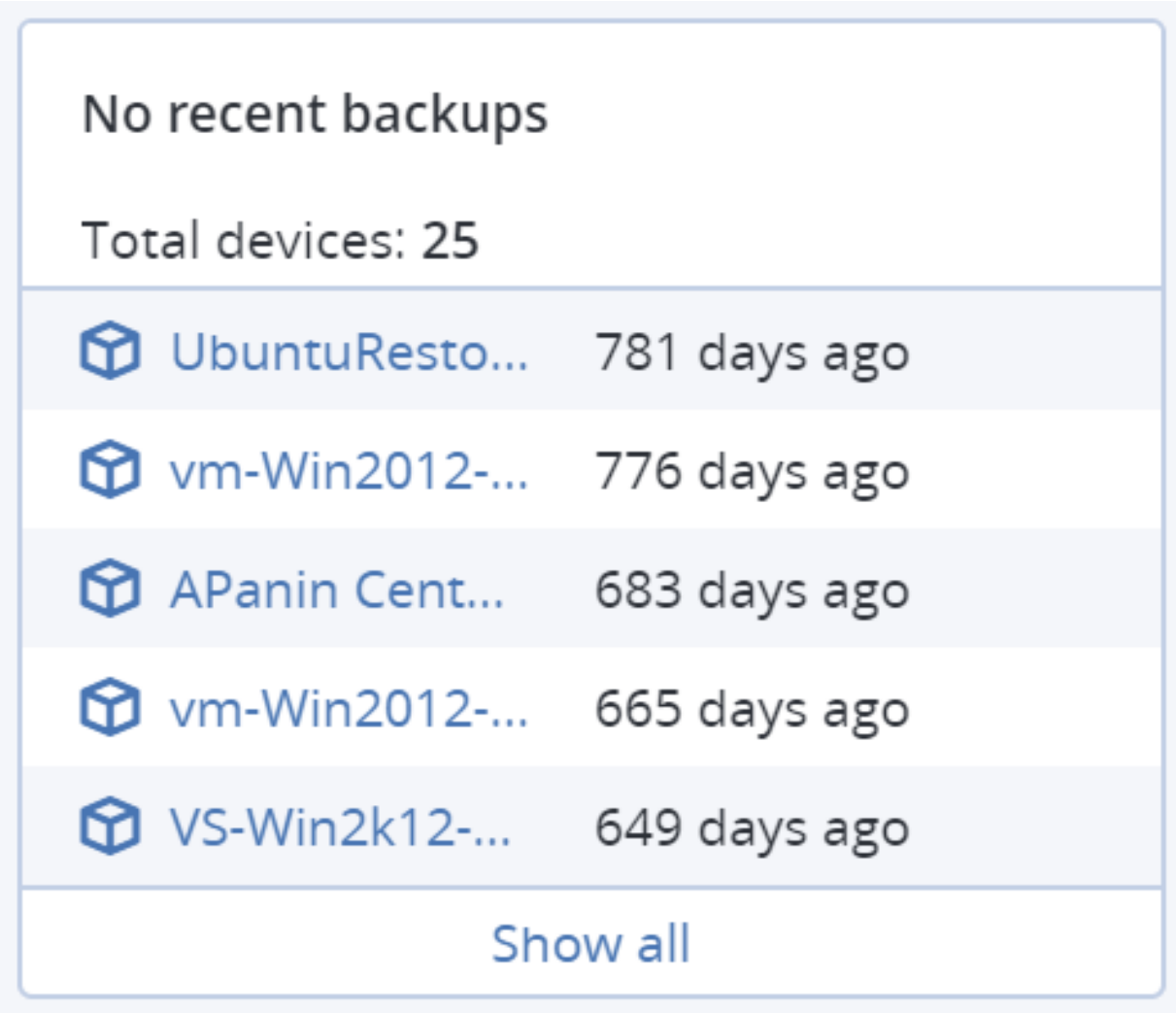
Ce widget est uniquement disponible si le service d'analyse est installé sur le serveur de gestion. Le widget affiche des informations détaillées concernant les menaces détectées dans les sauvegardes.

Affectés récemment

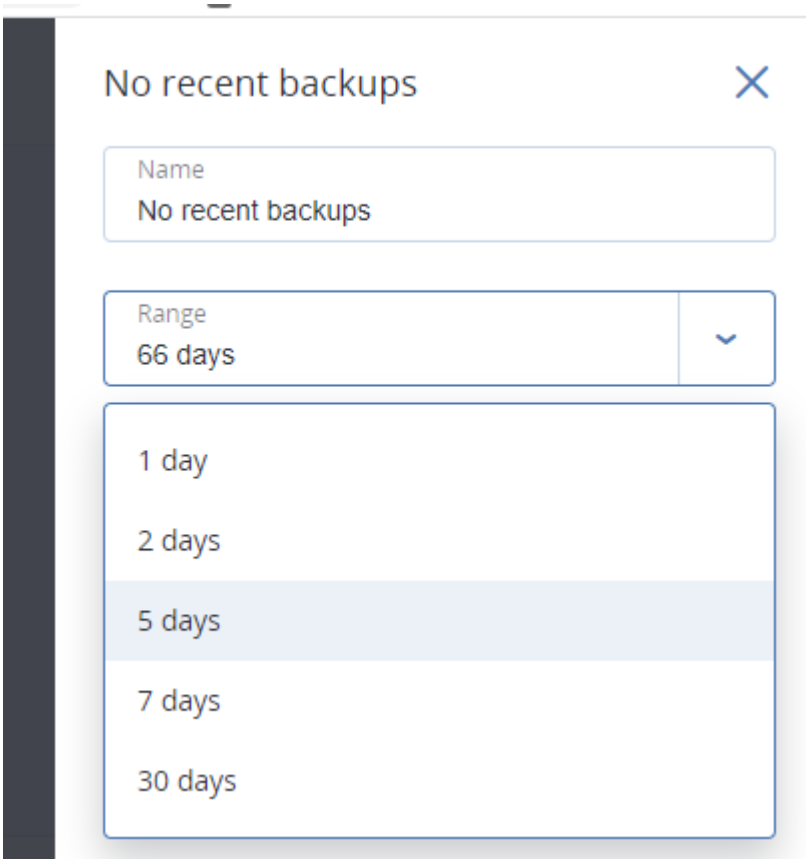
Ce widget affiche des informations détaillées concernant les ordinateurs infectés récemment. Vous y trouverez des informations concernant la menace détectée et le nombre de fichiers infectés.

Aucune sauvegarde récente

Ce widget montre les charges de travail auxquelles des plans de protection sont appliqués et dont la date de sauvegarde est antérieure à la plage de temps spécifiée dans les paramètres du widget.



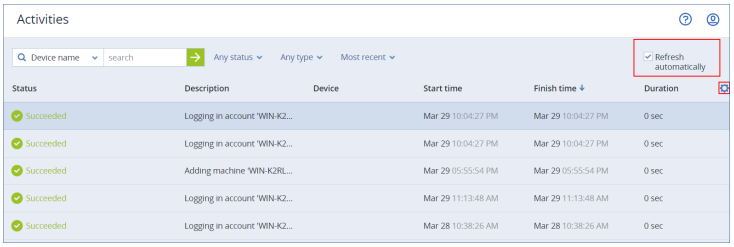
Par défaut, lorsque vous ajoutez ce widget, il affiche les informations des 5 derniers jours. Vous pouvez sélectionner une autre période à l'aide du menu déroulant ou entrer le nombre de jours manuellement. Le nombre maximum de jours que vous pouvez entrer est 180.



Onglet Activités

L'onglet **Activités** offre une vue d'ensemble des activités au cours des 90 derniers jours.

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**. Notez que la mise à jour fréquente de nombreuses activités peut dégrader les performances du serveur de gestion.



Vous pouvez effectuer une recherche parmi les activités répertoriées selon les critères suivants :

- **Nom du terminal**
  Nom de l'ordinateur sur lequel l'activité est exécutée.
- **Démarré par**
  Compte qui a démarré l'activité.

Vous pouvez également filtrer les activités selon les propriétés suivantes :

- **État**
  Par exemple, « A réussi », « A échoué », « En cours » ou « Annulé ».
- **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 modifier la période de rétention par défaut, modifiez le fichier de configuration task_manager.yaml.

Pour modifier la période de rétention

1. Sur la machine exécutant le serveur de gestion, ouvrez le fichier de configuration suivant dans un éditeur de texte :
   - Sous Windows : `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - Sous Linux : `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. Localisez la section suivante :

   ```
   database:
     connection-string: ""
     run-cleanup-at: "23:59"
     cleanup-batch-size: 10
     max-cleanup-retries: 10
     log-queries: false
     max-transaction-retries: 10
     shards:
      - connection-string: sqlite://task-manager.sqlite
        days-to-keep: 90
        space: "default"
        key: "00000000-0000-0000-0000-000000000000"
   ```

3. Modifiez la ligne `days-to-keep` (durée de rétention) comme vous le souhaitez.
   Par exemple :

   ```
   days-to-keep: 30
   ```

   Remarque
   Vous pouvez modifier la période de rétention en fonction de vos besoins. L'augmentation de la période de rétention a pour effet de dégrader les performances du serveur de gestion.

4. Redémarrez le service **Acronis Service Manager** comme décrit dans "Pour redémarrer le service Acronis Service Manager" (p. 204).

Rapports

Vous pouvez utiliser des rapports prédéfinis ou créer un rapport personnalisé. Un rapport peut inclure n'importe quel ensemble de widgets du tableau de bord.

Vous pouvez uniquement configurer des rapports pour les unités que vous gérez.

Les rapports peuvent être envoyés par courrier électronique ou téléchargés selon une planification. Pour envoyer les rapports par courrier électronique, assurez-vous que les paramètres du **Serveur de messagerie** sont configurés. Si vous voulez traiter un rapport en utilisant un logiciel tiers, planifiez la sauvegarde du rapport au format .xlsx dans un dossier spécifique.

Les rapports disponibles dépendent de l'édition de Cyber Protect. Les rapports par défaut sont répertoriés ci-dessous :

Nom du rapport	Disponibilité	Description
Alertes	Cyber Backup Advanced Cyber Protect Advanced	Affiche les alertes survenues pendant une période donnée.
Détails de l'analyse de la sauvegarde	Cyber Protect Advanced	Affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.
Sauvegardes	Cyber Backup Advanced Cyber Protect Advanced	Affiche les détails des sauvegardes et points de récupération actuels.
Statut actuel	Cyber Backup Advanced Cyber Protect Advanced	Affiche le statut actuel de votre environnement.
Activités quotidiennes	Cyber Backup Advanced Cyber Protect Advanced	Affiche un récapitulatif des activités réalisées pendant une période donnée.
Carte de la protection des données	Cyber Protect Advanced	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	Cyber Backup Advanced Cyber Protect Advanced	Affiche les détails des machines affectées en les classant par nombre de menaces bloquées, ainsi que des informations concernant les machines saines et vulnérables.
Machines découvertes	Cyber Backup Advanced Cyber Protect Advanced	Affiche toutes les machines qui ont été découvertes dans le réseau de l'organisation.
Prévision de l'état de santé du disque	Cyber Protect Advanced	Affiche des prévisions concernant le moment où votre disque dur/SSD tombera en panne, ainsi que l'état actuel des disques.

Vulnérabilités existantes	Cyber Backup Advanced Cyber Protect Advanced	Affiche les vulnérabilités existantes pour les systèmes d'exploitation et les applications dans votre environnement, ainsi que les ordinateurs affectés.
Licences	Cyber Backup Advanced Cyber Protect Advanced	Affiche un résumé des licences disponibles.
Emplacements	Cyber Backup Advanced Cyber Protect Advanced	Affiche les statistiques d'utilisation des emplacements de sauvegarde pendant une période donnée
Résumé de la gestion des correctifs	Cyber Protect Advanced	Affiche le nombre de correctifs manquants, installés et applicables. Vous pouvez explorer le rapport pour obtenir des informations sur les correctifs manquants/installés, ainsi que sur tous les systèmes.
Résumé	Cyber Backup Advanced Cyber Protect Advanced	Affiche un résumé des périphériques protégés pendant une période donnée.
Activités liées aux bandes	Cyber Backup Advanced Cyber Protect Advanced	Affiche la liste des bandes utilisées au cours des dernières 24 heures.
Activités hebdomadaires	Cyber Backup Advanced Cyber Protect Advanced	Affiche un récapitulatif des activités réalisées pendant une période donnée.

Opérations de base avec des rapports

- Pour afficher un rapport, cliquez sur son nom.
- Pour accéder aux autres opérations que vous pouvez effectuer avec un rapport, cliquez sur l'icône de points de suspension (...).

  Vous pouvez accéder aux mêmes informations au sein du rapport.

Pour ajouter un rapport

1. Cliquez sur **Ajouter un rapport**.
2. Effectuez l'une des actions suivantes :
   - Pour ajouter un rapport prédéfini, cliquez sur son nom.
   - Pour ajouter un rapport personnalisé, cliquez sur **Personnalisé**. Un nouveau rapport avec le nom **Personnalisé** est ajouté à la liste des rapports. Ouvrez ce rapport et ajoutez-y des widgets.
3. [Facultatif] Glissez-déplacez les widgets pour les réorganiser.
4. [Facultatif] Modifiez le rapport comme décrit ci-dessous.

Pour modifier un rapport

1. Cliquez sur l'icône en forme de points de suspension (...) située à côté du nom d'un rapport, puis cliquez sur **Paramètres**.
2. Modifiez le rapport. Vous pouvez :
   - Renommer le rapport
   - Modifier l'intervalle de temps pour tous les widgets présents dans le rapport
   - Planifier l'envoi du rapport par courrier électronique au format .pdf et/ou .xlsx.
3. Cliquez sur **Enregistrer**.

Pour planifier un rapport

1. Sélectionnez un rapport, puis cliquez sur **Planifier**.
2. Activez l'option **Envoyer un rapport planifié**.
3. Sélectionnez si vous souhaitez envoyer le rapport par courrier électronique, le sauvegarder dans un dossier ou les deux. En fonction de votre choix, indiquez les adresses électroniques, le chemin du dossier ou les deux.
4. Sélectionnez le format du rapport : .pdf, .xlsx ou les deux.
5. Sélectionnez la période du rapport : 1 jour, 7 jours ou 30 jours.
6. Sélectionnez les jours et l'heure auxquels le rapport sera envoyé ou sauvegardé.
7. Cliquez sur **Enregistrer**.

Exportation et importation de la structure des rapports

Vous pouvez exporter et importer la structure des rapports (ensemble de widgets et paramètres de planification) dans un fichier .json. Cela peut être utile en cas de réinstallation du serveur de gestion ou de copie de la structure des rapports vers un autre serveur de gestion.

Pour exporter la structure des rapports, sélectionnez-en un, puis cliquez sur **Exporter**.

Pour importer la structure des rapports, cliquez sur **Créer un rapport**, puis sur **Importer**.

Vidage mémoire des données du rapport

Vous pouvez sauvegarder un vidage mémoire des données du rapport dans un fichier .csv. Le vidage mémoire inclut toutes les données du rapport (sans filtrage) pour une plage de temps personnalisée.

Le logiciel génère le vidage mémoire des données à la volée. Si vous indiquez une plage de temps longue, cette action peut prendre plus de temps.

Pour vider les données du rapport

1. Sélectionnez un rapport, puis cliquez sur **Ouvrir**.
2. Cliquez sur l'icône en forme de points de suspension (...) dans l'angle supérieur droit, puis sur **Vider les données**.
3. Dans **Emplacement**, spécifiez le chemin du dossier pour le fichier .csv.

4. Dans **Plage de temps**, indiquez la plage de temps.
5. Cliquez sur **Enregistrer**.

Configuration de la gravité des alertes

Une alerte est un message qui avertit à propos de problèmes actuels ou potentiels. Vous pouvez les utiliser de différentes manières :

- La section **Alertes** de l'onglet **Présentation** vous permet de rapidement identifier et résoudre les problèmes en surveillant les alertes actuelles.
- Sous **Périphériques**, l'état des périphériques dérive des alertes. La colonne **État** vous permet de filtrer les périphériques qui posent problème.
- Lors de la configuration des notifications par e-mail, vous pouvez choisir les alertes qui déclencheront une notification.

Une alerte peut avoir l'un des niveaux de gravité suivants :

- **Critique**
- **Erreur**
- **Avertissement**

Vous pouvez modifier la gravité d'une alerte ou la désactiver complètement en utilisant le fichier de configuration des alertes comme décrit ci-dessous. Cette opération nécessite un redémarrage du serveur de gestion.

La modification de la gravité d'une alerte n'affecte pas les alertes déjà générées.

Fichier de configuration des alertes

Le fichier de configuration est situé sur la machine exécutant le serveur de gestion.

- Sous Windows : `<chemin d'installation>`**\AlertManager\alert_manager.yaml**
  Dans ce cas, `<installation_path>` est le chemin d'installation du serveur de gestion. Par défaut, il s'agit de **%ProgramFiles%\Acronis**.
- Sous Linux : **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

Le fichier est structuré comme un document YAML. Chaque alerte est un élément de votre liste `alertTypes`.

La clé `nom` identifie l'alerte.

La clé `gravité` définit la gravité de l'alerte. Il doit avoir l'une des valeurs suivantes : `critique`, `erreur` ou `avertissement`.

La clé facultative `activée` définit si l'alerte est activée ou désactivée. Sa valeur doit être `true` ou `false`. Par défaut (sans cette clé), toutes les alertes sont activées.

Pour modifier la gravité d'une alerte ou la désactiver

1. Sur la machine sur laquelle le serveur de gestion est installé, ouvrez le fichier **alert_manager.yaml** dans un éditeur de texte.
2. Localisez l'alerte que vous souhaitez modifier ou désactiver.
3. Effectuez l'une des actions suivantes :
   - Pour changer la gravité de l'alerte, modifiez la valeur de la clé `gravité`.
   - Pour désactiver l'alerte, ajoutez la clé `activée`, puis définissez sa valeur sur `false`.
4. Enregistrez le fichier.
5. Redémarrez le service du serveur de gestion comme décrit ci-dessous.

Pour redémarrer le service du serveur de gestion dans Windows

1. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis entrez : **cmd**.
2. Cliquez sur **OK**.
3. Exécutez les commandes suivantes :

```
net stop acrmngsrv
net start acrmngsrv
```

Pour redémarrer le service du serveur de gestion dans Linux

1. Ouvrir l'application **Terminal**.
2. Exécuter la commande suivante dans n'importe quel répertoire :

```
sudo service acronis_ams restart
```

Options de stockage avancées

Lecteurs de bandes

Les sections suivantes décrivent en détail la façon d'utiliser les lecteurs de bandes pour stocker les sauvegardes.

Qu'est-ce qu'un lecteur de bandes ?

Un **lecteur de bandes** est un terme générique qui signifie une bibliothèque de bandes ou un lecteur de bandes autonome.

Une **bibliothèque de bandes** (bibliothèque robotisée) est un périphérique de stockage à haute capacité qui contient les éléments suivants :

- un périphérique de bandes ou plus
- de multiples prises de connecteur (jusqu'à plusieurs milliers) pour contenir bandes
- un ou plusieurs changeurs (mécanismes robotisés) destinés à déplacer les bandes entre les prises de connecteur et les lecteurs de bandes.

Il peut également contenir d'autres éléments tels qu'un lecteurs de code-barres ou une imprimante de code-barres.

Un **autoloader** est un cas particulier d'une bibliothèque de bandes. Il contient un lecteur, plusieurs prises de connecteur, un changeur et un lecteur de code-barres (facultatif).

Un **lecteur de bandes autonome** (appelé également **gestionnaire de flux**) possède un logement et peut contenir une seule bande à la fois.

Aperçu de la prise en charge des bandes

Les agents de protection peuvent sauvegarder des données directement sur un lecteur de bandes ou via un nœud de stockage. Dans les deux cas, le fonctionnement automatique complet du lecteur de bandes est assuré. Lorsqu'un périphérique à bandes avec plusieurs lecteurs est connecté à un nœud de stockage, plusieurs agents peuvent effectuer des sauvegardes simultanées vers des bandes.

Compatibilité avec les logiciels GSA et tiers

Coexistence avec des logiciels tiers

Il n'est pas possible d'utiliser des bandes sur une machine sur laquelle est installé un logiciel tiers avec des outils de gestion de bandes propriétaires. Pour utiliser des bandes sur une telle machine, vous devez désinstaller ou désactiver le logiciel de gestion de bandes tiers.

Interaction avec le gestionnaire de stockage amovible (RSM) de Windows.

Les agents de protection et les nœuds de stockage n'utilisent pas RSM. Lors de la détection d'un périphérique à bandes, ils désactivent le lecteur de RSM (à moins qu'il ne soit en cours d'utilisation par un autre logiciel). Tant que vous voudrez utiliser le périphérique à bandes, assurez-vous que ni un logiciel d'utilisateur ni un logiciel tiers n'active le lecteur dans RSM. Si le lecteur de bandes était activé dans RSM, renouvelez la détection du lecteur de bande.

Matériel pris en charge

Acronis Cyber Protect prend en charge les terminaux SCSI externes. Ce sont des périphériques connectés à Fibre Channel ou qui utilisent les interfaces SCSI, iSCSI et Serial Attached SCSI (SAS). En outre, Acronis Cyber Protect prend en charge les lecteurs de bandes connectés via USB.

Dans Windows, Acronis Cyber Protect permet d'effectuer des sauvegardes sur un lecteur de bandes, même si les pilotes du changeur du terminal ne sont pas installés. Un tel périphérique à bandes est affiché dans le **Gestionnaire de périphériques** comme **Changeur de médias inconnu**. Toutefois, les pilotes pour les lecteurs du périphérique doivent être installés. Dans Linux et lors de l'utilisation d'un support de démarrage, la sauvegarde sur un périphérique à bandes sans pilote n'est pas possible.

La reconnaissance des périphériques IDE ou SATA connectés n'est pas garantie. Cela dépend si les pilotes appropriés sont installés ou non dans le système d'exploitation.

Pour savoir si votre terminal spécifique est pris en charge, utilisez l'outil de compatibilité matérielle comme décrit dans l'article http://kb.acronis.com/content/57237. Vous pouvez envoyer un rapport sur les résultats des tests à Acronis. Le matériel disposant d'une prise en charge confirmée est répertorié dans la liste de compatibilité matérielle : https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl.

Base de données de gestion des bandes

Les informations à propos de tous les périphériques à bandes attachés à une machine sont stockées dans la base de données de gestion des bandes. Le chemin de la base de données par défaut est le suivant :

- Sous Windows XP/Server 2003 : `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`.
- Sous Windows 7 et les versions ultérieures de Windows : `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`.
- Sous Linux : `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`.

La taille de la base de données dépend du nombre de sauvegardes stockées sur les bandes, et elle est approximativement égale à 10 Mo par centaine de sauvegardes. La base de données peut être volumineuse si la bibliothèque de bandes contient des milliers de sauvegardes. Dans ce cas, vous devriez stocker la base de données de bandes sur un volume différent.

Pour relocaliser la base de données sous Windows :

1. Arrêtez le service Removable Storage Management.
2. Déplacez tous les fichiers de l'emplacement par défaut vers le nouvel emplacement.
3. Trouvez la clé de la base de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`.
4. Spécifiez le chemin d'accès du nouvel emplacement dans la valeur de registre `ArsmDmlDbProtocol`. La chaîne peut contenir jusqu'à 32 765 caractères.
5. Démarrez le service Removable Storage Management.

Pour relocaliser la base de données sous Linux :

1. Arrêtez le service `acronis_rsm`.
2. Déplacez tous les fichiers de l'emplacement par défaut vers le nouvel emplacement.
3. Ouvrez le fichier de configuration `/etc/Acronis/ARSM.config` avec un éditeur de texte.
4. Localisez la ligne `<nom de la valeur="ArsmDmlDbProtocol" type="TString">`.
5. Modifiez le chemin d'accès sous cette ligne.
6. Enregistrez le fichier.
7. Démarrez le service `acronis_rsm`.

Le dossier `TapeLocation`

Le dossier `TapeLocation` contient un cache des métadonnées du système de fichiers de tous les volumes sauvegardés sur des bandes.

Le chemin d'accès par défaut au dossier `TapeLocation` est :

- Sous Windows XP/Server 2003 : `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`
- Sous Windows 7 et versions ultérieures : `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- Sous Linux : `/var/lib/Acronis/BackupAndRecovery/TapeLocation`

La taille du dossier `TapeLocation` est d'environ 0,5 à 1 % de la taille de toutes les sauvegardes stockées sur bande. Pour les sauvegardes de disque pour lesquelles l'option de restauration de fichiers est activée, il se peut que la taille du dossier `TapeLocation` soit un peu plus importante, en fonction du nombre de fichiers sauvegardés.

Paramètres d'écriture sur des bandes

Les paramètres d'écriture de bande (taille de bloc et de cache) vous permettent de régler le logiciel pour obtenir des performances optimales. Les deux paramètres sont nécessaires pour l'écriture sur des bandes, mais il suffit généralement de régler la taille des blocs. La valeur optimale dépend du type de périphérique à bandes et des données sauvegardées, comme le nombre de fichiers et leur taille.

Remarque
Lorsque le logiciel lit des données d'une bande, il utilise la même taille de bloc que lors de l'écriture sur la bande. Si le périphérique à bandes ne prend pas en charge cette taille de blocs, la lecture échoue.

Les paramètres sont définis sur chaque machine disposant d'un périphérique à bandes connecté. Cela peut être un ordinateur avec un nœud de stockage ou un agent. Sur un ordinateur Windows, la configuration s'effectue dans le registre ; sur un ordinateur Linux, cela s'effectue dans le fichier de configuration **/etc/Acronis/BackupAndRecovery.config**.

Dans Windows, créez les clés de registre respectives et leurs valeurs DWORD. Dans Linux, ajoutez le texte suivant à la fin du fichier de configuration, juste avant la balise `</registry>` :

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

La taille de bloc (en octets) utilisée lors de l'écriture sur des bandes.

Valeurs possibles : 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Si la valeur est 0 ou que le paramètre est absent, la taille de bloc est déterminée comme suit :

- Dans Windows, la valeur est obtenue du pilote de périphérique à bandes.
- Dans Linux, la valeur est de **64 Ko**.

Clé de registre (sur un ordinateur Windows) : **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

Ligne dans /etc/Acronis/BackupAndRecovery.config (sur un ordinateur Linux) :

```
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
```

Si la valeur fournie n'est pas acceptée par le lecteur de bandes, le logiciel la divise par deux jusqu'à atteindre la valeur applicable ou jusqu'à ce qu'elle atteigne 32 octets. Si la valeur applicable est introuvable, le logiciel multiplie la valeur spécifiée par deux jusqu'à atteindre la valeur applicable ou 1 Mo. Si aucune valeur n'est acceptée par le disque, la sauvegarde échoue.

WriteCacheSize

La taille de mémoire tampon (en octets) utilisée lors de l'écriture sur des bandes.

Valeurs possibles : 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, sans être inférieure à la valeur du paramètre **DefaultBlockSize**.

Si la valeur est 0 ou que le paramètre est absent, la taille du tampon est de **1 Mo**. Si le système d'exploitation ne prend pas en charge cette valeur, le logiciel la divise par deux jusqu'à ce que la valeur applicable soit trouvée ou que la valeur de paramètre **DefaultBlockSize** soit atteinte. Si la valeur prise en charge par le système d'exploitation est introuvable, la sauvegarde échoue.

Clé de registre (sur un ordinateur Windows) :
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Ligne dans /etc/Acronis/BackupAndRecovery.config (sur un ordinateur Linux) :

```
<value name="WriteCacheSize" type="Dword">
    "value"
</value>
```

Si vous spécifiez une valeur différente de zéro non prise en charge par le système d'exploitation, la sauvegarde échoue.

Options de sauvegarde liées aux bandes

Vous pouvez configurer les options de sauvegarde **Gestion des bande** pour déterminer :

- S'il faut activer la restauration de fichiers à partir de sauvegardes de niveau disque stockées sur bandes.
- Si vous devez renvoyer des bandes dans les logements une fois le plan de protection terminé.
- Si vous devez éjecter les bandes après l'achèvement de la sauvegarde.
- S'il faut utiliser une bande libre pour chaque sauvegarde complète.
- S'il faut écraser une bande lors de la création d'une sauvegarde complète (pour des lecteurs de bande autonomes uniquement).
- Si vous devez utiliser des ensembles de bandes pour différencier les bandes utilisées par exemple, pour des sauvegardes créées différents jours de la semaine ou pour des sauvegardes de différents types de machine.

Opérations parallèles

Acronis Cyber Protect peut simultanément effectuer des opérations avec les divers composants d'un lecteur de bandes. Pendant une opération qui utilise un lecteur (sauvegarde, restauration, nouvelle analyse ou effacement), vous pouvez lancer une opération qui utilise un changeur (déplacement d'une bande vers un autre logement ou éjection d'une bande) et vice versa. Si votre

bibliothèque de bandes possède plus d'un lecteur, vous pouvez également lancer une opération qui utilise un des lecteurs pendant une opération avec un autre. Par exemple, plusieurs machines peuvent sauvegarder ou restaurer simultanément en utilisant différents lecteurs de la même bibliothèque de bandes.

L'opération de détection des nouveaux lecteurs de bandes peut être exécutée simultanément à toute autre opération. Pendant la prise d'inventaire, aucune autre opération n'est disponible, sauf la détection des nouveaux lecteurs de bandes.

Les opérations que ne peuvent pas être exécutées en parallèle sont en mises en file d'attente.

Limites

L'utilisation du périphérique à bandes a les limites suivantes :

1. Les périphériques à bandes ne sont pas pris en charge lorsqu'une machine est démarrée à partir d'un support de démarrage Linux 32 bits.
2. Vous ne pouvez pas sauvegarder les types de données suivants sur des bandes : Boîtes aux lettres Microsoft 365, boîtes aux lettres Microsoft Exchange.
3. Vous ne pouvez pas créer de sauvegardes reconnaissant les applications pour des machines physiques et virtuelles.
4. Dans macOS, seule la sauvegarde de niveau fichier vers un emplacement basé sur bandes est prise en charge.
5. La consolidation des sauvegardes situées sur des bandes n'est pas possible. De ce fait, le modèle de sauvegarde **Toujours incrémentielle** est indisponible lorsque vous sauvegardez sur des bandes.
6. La déduplication des sauvegardes situées sur des bandes n'est pas possible.
7. Le logiciel ne peut pas écraser automatiquement une bande si celle-ci contient des sauvegardes non effacées ou s'il existe des sauvegardes dépendantes sur d'autres bandes.
   La seule exception à cette règle est lorsque l'option « Écraser une bande dans le lecteur autonome lors de la création d'une sauvegarde complète » est activée.
8. Vous ne pouvez pas restaurer sous un système d'exploitation à partir d'une sauvegarde stockée sur bandes si la restauration nécessite le redémarrage du système d'exploitation. Utilisez un support de démarrage pour effectuer cette restauration.
9. Vous pouvez valider n'importe quelle sauvegarde stockée sur des bandes, mais vous ne pouvez pas sélectionner pour validation un emplacement de stockage basé sur bandes ou un périphérique à bandes tout entier.
10. Un emplacement géré basé sur bandes ne peut pas être protégé par chiffrement. Chiffrez vos sauvegardes plutôt.
11. Le logiciel ne peut pas simultanément écrire une sauvegarde sur plusieurs bandes ou plusieurs sauvegardes en utilisant le même lecteur sur la même bande.
12. Les périphériques utilisant le Network Data Management Protocol (NDMP) ne sont pas pris en charge.

13. Les imprimantes de code-barres ne sont pas prises en charge.
14. Les bandes formatées Linear Tape File System (LTFS) ne sont pas prises en charge.

Lisibilité des bandes écrites par les anciens produits Acronis

Le tableau suivant résume la lisibilité des bandes écrites par les produits des gammes Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, 11.7 et 12.5 dans Acronis Cyber Protect. Le tableau représente également la compatibilité des bandes écrites par les divers composants d'Acronis Cyber Protect.

Vous pouvez ajouter des sauvegardes incrémentielles et différentielles aux sauvegardes réanalysées créées par Acronis Backup 11.5, 11.7 et 12.5.

	...est lisible sur un lecteur de bandes associé à un ordinateur avec...			
	Support de démarrage Acronis Cyber Protect	Agent Acronis Cyber Protect pour Windows	Agent Acronis Cyber Protect pour Linux	Agent Acronis Cyber Protect pour Storage Node

Bande écrite sur un lecteur de bandes localement attaché (lecteur ou bibliothèque de bandes) par...	Support de démarrage	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Sauvegarde 11.5/11.7/12.5	+	+	+	-
	Agent pour Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Sauvegarde 11.5/11.7/12.5	+	+	+	-
	Agent pour Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Sauvegarde 11.5/11.7/12.5	+	+	+	-
Bande écrite sur un lecteur de bandes à travers...	Serveur de sauvegarde	9.1	-	-	-	-
		Echo	-	-	-	-
		ABR10	+	+	+	+
	Nœud de stockage	ABR11/ Acronis Sauvegarde 11.5/11.7/12.5	+	+	+	+

Prise en main avec un lecteur de bandes

Sauvegarde d'une machine sur un périphérique à bandes connecté localement

Prérequis

- Le lecteur de bandes est attaché à la machine conformément aux instructions du fabricant.
- L'agent de protection est installé sur l'ordinateur.

Avant la sauvegarde

1. Chargez les bandes dans le lecteur de bandes.
2. Connectez-vous à la console Web Cyber Protect.
3. Dans **Paramètres** > **Gestion des bandes**, développez le nœud de la machine, puis cliquez sur **Périphériques à bandes**.
4. Assurez-vous que le périphérique à bandes connecté est affiché. S'il ne l'est pas, cliquez sur **Détecter des périphériques**.
5. Effectuez l'inventaire de bande :
   a. Cliquez sur le nom du périphérique à bandes.
   b. Cliquez sur **Inventaire** pour détecter les bandes chargées. Laissez **Inventaire complet** activé. N'activez pas **Déplacer les bandes non reconnues ou importées vers le pool « bandes libres »**. Cliquez sur **Démarrer l'inventaire maintenant**.
   Résultat. Les bandes chargées ont été déplacées vers les pools appropriés tel que spécifié dans la section « Prise d'inventaire ».

   Remarque
   La prise d'inventaire complète d'un périphérique à bandes intégral peut prendre beaucoup de temps.

   c. Si les bandes chargées ont été envoyées vers le pool des **Bandes non reconnues** ou des **Bandes importées** et que vous voulez les utiliser pour la sauvegarde, déplacez ces bandes vers le pool des **Bandes libres** manuellement.

   Remarque
   Les bandes envoyées au pool **Bandes importées** contiennent des sauvegardes réalisées par le logiciel Acronis. Avant de déplacer ces bandes vers le pool des **Bandes libres**, assurez-vous que vous n'avez pas besoin de ces sauvegardes.

Sauvegarde

Créez un plan de protection comme décrit dans la section Sauvegarde. Lorsque vous spécifiez l'emplacement de sauvegarde, sélectionnez **Pool de bandes « Acronis »**.

Résultats

- Pour accéder à l'emplacement où les sauvegardes seront créées, cliquez sur **Stockage de sauvegarde** > **Pool de bandes « Acronis »**.
- Les bandes avec les sauvegardes seront déplacées vers le pool **Acronis**.

Sauvegarde vers un lecteur de bandes attaché à un nœud de stockage

Prérequis

- Un nœud de stockage est enregistré sur le serveur de gestion.
- Le lecteur de bandes est attaché au nœud de stockage conformément aux instructions du fabricant.

Avant la sauvegarde

1. Chargez les bandes dans le lecteur de bandes.
2. Connectez-vous à la console Web Cyber Protect.
3. Cliquez sur **Paramètres** > **Gestion des bandes**, développez le nœud portant le nom du nœud de stockage, puis cliquez sur **Périphériques à bandes**.
4. Assurez-vous que le périphérique à bandes connecté est affiché. S'il ne l'est pas, cliquez sur **Détecter des périphériques**.
5. Effectuez l'inventaire de bande :
   a. Cliquez sur le nom du périphérique à bandes.
   b. Cliquez sur **Inventaire** pour détecter les bandes chargées. Laissez **Inventaire complet** activé. N'activez pas **Déplacer les bandes non reconnues ou importées vers le pool « bandes libres »**. Cliquez sur **Démarrer l'inventaire maintenant**.
   Résultat. Les bandes chargées ont été déplacées vers les pools appropriés tel que spécifié dans la section « Prise d'inventaire ».

   Remarque
   La prise d'inventaire complète d'un périphérique à bandes intégral peut prendre beaucoup de temps.

   c. Si les bandes chargées ont été envoyées vers le pool des **Bandes non reconnues** ou des **Bandes importées** et que vous voulez les utiliser pour la sauvegarde, déplacez ces bandes vers le pool des **Bandes libres** manuellement.

Remarque
Les bandes envoyées au pool **Bandes importées** contiennent des sauvegardes réalisées par le logiciel Acronis. Avant de déplacer ces bandes vers le pool des **Bandes libres**, assurez-vous que vous n'avez pas besoin de ces sauvegardes.

d. Décidez si vous souhaitez sauvegarder dans le **pool** Acronis ou créer un nouveau pool.
Détails. Avoir plusieurs pools vous permet d'utiliser un jeu de bandes distinct pour chaque machine ou chaque service de votre entreprise. En utilisant plusieurs pools, vous pouvez empêcher que des sauvegardes créées par différents plans de protection se mélangent sur une seule bande.

e. Si le pool sélectionné est autorisé à prendre des bandes à partir du pool de **Bandes libres** lorsque cela est nécessaire, ignorez cette étape.
Autrement, déplacez les bandes à partir du pool **Bandes libres** vers le pool sélectionné.
Conseil. Pour savoir si un pool peut prendre des bandes à partir du pool **Bandes libres**, cliquez sur le pool, puis cliquez sur **Infos**.

Sauvegarde

Créez un plan de protection comme décrit dans la section Sauvegarde. Lorsque vous spécifiez l'emplacement de la sauvegarde, sélectionnez le pool de bandes créé.

Résultats

- Pour accéder à l'emplacement où les sauvegardes seront créées, cliquez sur **Sauvegardes**, puis sur le nom du pool de bandes créé.
- Les bandes avec les sauvegardes seront déplacées vers le pool sélectionné.

Conseils pour d'autres utilisations de la bibliothèque de bandes

- Vous n'avez pas à exécuter une prise d'inventaire complète chaque fois que vous chargez une nouvelle bande. Pour gagner du temps, suivez la procédure décrite dans la section « Prise d'inventaire » sous « Combinaison de la prise d'inventaire rapide et complète ».
- Vous pouvez créer d'autres pools sur la même bibliothèque de bandes et sélectionner n'importe lequel d'entre eux comme destination pour les sauvegardes.

Restauration sous un système d'exploitation à partir d'un lecteur de bandes

Pour restaurer sous un système d'exploitation à partir d'un lecteur de bandes :

1. Connectez-vous à la console Web Cyber Protect.
2. Cliquez sur **Périphériques**, puis sélectionnez la machine sauvegardée.
3. Cliquez sur **Restauration**.
4. Sélectionnez un point de restauration. Vous remarquerez que les points de restauration sont filtrés en fonction de leur emplacement.

5. Le logiciel affiche la liste des bandes requises pour la restauration. Les bandes manquantes sont grisées. Si votre périphérique à bandes a des prises de connecteur libres, chargez ces bandes dans le périphérique.
6. Configurez les autres paramètres de restauration.
7. Cliquez sur **Démarrer la récupération** pour lancer l'opération de récupération.
8. Si une des bandes requises n'est pas chargée pour n'importe quelle raison, le logiciel vous affiche un message avec les identifiants de la bande requise. Faites ce qui suit :
   a. Chargez la bande.
   b. Effectuez la prise d'inventaire rapide.
   c. Cliquez sur **Présentation** > **Activités**, puis sur l'activité de récupération avec l'état **Intervention requise**.
   d. Cliquez sur **Afficher les détails**, puis sur **Réessayer** pour poursuivre la restauration.

Que se passe-t-il si je ne vois aucune sauvegarde stockée sur des bandes ?

Cela signifie probablement que la base de données avec le contenu des bandes est perdue ou endommagée pour une raison quelconque.

Pour restaurer la base de données, procédez comme suit :

1. Effectuez la prise d'inventaire rapide.

   Avertissement !
   Durant l'opération d'inventaire, *n'activez pas* l'option **« Déplacer les bandes non reconnues et importées vers le pool de "Bandes libres" »**. Si l'option est activée, vous pouvez perdre toutes vos sauvegardes.

2. Ré-analysez le pool **Bandes non reconnues**. Par conséquent, vous obtiendrez le contenu du (des) lecteur(s) chargé(s).
3. Si l'une des sauvegardes détectées se poursuit sur d'autres bandes qui n'ont pas encore été ré-analysées, vous êtes invité à charger ces bandes et à les ré-analyser.

La restauration sous le support de démarrage à partir d'un périphérique à bandes connecté localement.

Pour restaurer sous le support de démarrage à partir d'un périphérique à bandes connecté localement.

1. Chargez la(les) bande(s) requise(s) pour la restauration dans le périphérique à bandes.
2. Démarrez la machine à partir du support de démarrage.
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 le périphérique à bandes est connecté à l'aide de l'interface iSCSI, configurez le périphérique comme décrit dans « Configuration des périphériques iSCSI et NDAS ».

5. Cliquez sur **Gestion des bandes**.
6. Cliquez sur **Inventaire**.
7. Dans **Objets à inventorier**, sélectionnez le périphérique à bandes.
8. Cliquez sur **Démarrer** pour démarrer la prise d'inventaire.
9. Après la fin de l'inventaire, cliquez sur **Fermer**.
10. Cliquez sur **Actions** > **Restaurer**.
11. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
12. Développez **Périphériques à bandes**, puis sélectionnez le périphérique nécessaire. Le système invite à confirmer la ré-analyse. Cliquez sur **Oui**.
13. Sélectionnez le pool **Bandes non reconnues**.
14. Sélectionnez les bandes à analyser de nouveau. Pour sélectionner toutes les bandes du pool, activez la case près de l'en-tête de colonne **Nom de la bande**.
15. Si les bandes contiennent une sauvegarde protégée par un mot de passe, sélectionnez la case à cocher correspondante, puis indiquez le mot de passe pour la sauvegarde dans le champ **Mot de passe**. Si vous n'indiquez pas de mot de passe, ou si le mot de passe est incorrect, la sauvegarde ne sera pas détectée. Veuillez garder cela à l'esprit dans le cas où vous ne verriez pas de sauvegardes après la nouvelle analyse.

    Conseil. Si les bandes contiennent des sauvegardes protégées par différents mots de passe, vous devrez répéter la nouvelle analyse plusieurs fois en spécifiant chaque mot de passe.
16. Cliquez sur **Démarrer** pour démarrer la ré-analyse. Par conséquent, vous obtiendrez le contenu du(des) lecteur(s) chargé(s).
17. Si l'une des sauvegardes détectées se poursuit sur d'autres bandes qui n'ont pas encore été ré-analysées, vous êtes invité à charger ces bandes et à les ré-analyser.
18. Cliquez sur **OK** une fois la nouvelle analyse terminée.
19. Dans la **Vue d'archive**, sélectionnez la sauvegarde dont il faut restaurer les données, puis sélectionnez les données que vous voulez restaurer. Après avoir cliqué sur **OK**, la page **Récupérer des données** vous indiquera la liste de bandes nécessaires pour la restauration. Les bandes manquantes sont grisées. Si votre périphérique à bandes a des prises de connecteur libres, chargez ces bandes dans le périphérique.
20. Configurez les autres paramètres de restauration.
21. Cliquez sur **OK** pour démarrer la restauration.
22. Si une des bandes requises n'est pas chargée pour n'importe quelle raison, le logiciel vous affiche un message avec les identifiants de la bande requise. Faites ce qui suit :
    a. Chargez la bande.
    b. Effectuez la prise d'inventaire rapide.
    c. Cliquez sur **Présentation** > **Activités**, puis sur l'activité de récupération avec l'état **Intervention requise**.
    d. Cliquez sur **Afficher les détails**, puis sur **Réessayer** pour poursuivre la restauration.

Restauration sous un support de démarrage à partir d'un lecteur de bandes relié à un nœud de stockage

Pour restaurer sous un support de démarrage à partir d'un lecteur de bandes relié à un nœud de stockage :

1. Chargez la(les) bande(s) requise(s) pour la restauration dans le périphérique à bandes.
2. Démarrez la machine à partir du support de démarrage.
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. Cliquez sur **Restaurer**.
5. Cliquez sur **Sélectionner des données**, puis cliquez sur **Parcourir**.
6. Dans la zone **Chemin d'accès**, tapez `bsp://<adresse du nœud de stockage><nom du pool>/`, où `<adresse du nœud de stockage>` est l'adresse IP du nœud de stockage qui contient la sauvegarde nécessaire et `<nom du pool>` est le nom du pool de bandes. Cliquez sur **OK** et indiquez les accréditations pour le pool.
7. Sélectionnez la sauvegarde, puis sélectionnez les données que vous voulez restaurer. Après avoir cliqué sur **OK**, la page **Récupérer des données** vous indiquera la liste de bandes nécessaires pour la restauration. Les bandes manquantes sont grisées. Si votre périphérique à bandes a des prises de connecteur libres, chargez ces bandes dans le périphérique.
8. Configurez les autres paramètres de restauration.
9. Cliquez sur **OK** pour démarrer la restauration.
10. Si une des bandes requises n'est pas chargée pour n'importe quelle raison, le logiciel vous affiche un message avec les identifiants de la bande requise. Faites ce qui suit :
    a. Chargez la bande.
    b. Effectuez la prise d'inventaire rapide.
    c. Cliquez sur **Présentation** > **Activités**, puis sur l'activité de récupération avec l'état **Intervention requise**.
    d. Cliquez sur **Afficher les détails**, puis sur **Réessayer** pour poursuivre la restauration.

Gestion des bandes

Détection des lecteurs de bandes

Lors de la détection des lecteurs de bandes, le logiciel de sauvegarde trouve des lecteurs de bande connectés à la machine et place les informations les concernant dans la base de données de gestion des bandes. Les périphériques à bandes détectés sont désactivés du gestionnaire de stockage amovible (RSM).

En général, un périphérique à bandes est détecté automatiquement dès qu'il est connecté à une machine sur laquelle le produit est installé. Cependant, vous pourriez avoir besoin de détecter les périphériques à bandes dans l'un des cas suivants :

- Après avoir attaché ou rattaché un lecteur de bandes.
- Après avoir installé ou réinstallé le logiciel de sauvegarde sur l'ordinateur auquel un lecteur de bandes est attaché.

Pour détecter les lecteurs de bandes

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine à laquelle le périphérique à bandes est connecté.
3. Cliquez sur **Détecter des périphériques**. Vous verrez les périphériques à bandes connectés, leurs lecteurs et leurs emplacements.

Pools de bandes

Le logiciel de sauvegarde utilise les pools de bandes qui sont des groupes logiques ou des bandes. Le logiciel contient les pools de bandes prédéfinies suivantes : **Bandes non reconnues**, **Bandes importées**, **Bandes libres** et **Acronis**. Vous pouvez également créer vos propres pools personnalisés.

Le pool **Acronis** et le pool personnalisé sont également utilisés en tant qu'emplacements de sauvegarde.

Pools prédéfinis

Bandes non reconnues

Le pool contient des bandes qui ont été écrites par des applications tierces. Pour pouvoir écrire sur ces bandes, vous devez les déplacer explicitement vers le pool de **Bandes libres**. Vous ne pouvez pas déplacer des bandes à partir de ce pool vers tout autre pool, sauf le pool de **Bandes libres**.

Bandes importées

Le pool contient des bandes qui ont été écrites par Acronis Cyber Protect dans un lecteur de bandes connecté à un autre nœud de stockage ou agent. Pour pouvoir écrire sur ces bandes, vous devez les déplacer explicitement vers le pool de **Bandes libres**. Vous ne pouvez pas déplacer des bandes à partir de ce pool vers tout autre pool, sauf le pool de **Bandes libres**.

Bandes libres

Le pool contient des bandes libres (vides). Vous pouvez déplacer manuellement des bandes vers ce pool à partir d'autres pools.

Quand vous déplacez une bande vers le pool **Bandes libres**, le logiciel la marque comme vide. Si la bande contient des sauvegardes, elles sont marquées de l'icône  . Lorsque le logiciel commence à écraser la bande, les données liées aux sauvegardes sont supprimées de la base de données.

Acronis

Le pool est utilisé pour la sauvegarde par défaut, quand vous ne voulez pas créer vos propres pools. Il s'applique habituellement à un lecteur de bandes avec une petite quantité de bandes.

Pools personnalisés

Vous devez créer plusieurs pools si vous voulez dissocier les sauvegardes de données différentes. Par exemple, il se peut que vous vouliez créer des pools personnalisés afin de dissocier :

- les sauvegardes de différents services de votre entreprise
- les sauvegardes de machines différentes
- les sauvegardes de volumes système et de données utilisateur.

Opérations avec les pools

Création d'un pool

Pour créer un pool :

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur **Créer un pool**.
4. Spécifiez le nom du pool.
5. [Facultatif] Désactivez la case **Prendre les bandes à partir du pool Bandes libres automatiquement...**. Si la case est désactivée, seules les bandes qui sont incluses dans le nouveau pool à un certain moment seront utilisées pour la sauvegarde.
6. Cliquez sur **Créer**.

Modification d'un pool

Vous pouvez modifier les paramètres du pool **Acronis** ou de votre propre pool personnalisé.

Pour modifier un pool :

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Sélectionnez le pool requis, puis cliquez sur **Éditer le pool**.
4. Vous pouvez modifier le nom du pool ou les paramètres. Pour plus d'informations à propos des paramètres de pool, consultez la section « Création d'un pool ».
5. Cliquez sur **Enregistrer** pour enregistrer les modifications.

Suppression d'un pool

Vous pouvez supprimer seulement les pools personnalisés. Les pools de bandes prédéfinis (**Bandes non reconnues**, **Bandes importées**, **Bandes libres** et **Acronis**) ne peuvent pas être supprimés.

Remarque
Après suppression d'un pool, n'oubliez pas de modifier les plans de protection ayant le pool comme emplacement de sauvegarde. Sinon, ces plans de protection échoueront.

Pour supprimer un pool :

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Sélectionnez le pool requis et cliquez sur **Supprimer**.
4. Sélectionnez le pool vers lequel les bandes du pool en cours de suppression seront déplacées après la suppression.
5. Cliquez sur **OK** pour supprimer le pool.

Opérations sur les bandes

Déplacement vers une autre prise de connecteur

Utilisez cette opération dans les situations suivantes :

- Vous devez éjecter plusieurs bandes d'un lecteur de bandes simultanément.
- Votre lecteur de bandes ne possède pas de prise de connecteur de courrier électronique et les bandes à éjecter sont situées dans des magasins de prises de connecteur non amovibles.

Vous devez déplacer les bandes une par une vers des prises de connecteurs d'un magasin de prises de connecteur, puis éjecter le magasin manuellement.

Pour déplacer une bande vers une autre prise de connecteur

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient la bande nécessaire, puis sélectionnez la bande requise.
4. Cliquez sur **Déplacer vers le logement**.
5. Sélectionnez une nouvelle prise de connecteur vers laquelle déplacer la bandes sélectionnée.
6. Cliquez sur **Déplacer** pour démarrer l'opération.

Déplacement vers un autre pool

L'opération vous permet de déplacer une ou plusieurs bandes d'un pool à l'autre.

Quand vous déplacez une bande vers le pool **Bandes libres**, le logiciel la marque comme vide. Si la bande contient des sauvegardes, elles sont marquées de l'icône  . Lorsque le logiciel commence à écraser la bande, les données liées aux sauvegardes sont supprimées de la base de données.

Remarques à propos des types spécifiques de bandes

- Vous ne pouvez pas déplacer des bandes protégées en écriture et des bandes WORM (Write-Once-Read-Many) déjà enregistrées vers le pool **Bandes libres**.
- Les bandes de nettoyage sont toujours affichées dans le pool **Bandes non reconnues** ; vous ne pouvez pas les déplacer vers un autre pool.

Pour déplacer des bandes vers un autre pool

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient les bandes nécessaires, et ensuite sélectionnez les bandes requises.
4. Cliquez sur **Déplacer vers le pool**.
5. [Facultatif] Cliquez sur **Créer un nouveau pool** si vous voulez créer un autre pool pour les bandes sélectionnées. Exécutez les actions décrites dans la section « Création d'un pool ».
6. Sélectionnez le pool vers lequel déplacer les bandes.
7. Cliquez sur **Déplacer** pour enregistrer les modifications.

Remarque
Si vous possédez des sauvegardes récupérables sur la bande et que vous la déplacez vers un autre pool, assurez-vous de réactualiser l'emplacement de stockage sous le stockage de sauvegarde une fois l'opération de déplacement terminée. Les sauvegardes seront disponibles dans le second pool, quelle que soit la destination de sauvegarde d'origine.

Prise d'inventaire

L'opération de prise d'inventaire détecte les bandes chargées dans un périphérique à bandes et attribue des noms à celles qui n'ont ont pas.

Méthodes de prise d'inventaire

Il existe deux méthodes d'inventaire :

Prise d'inventaire rapide

L'agent ou le nœud de stockage analyse les bandes pour trouver les codes-barres. En utilisant les codes-barres, le logiciel peut rapidement retourner une bande vers le pool dans lequel elle était précédemment.

Sélectionnez cette méthode pour reconnaître les bandes utilisées par le même périphérique à bandes attaché à la même machine. Les autres bandes seront envoyées dans le pool **Bandes non reconnues**.

Si votre bibliothèque de bandes ne contient aucun lecteur de code-barres, toutes les bandes seront envoyées dans le pool **Bandes non reconnues**. Pour reconnaître vos bandes, effectuez une prise d'inventaire complète ou combinez une prise d'inventaire rapide et complète tel que décrit plus loin dans cette section.

Prise d'inventaire complète

L'agent ou le nœud de stockage lit les étiquettes écrites et analyse les autres informations relatives au contenu des bandes chargées. Sélectionnez cette méthode pour reconnaître les bandes vides et les bandes écrites par le même logiciel sur n'importe quel périphérique à bandes et n'importe quelle machine.

Le tableau suivant montre les pools vers lesquels les bandes sont envoyées à la suite de la prise d'inventaire complète.

La bande a été utilisée par...	La bande est lue par...	La bande est envoyée vers le pool...
Agent	Le même agent	À l'endroit où était la bande avant
	Un autre agent	**Bandes importées**
	Nœud de stockage	**Bandes importées**
Nœud de stockage	Le même nœud de stockage	À l'endroit où était la bande avant
	Un autre nœud de stockage	**Bandes importées**
	Agent	**Bandes importées**
Application de sauvegarde tierce	Agent ou nœud de stockage	**Bandes non reconnues**

Les bandes de certains types sont envoyées vers des pools spécifiques :

Type de bande	La bande est envoyée vers le pool...
Bande vide	**Bandes libres**
Bande vide protégée en écriture	**Bandes non reconnues**
Bande de nettoyage	**Bandes non reconnues**

La prise d'inventaire rapide peut être appliquée à des périphériques à bandes entiers. La prise d'inventaire complète peut être appliquée à des périphériques à bandes entiers, des lecteurs individuels ou des prises de connecteur. Pour un lecteur de bandes autonome, la prise d'inventaire complète est effectuée, même si vous avez sélectionné la prise d'inventaire rapide.

Combinaison des prises d'inventaire rapide et complète

La prise d'inventaire complète d'un périphérique à bandes intégral peut prendre beaucoup de temps. Si vous avez besoin de prendre l'inventaire de seulement quelques bandes, procédez comme suit :

1. Effectuez la prise d'inventaire rapide du périphérique à bandes.
2. Cliquez sur le pool **Bandes non reconnues**. Trouvez les bandes dont vous voulez prendre l'inventaire et prenez en note quelles prises de connecteur elles occupent.
3. Exécutez la prise d'inventaire complète de ces prises de connecteur.

Quoi faire après la prise d'inventaire

Si vous voulez sauvegarder les bandes qui ont été placées dans le pool **Bandes non reconnues** ou **Bandes importées**, déplacez-les dans le pool **Bandes libres**, puis dans le pool **Acronis** ou un pool personnalisé. Si le pool vers lequel vous voulez sauvegarder est réapprovisionnable, vous pouvez laisser les bandes dans le pool **Bandes libres**.

Si vous voulez effectuer une restauration à partir d'une bande qui a été placée dans le pool **Bandes non reconnues** ou **Bandes importées**, vous devez la réanalyser. La bande sera déplacée dans le pool sélectionné pendant la nouvelle analyse et les sauvegardes stockées sur la bande apparaîtront dans l'emplacement de stockage.

Séquence d'actions

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine à laquelle le périphérique à bandes est relié, puis le périphérique à bandes dont vous voulez faire l'inventaire.
3. Cliquez sur **Inventaire**.
4. [Facultatif] Pour sélectionner la prise d'inventaire rapide, désactivez **Inventaire complet**.
5. [Facultatif] Activez **Déplacer les bandes non reconnues et importées vers le pool de « bandes libres »**.

   Avertissement !
   Utilisez ce paramètre seulement si vous êtes absolument sûr que les données stockées sur vos bandes peuvent être écrasées.

6. Cliquez sur **Démarrer l'inventaire maintenant** pour commencer l'inventaire.

Ré-analyser

Les informations à propos du contenu des bandes sont stockées dans une base de données dédiée. L'opération de ré-analyse lit le contenu des bandes et met à jour la base de données si les informations qu'elle contient ne correspond pas aux données stockées sur les bandes. Les sauvegardes détectées suite à cette opération sont placées dans le pool spécifié.

En une opération, vous pouvez ré-analyser les bandes d'un pool. Seules les bandes en ligne peuvent être sélectionnées pour l'opération.

Pour réanalyser des bandes avec une sauvegarde multiflux ou avec une sauvegarde multiflux et multiplexée, vous avez besoin du même nombre de lecteurs que le nombre de lecteurs utilisés pour créer cette sauvegarde. Une telle sauvegarde ne peut pas être réanalysée via un lecteur de bandes autonome.

Exécution de la ré-analyse :

- Si la base de données d'un nœud de stockage ou une machine gérée est perdue ou endommagée.
- Si les informations sur une bande dans la base de données est périmée (par exemple, le contenu d'une bande a été modifié par un autre nœud de stockage ou un autre agent).
- Pour obtenir l'accès aux sauvegardes stockées sur les bandes lors du fonctionnement avec un support de démarrage.
- Si vous avez retiré par erreur les informations d'une bande à partir de la base de données. Lorsque vous ré-analysez une bande retirée, les sauvegardes qui y sont stockées réapparaissent dans la base de données et sont disponibles pour la restauration de données.
- Si les sauvegardes ont été supprimées d'une bande manuellement ou via les règles de rétention, mais vous voulez qu'elles deviennent accessibles pour la restauration de données. Avant de ré-analyser une telle bande, éjectez-la, supprimez ses informations de la base de données puis insérez la bande dans le périphérique à bandes de nouveau.

Pour réanalyser des bandes

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Périphériques à bandes**.
3. Sélectionnez le périphérique à bandes dans lequel vous avez chargé les bandes.
4. Effectuez la prise d'inventaire rapide.

> **Remarque**
> Lors de l'inventaire, *n'activez pas* l'option **Déplacer les bandes non reconnues et importées vers le pool de bandes libres**.

5. Sélectionnez le pool **Bandes non reconnues**. Il s'agit du pool vers lequel la plupart des bandes sont envoyées à la suite de la prise d'inventaire rapide. La nouvelle analyse de tout autre pool est également possible.
6. [Facultatif] Pour ré-analyser uniquement des bandes individuelles, sélectionnez-les.
7. Cliquez sur **Ré-analyser**.
8. Sélectionnez le pool dans lequel les archives de sauvegarde nouvellement détectées seront placées.
9. Si nécessaire, cochez la case **Activer la restauration de fichiers à partir de sauvegardes de disque stockées sur bandes**.

   Détails. Si la case est cochée, le logiciel crée des fichiers supplémentaires spéciaux sur un disque dur de la machine à laquelle le périphérique à bandes est attaché. La restauration des fichiers à partir de sauvegardes de disques est possible tant que ces fichiers supplémentaires sont intacts. Assurez-vous de cocher cette case si les bandes contiennent des sauvegardes reconnaissant les applications. Sinon, vous ne pourrez pas restaurer les données d'application depuis ces sauvegardes.
10. Si les bandes contiennent des sauvegardes protégées par mot de passe, sélectionnez la case à cocher correspondante, puis indiquez le mot de passe pour les sauvegardes. Si vous n'indiquez pas de mot de passe ou si le mot de passe est incorrect, les sauvegardes ne seront pas détectées. Veuillez garder cela à l'esprit dans le cas où vous ne verriez pas de sauvegardes après la nouvelle analyse.

    Conseil. Si les bandes contiennent des sauvegardes protégées par différents mots de passe, vous devrez répéter la nouvelle analyse plusieurs fois en spécifiant chaque mot de passe à son tour.
11. Cliquez sur **Démarrer la ré-analyse** pour démarrer la nouvelle analyse.

Résultat. Les bandes sélectionnées sont déplacées vers le pool sélectionné. Les sauvegardes stockées sur les bandes peuvent être trouvées dans ce pool. Une sauvegarde répartie sur plusieurs bandes n'apparaîtra pas dans le pool jusqu'à ce que toutes ces bandes soient ré-analysées.

Renommage

Lorsqu'une nouvelle bande est détectée par le logiciel, un nom du format suivant lui est automatiquement attribué : **Bande XXX**, où **XXX** est un numéro unique. Les bandes sont numérotées de manière séquentielle. L'opération de renommage vous permet de modifier manuellement le nom d'une bande.

Pour renommer des bandes

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient la bande nécessaire, puis sélectionnez la bande requise.
4. Cliquez sur **Renommer**.

5. Saisissez le nouveau nom de la bande sélectionnée.
6. Cliquez sur **Renommer** pour enregistrer les modifications.

Effacement

L'effacement physique d'une bande supprime toutes les sauvegardes stockées sur la bande et supprime les informations de ces sauvegardes de la base de données. Cependant, les informations sur la bande elle-même restent dans la base de données.

Après l'effacement, une bande située dans le pool **Bandes inconnues** ou **Bandes importées**, est déplacée vers le pool **Bandes libres**. Une bande située dans n'importe quel autre pool n'est pas déplacée.

Pour effacer des bandes

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient les bandes nécessaires, et ensuite sélectionnez les bandes requises.
4. Cliquez sur **Effacer**. Le système vous demande à confirmer l'opération.
5. Sélectionnez la méthode d'effacement : rapide ou complète.
6. Cliquez sur **Effacer** pour démarrer l'opération.
   Détails. Vous ne pouvez pas annuler l'opération d'effacement.

Éjection

Pour réussir l'éjection d'une bande d'une bibliothèque de bandes, la bibliothèque de bandes doit posséder la prise de connecteur du courrier électronique et la prise de connecteur ne doit pas être verrouillée par un utilisateur ou un autre logiciel.

Pour éjecter des bandes

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient les bandes nécessaires, et ensuite sélectionnez les bandes requises.
4. Cliquez sur **Éjecter**. Le logiciel vous invitera à fournir la description de la bande. Nous vous recommandons de décrire l'emplacement physique où les bandes seront conservées. Pendant la restauration, le logiciel affiche cette description afin que vous puissiez facilement trouver les bandes.
5. Cliquez sur **Éjecter** pour démarrer l'opération.

Après l'éjection manuelle ou automatique d'une bande, il est recommandé d'écrire son nom sur cette dernière.

Suppression

L'opération de suppression supprime de la base de données les informations sur les sauvegardes stockées sur la bande sélectionnée et à propos de la bande elle-même.

Vous pouvez retirer uniquement une bande hors ligne (éjectée).

Pour retirer une bande

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient la bande nécessaire, puis sélectionnez la bande requise.
4. Cliquez sur **Supprimer**. Le système vous demande à confirmer l'opération.
5. Cliquez sur **Supprimer** pour retirer la bande.

Quoi faire si je retire une bande accidentellement ?

Contrairement à une bande effacée, les données d'une bande retirée ne sont pas physiquement supprimées. Par conséquent, vous pouvez rendre les sauvegardes sur une telle bande disponibles de nouveau. Pour cela :

1. chargez la bande dans votre lecteur de bandes.
2. Exécutez la prise d'inventaire rapide pour détecter la bande.

   Remarque
   Lors de l'inventaire, *n'activez pas* l'option **Déplacer les bandes non reconnues et importées vers le pool de bandes libres**.

3. Effectuez une nouvelle analyse pour faire correspondre les données enregistrées sur les bandes avec la base de données.

Spécifier un ensemble de bandes

Cette opération vous permet de spécifier un ensemble de bandes pour les bandes.

Un **ensemble de bandes** est un groupe de bandes au sein d'un pool.

Contrairement au fait de spécifier des ensembles de bandes dans les options de sauvegarde, où vous pouvez utiliser des variables, vous ne pouvez spécifier ici qu'une seule valeur de chaîne.

Effectuez cette opération si vous souhaitez que le logiciel effectue une sauvegarde dans des bandes *spécifiques* selon une certaine règle (par exemple, si vous souhaitez stocker les sauvegardes de lundi sur la bande 1, les sauvegardes de mardi sur la bande 2, etc.). Spécifiez un certain ensemble de bandes pour chacune des bandes requises, puis spécifiez le même ensemble de bandes ou utilisez les bonnes variables dans les options de sauvegarde.

Pour l'exemple ci-dessus, spécifiez un ensemble de bandes `Lundi` pour la bande 1, `Mardi` pour la bande 2, etc. Dans les options de sauvegarde, spécifiez `[Jour ouvré]`. Dans ce cas, une bande appropriée sera utilisée le jour respectif de la semaine.

Pour spécifier un ensemble de bandes pour une ou plusieurs bandes

1. Cliquez sur **Paramètres** > **Gestion des bandes**.
2. Sélectionnez la machine ou le nœud de stockage auxquels votre périphérique à bandes est connecté, puis cliquez sur **Pools de bandes** sous cette machine.
3. Cliquez sur le pool qui contient les bandes nécessaires, et ensuite sélectionnez les bandes requises.
4. Cliquez sur **Ensemble de bandes**.
5. Tapez le nom de l'ensemble de bandes. Si un autre ensemble de bandes est déjà spécifié pour les bandes sélectionnées, il sera remplacé. Si vous souhaitez exclure les bandes d'un ensemble de bandes sans en spécifier un autre, effacez le nom de l'ensemble de bandes existant.
6. Cliquez sur **Enregistrer** pour enregistrer les modifications.

Nœuds de stockage

Un nœud de stockage est un serveur destiné à optimiser l'utilisation de plusieurs ressources (telles que la capacité de stockage pour l'entreprise, la bande passante du réseau et la charge de l'UC des serveurs de production) requises pour la protection de données de l'entreprise. Ce but est atteint grâce à l'organisation et à la gestion des emplacements qui servent d'emplacements de stockage dédiés aux sauvegardes de l'entreprise (emplacements gérés).

Le principal objectif du nœud de stockage Acronis est de permettre l'accès centralisé aux lecteurs ou bibliothèques de bandes, par exemple, aux données de sauvegarde et de restauration issues de plusieurs terminaux vers le même lecteur de bandes ou la même bibliothèque de bandes (emplacement de stockage géré sur bande).

Un autre cas d'utilisation consiste à permettre la déduplication avancée quand des données réparties sur plusieurs terminaux doivent être dédupliquées et stockées à un seul emplacement (emplacement de stockage géré avec déduplication activée).

Installer un nœud de stockage et un service de catalogue

Avant l'installation d'un nœud de stockage, assurez-vous que la machine réponde à la configuration requise.

Nous vous recommandons d'installer un service de catalogue et un nœud de stockage sur des machines distinctes. La configuration système nécessaire pour un ordinateur exécutant un service de catalogue est décrite dans "Meilleures pratiques de catalogage" (p. 651).

Pour installer un nœud de stockage et/ou un service de catalogue

1. Connectez-vous comme administrateur et lancez le programme d'installation d'Acronis Cyber Protect.
2. [Facultatif] Pour changer la langue du programme d'installation, cliquez sur **Configurer la langue**.
3. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
4. Cliquez sur **Installer un agent de protection**.
5. Cliquez sur **Personnaliser les paramètres d'installation**.
6. En regard de **Éléments à installer**, cliquez sur **Modifier**.
7. Sélectionnez les composants à installer :
   - Pour installer un nœud de stockage, cochez la case **Nœud de stockage**. La case **Agent pour Windows** est automatiquement sélectionnée.
   - Pour installer un service de catalogue, cochez **Service de catalogue**.
   - Si vous ne souhaitez pas installer d'autre composants sur cette machine, décochez les cases correspondantes.

   Cliquez sur **Terminé** pour continuer.
8. Indiquez le serveur de gestion sur lequel les composants seront enregistrés :
   a. En regard de **Serveur de gestion AcronisCyber Protect**, cliquez sur **Spécifier**.
   b. Spécifiez le nom d'hôte ou l'adresse IP de la machine sur laquelle le serveur de gestion est installé.
   c. Spécifiez les informations d'identification d'un administrateur du serveur de gestion ou un jeton d'enregistrement.

      Pour en savoir plus sur la génération d'un jeton d'enregistrement, reportez-vous à "Etape 1 : Génération d'un jeton d'enregistrement" (p. 183).
   d. Cliquez sur **Valider**.
9. Si vous y êtes invité, sélectionnez si la machine avec le nœud de stockage et/ou le service de catalogue sera ajouté à l'organisation ou à l'une des unités.

   Cette invite apparaît si vous administrez plus d'une unité ou une organisation possédant au moins une unité. Sinon, la machine sera silencieusement ajoutée à l'unité que vous administrez ou à l'organisation. Pour plus d'informations, consultez la page « Administrateurs et unités ».
10. [Facultatif] Modifiez d'autres paramètres d'installation comme décrit dans « Personnalisation des paramètres d'installation ».
11. Cliquez sur **Installer** pour procéder à l'installation.
12. Une fois l'installation terminée, cliquez sur **Fermer**.

Mise à jour du service de catalogue vers Acronis Cyber Protect 15 Update 4

Acronis Cyber Protect 15 Update 4 utilise une nouvelle version du service de catalogue. La nouvelle version n'est pas directement compatible avec les données de catalogue créées par de précédentes versions.

Lors de la mise à jour vers Acronis Cyber Protect 15 Update 4, vous pouvez manuellement migrer ces données vers la nouvelle version du service de catalogue. Autrement, vous pouvez ignorer la migration et recréer les données de catalogue ultérieurement. Une nouvelle création des données de catalogue prend plus de temps que leur migration.

Pour migrer les données de catalogue

1. Sur l'ordinateur où le service de catalogue est installé, exécutez le programme d'installation Acronis Cyber Protect.
2. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
3. Cochez la case **J'ai compris**, puis cliquez sur **Mettre à jour**.
4. Sélectionnez la case à cocher **Spécifier un dossier temporaire**.
5. Spécifiez le dossier dans lequel les données de catalogue seront exportées.
   Les données exportées sont chiffrées. Le dossier temporaire est automatiquement supprimé une fois la migration terminée.
6. Cliquez sur **Valider**.

Pour ignorer la migration des données de catalogue

1. Sur l'ordinateur où le service de catalogue est installé, exécutez le programme d'installation Acronis Cyber Protect.
2. Acceptez les termes du contrat de licence et la politique de confidentialité, puis cliquez sur **Suivant**.
3. Cochez la case **J'ai compris**, puis cliquez sur **Mettre à jour**.
4. Décochez la case **Spécifier un dossier temporaire**.
5. Cliquez sur **Valider**.
6. Confirmez votre choix :

Par conséquent, les données de catalogue existantes deviendront indisponibles après la mise à jour vers Acronis Cyber Protect 15 Update 4. Pour recréer les données de catalogue, exécutez une sauvegarde.

Remarque
Si le service de catalogue, le nœud de stockage et le serveur de gestion s'exécutent sur des ordinateurs distincts, assurez-vous de tous les mettre à jour vers Acronis Cyber Protect 15 Update 4, dans cet ordre :

1. Serveur de gestion
2. Nœud de stockage
3. Service de catalogue

Ajout d’un emplacement géré

Un emplacement géré peut être organisé :

- Dans un dossier local ;
  - Sur un disque dur local au nœud de stockage ;
  - Sur un stockage SAN qui est reconnu par le système d’exploitation en tant que périphérique connecté localement
- Dans un dossier réseau :
  - Sur un partage SMB/CIFS ;
  - Sur un stockage SAN qui est reconnu par le système d’exploitation en tant que dossier réseau ;
  - Sur un NAS ;
- Sur un périphérique à bandes connecté localement au nœud de stockage.

  Les emplacements basés sur bandes sont créés sous forme de pools de bandes. Un pool de bandes existe par défaut. Le cas échéant, vous pouvez créer d’autres pools de bandes, comme décrit ultérieurement dans cette section.

Pour créer un emplacement géré dans un dossier local ou réseau

1. Effectuez l'une des actions suivantes :
   - Cliquez sur **Stockage de sauvegarde** > **Ajouter un emplacement**, puis cliquez sur **Nœud de stockage**.
   - Lors de la création d'un plan de protection, cliquez sur **Où sauvegarder** > **Ajouter un emplacement**, puis cliquez sur **Nœud de stockage**.
   - Cliquez sur **Paramètres** > **Nœuds de stockage**, sélectionnez le nœud de stockage qui gérera l’emplacement, puis cliquez sur **Ajouter un emplacement**.
2. Dans **Nom**, spécifiez un nom unique pour l’emplacement. « Unique » signifie qu'il ne doit pas y avoir un autre emplacement avec le même nom, géré par le même nœud de stockage.
3. [Facultatif] Sélectionnez le nœud de stockage qui gérera l’emplacement. Si vous avez sélectionné la dernière option dans l'étape 1, vous ne pourrez pas modifier le nœud de stockage.
4. Sélectionnez le nœud de stockage ou l’adresse IP que les agents utiliseront pour accéder à l'emplacement.

   Par défaut, le nom du nœud de stockage est choisi. Vous devez modifier ce paramètre si le serveur DNS ne parvient pas à résoudre le nom vers l’adresse IP, ce qui se traduit par un échec d’accès. Pour modifier ce paramètre plus tard, cliquez sur **Stockage de sauvegarde** > l'emplacement > **Modifier**, puis modifiez la valeur du champ **Adresse**.
5. Saisissez le chemin d'accès au dossier ou sélectionnez le dossier souhaité.
6. Cliquez sur **Valider**. Le logiciel vérifie l’accès vers le dossier indiqué.
7. [Facultatif] Activer la déduplication de sauvegarde dans l’emplacement.

   La déduplication réduit le trafic de sauvegarde et la taille des sauvegardes dans l’emplacement en éliminant les blocs de disque dupliqués.

Pour plus d'informations sur les restrictions de déduplication, consultez « Restrictions de déduplication ».

8. [Uniquement si la déduplication est activée] Spécifiez ou modifiez la valeur du champ **Chemin d'accès à la base de données de déduplication**.

   Il doit s'agir d'un dossier sur un disque dur local au nœud de stockage. Pour améliorer les performances du système, nous vous recommandons de créer la base de données de déduplication et l'emplacement géré sur des disques différents.

   Pour plus d'informations sur la base de données de déduplication, consultez « Bonnes pratiques de déduplication ».
9. [Facultatif] Choisissez si vous voulez ou non protéger l'emplacement par chiffrement. Tout ce qui est écrit dans l'emplacement sera chiffré et tout ce qui y est lu sera déchiffré de façon transparente par le nœud de stockage à l'aide d'une clé de chiffrement spécifique à l'emplacement, laquelle est stockée dans le nœud de stockage.

   Pour plus d'informations sur le chiffrement, consultez la section « Chiffrement de l'emplacement ».
10. [Facultatif] Choisissez si vous voulez ou non cataloguer les sauvegardes stockées à cet emplacement. Le catalogue de données vous permet de facilement trouver la version requise des données et de la sélectionner pour la restauration.

    Si plusieurs services de catalogage sont enregistrés sur le serveur de gestion, vous pouvez sélectionner le service qui cataloguera les sauvegardes stockées dans l'emplacement.

    Le catalogage peut être activé ou désactivé ultérieurement, comme décrit dans « Comment activer ou désactiver le catalogage ».
11. Cliquez sur **Terminé** pour créer l'emplacement.

Pour créer un emplacement géré sur un périphérique à bandes

1. Cliquez sur **Stockage de sauvegarde** > **Ajouter un emplacement** ou, lors de la création d'un plan de protection, cliquez sur **Où sauvegarder** > **Ajouter un emplacement**.
2. Cliquez sur **Bandes**.
3. [Facultatif] Sélectionnez le nœud de stockage qui gérera l'emplacement.
4. Suivez les étapes décrites dans « Création d'un pool » à partir de l'étape 4.

Remarque
Par défaut, les agents utilisent le nom de nœud de stockage pour accéder à l'emplacement à bandes géré. Pour que les agents utilisent l'adresse IP du nœud de stockage, cliquez sur **Stockage de sauvegarde** > l'emplacement > **Modifier**, puis modifiez la valeur du champ **Adresse**.

Déduplication

Restrictions de déduplication

Restrictions communes

Les sauvegardes chiffrées ne peuvent pas être dédupliquées. Si vous souhaitez utiliser simultanément la déduplication et le chiffrement, laissez les sauvegardes non chiffrées et orientez-les vers un emplacement où la déduplication et le chiffrement sont tous deux activés.

Sauvegarde au niveau disque

La déduplication des blocs du disque n'est pas effectuée si la taille de l'unité d'allocation du volume — également appelée taille de cluster ou taille de bloc — n'est pas divisible par 4 Ko.

Remarque
La taille de l'unité d'allocation sur la plupart des volumes NTFS et ext3 est de 4 Ko. Cela permet la déduplication au niveau du bloc. Autres exemples de tailles d'unité d'allocation permettant la déduplication de niveau bloc : 8 Ko, 16 Ko et 64 Ko.

Sauvegarde au niveau fichier

La déduplication d'un fichier n'est pas effectuée si le fichier est chiffré.

Déduplication et flux de données NTFS

Dans le système de fichiers NTFS, un fichier peut être associé à un ou plusieurs ensembles de données supplémentaires — souvent appelés *flux de données alternatives*.

Lorsqu'un tel fichier est sauvegardé, ses flux de données alternatives le sont également. Cependant, ces flux ne sont jamais dédupliqués — même lorsque le fichier lui-même l'est.

Meilleures pratiques pour la déduplication

La déduplication est un processus complexe qui dépend de nombreux facteurs.

Les facteurs les plus importants qui ont une incidence sur la vitesse de déduplication sont :

- la vitesse d'accès à la base de données de déduplication
- la capacité de la RAM du nœud de stockage
- Nombre d'emplacements de déduplication sur le nœud de stockage.

Pour augmenter la performance de la déduplication, suivez les recommandations ci-dessous.

Placez la base de données de déduplication et l'emplacement de la déduplication sur des périphériques physiques séparés.

La base de données de déduplication stocke les valeurs de hachage de tous les éléments stockés dans l'emplacement, sauf pour ceux qui ne peuvent pas être dédupliqués, tels que les fichiers chiffrés.

Pour augmenter la vitesse d'accès à une base de données de déduplication, la base de données et l'emplacement doivent être situés sur des périphériques physiques différents.

Il vaut mieux allouer des périphériques dédiés pour l'emplacement et la base de données. Si ce n'est pas possible, du moins ne placez pas un emplacement ou une base de données sur le même disque avec le système d'exploitation. La raison est que le système d'exploitation exécute un grand nombre d'opérations de lecture/écriture sur le disque dur, ce qui ralentit sensiblement la déduplication.

Sélection d'un disque pour une base de données de déduplication

- La base de données doit être située sur un lecteur fixe. Veuillez ne pas essayer de mettre la base de données de déduplication sur des lecteurs externes détachables.
- Pour réduire le plus possible le temps d'accès à la base de données, stockez-la sur un disque directement attaché et non sur un volume réseau monté. Il se peut que la latence du réseau réduise considérablement les performances de déduplication.
- L'espace disque requis pour une base de données de déduplication peut être estimé en utilisant la formule suivante :

$$S = U \times 90 / 65536 + 10$$

Ici,

S correspond à taille du disque, en Go

U est la quantité prévue de données uniques dans le magasin de données de déduplication, en Go

Par exemple, si la quantité prévue de données uniques dans le magasin de données de déduplication est U=5 To, la base de données de déduplication nécessitera un espace libre minimum, comme indiqué ci-dessous :

$$S = 5\,000 \times 90 / 65\,536 + 10 = 17 \text{ Go}$$

Sélection d'un disque pour un emplacement dédupliqué

Dans le but d'empêcher une perte de données, nous conseillons d'utiliser RAID 10, 5 ou 6. RAID 0 n'est pas conseillé puisqu'il n'est pas tolérant aux pannes. RAID 1 n'est pas conseillé à cause de sa vitesse relativement faible. Il n'y a pas de préférence pour les disques locaux ou le SAN, les deux sont bons.

40 à 160 Mo de mémoire RAM pour 1 To de données uniques

Lorsque la limite est atteinte, la déduplication s'arrêtera mais la sauvegarde et la restauration se poursuivront. Si vous ajoutez de la mémoire vive supplémentaire au nœud de stockage, après la sauvegarde suivante, la déduplication reprendra. En général, plus vous avez de mémoire vive, plus les volumes de données uniques que vous pouvez stocker sont gros.

Uniquement un emplacement dédupliqué sur chaque nœud de stockage

Il est vivement recommandé de créer un seul emplacement dédupliqué sur un nœud de stockage. Sinon, il est possible que l'ensemble du volume de RAM disponible soit réparti proportionnellement au nombre d'emplacements.

Absence d'applications utilisant les mêmes ressources

La machine avec le nœud de stockage ne doit pas exécuter des applications qui nécessitent beaucoup de ressources système ; par exemple, des systèmes de gestion de bases de données (DBMS) ou des systèmes de planification de ressources d'entreprise (ERP).

Processeur multicœur avec une vitesse d'horloge d'au moins 2,5 GHz

Nous vous conseillons d'utiliser un processeur avec au moins quatre cœurs et une vitesse d'horloge d'au moins 2,5GHz.

Espace libre suffisant dans l'emplacement

La déduplication cible nécessite autant d'espace libre que celui occupé par les données de sauvegarde immédiatement après avoir été enregistrées dans l'emplacement. Sans une compression ou une déduplication à la source, cette valeur est égale à la taille des données d'origine sauvegardées pendant l'opération de sauvegarde donnée.

Réseau local haute vitesse

Un réseau local de 1 Gbit est recommandé. Cela permettra au logiciel d'exécuter 5 à 6 sauvegardes avec une déduplication en parallèle sans réduire considérablement la vitesse.

Sauvegardez une machine typique avant de sauvegarder plusieurs machines ayant un contenu similaire

Lorsque vous sauvegardez plusieurs machines ayant un contenu similaire, nous vous recommandons de sauvegarder d'abord une machine et d'attendre la fin de l'indexation des données sauvegardées. Après cela, les autres machines seront sauvegardées plus vite en raison de la déduplication efficace. Du fait que la sauvegarde de la première machine a été indexée, la plupart des données sont déjà dans le magasin de données de déduplication.

Sauvegardez différentes machines à des moments différents

Si vous sauvegardez un grand nombre de machines, étalez les opérations de sauvegarde dans le temps. Pour ce faire, créez plusieurs plans de plan de protection avec plusieurs planifications.

Chiffrement de l'emplacement

Si vous protégez un emplacement par chiffrement, tout ce qui y est écrit sera chiffré et tout ce qui y est lu sera déchiffré de façon transparente par le nœud de stockage en utilisant une clé de chiffrement spécifique à l'emplacement de stockage, laquelle est stockée dans le nœud. Si le support de stockage est volé ou si une personne non autorisée y accède avec des intentions malveillantes, elle ne pourra pas déchiffrer le contenu de l'emplacement de stockage sans pouvoir accéder au nœud de stockage.

Ce chiffrement n'a rien à voir avec le chiffrement de sauvegarde spécifié par le plan de protection et exécuté par un agent. Si la sauvegarde est déjà chiffrée, le chiffrement côté nœud de stockage est appliqué par dessus le chiffrement exécuté par l'agent.

Pour protéger l'emplacement avec chiffrement

1. Spécifiez un mot (mot de passe) à utiliser pour générer la clé de chiffrement.
   Le mot est sensible à la casse. On vous demandera ce mot uniquement si vous reliez l'emplacement à un autre nœud de stockage.
2. Sélectionnez l'un des algorithmes de chiffrement suivants :
   - **AES 128** – le contenu de l'emplacement est chiffré à l'aide de l'algorithme du standard de chiffrement avancé (AES) avec une clé de 128 bits.
   - **AES 192** – le contenu de l'emplacement est chiffré à l'aide de l'algorithme du standard de chiffrement avancé (AES) avec une clé de 192 bits.
   - **AES 256** – le contenu de l'emplacement est chiffré à l'aide de l'algorithme du standard de chiffrement avancé (AES) avec une clé de 256 bits.
3. Cliquez sur **OK**.

L'algorithme de chiffrement AES fonctionne en mode Enchaînement des blocs (CBC) et utilise une clé générée de manière aléatoire avec une taille définie par l'utilisateur de 128, 192 ou 256 bits. Plus la taille de la clé est grande, plus le programme mettra du temps à chiffrer les sauvegardes stockées dans l'emplacement et plus les archives seront sécurisées.

La clé de chiffrement est ensuite chiffrée avec l'algorithme AES-256 en utilisant un hachage SHA-256 du mot sélectionné en tant que clé. Le mot lui-même n'est pas stocké sur le disque ; le hachage du mot n'est utilisé que pour des considérations de vérification. Avec cette sécurité à deux niveaux, les sauvegardes sont protégées contre tout accès non autorisé, mais la récupération d'un mot oublié n'est pas possible.

Catalogage

Catalogue de données

Le catalogue de données vous permet de facilement trouver la version requise des données et de la sélectionner pour la restauration. Le catalogue de données affiche les données stockées dans les emplacements gérés pour lesquels le catalogage est ou était activé.

La section **Catalogue** s'affiche sous l'onglet **stockage de sauvegarde** uniquement si un service de catalogue au moins est enregistré sur le serveur de gestion. Pour obtenir plus d'informations sur l'installation du service de catalogue, consultez la section « Installation d'un nœud de stockage et d'un service de catalogue ».

La section **Catalogue** est visible uniquement par les administrateurs de l'organisation.

Limites

Le catalogage n'est disponible que pour les sauvegardes des machines physiques sur disque et au niveau des fichiers et pour les sauvegardes de machines virtuelles.

Les données suivantes ne peuvent pas être affichées dans le catalogue :

- Données provenant de sauvegardes chiffrées
- Données sauvegardées sur un périphérique à bandes
- Données sauvegardées sur Cloud Storage.
- Données sauvegardées par les versions de produit Acronis Cyber Protect antérieures à la version 12.5

Sélection des données sauvegardées pour la récupération

1. Cliquez sur **Stockage de sauvegarde** > **Catalogue**.
2. Si plusieurs services de catalogage sont enregistrés sur le serveur de gestion, sélectionnez le service qui catalogue les sauvegardes stockées dans l'emplacement.

   Remarque
   Pour voir quel service catalogue un emplacement, sélectionnez l'emplacement dans **Stockage de sauvegarde** > **Emplacements > Emplacements**, puis cliquez sur **Détails**.

3. Le logiciel affiche les machines qui ont été sauvegardées dans les emplacements gérés catalogués par le service de catalogue sélectionné.
   Sélectionnez les données à récupérer en les parcourant ou en effectuant une recherche.
   - **Parcourir**
     Double-cliquez sur une machine pour voir les disques, volumes, dossiers et fichiers sauvegardés.

Pour restaurer un disque, sélectionnez un disque signalé par l'icône suivante : 

Pour restaurer un volume, double-cliquez sur le disque qui contient le volume, puis sélectionnez le volume.

Pour restaurer des fichiers et des dossiers, parcourez le volume sur lequel ils se trouvent.

Vous pouvez parcourir les volumes signalés par l'icône dossier : 

- **Rechercher**

  Dans le champ de recherche, tapez l'information qui permet d'identifier les éléments de données requis (cela peut être un nom de machine, un nom de fichier ou de dossier, ou un nom de disque), puis cliquez sur **Rechercher**.

  Vous pouvez utiliser les caractères génériques astérisque (*) et point d'interrogation (?).

  Vous verrez alors la liste des éléments de données sauvegardés dont les noms correspondent entièrement ou partiellement à la valeur saisie.

4. Par défaut, les données seront ramenées au dernier point dans le temps. Si un seul élément est sélectionné, vous pouvez utiliser le bouton **Versions** pour sélectionner un point de récupération.
5. Après voir sélectionné les données requises, effectuez l'une des actions suivantes :
   - Cliquez sur **Restaurer**, puis configurez les paramètres de l'opération de récupération comme décrit dans « Récupération ».
   - [Uniquement pour les fichiers/dossiers] Si vous souhaitez enregistrer les fichiers au format .zip, cliquez sur **Télécharger**, sélectionnez l'emplacement où enregistrer les données et cliquez sur **Enregistrer**.

Meilleures pratiques de catalogage

Pour améliorer les performances du catalogage, suivez les recommandations ci-après.

Installation

Nous vous recommandons d'installer un service de catalogue et un nœud de stockage sur des machines distinctes. Sinon, ces composants diviseront les ressources du processeur et de la RAM.

Si plusieurs nœuds de stockage sont enregistrés sur le serveur de gestion, un service de catalogue suffit, sauf si les performances d'indexation ou de recherche se dégradent. Par exemple, si vous remarquez que le catalogage fonctionne 24 h/24 et 7 j/7 (c'est-à-dire sans pause), installez un autre service de catalogue sur une machine distincte. Supprimez ensuite certains des emplacements gérés et recréez-les avec le nouveau service de catalogue. Les sauvegardes stockées à ces emplacements seront conservées intactes.

Configuration requise

Paramètre	Valeur minimum	Valeur recommandée
Nombre de cœurs du processeur	2	4 et plus

RAM	8 Go	16 Go et plus
Disque dur	7 200 tpm	SSD
Connexion réseau entre la machine avec le nœud de stockage et la machine avec le service de catalogue	100 Mbits/s	1 Gbits/s

Comment activer ou désactiver le catalogage

Si le catalogage est activé pour un emplacement géré, le contenu de chaque sauvegarde envoyée vers l'emplacement est ajouté au catalogue de données dès que la sauvegarde est créée.

Vous pouvez activer le catalogage quand vous ajoutez un emplacement géré ou ultérieurement. Une fois le catalogage activé, toutes les sauvegardes stockées à un emplacement, mais non cataloguées précédemment le seront après la sauvegarde suivante vers cet emplacement.

Le processus de catalogage peut être chronophage, surtout si un grand nombre de machines est sauvegardé au même emplacement. Vous pouvez désactiver le catalogage à n'importe quel moment. Le catalogage de sauvegardes créées avant la désactivation sera finalisé. Les sauvegardes nouvellement créées ne seront pas cataloguées.

Pour configurer le catalogage à des emplacements existants

1. Cliquez sur **Stockage de sauvegarde** > **Emplacements**.
2. Cliquez sur **Emplacements**, puis sélectionnez l'emplacement géré pour lequel vous souhaitez configurer le catalogage.
3. Cliquez sur **Éditer**.
4. Activez ou désactivez le commutateur **Service de catalogue**.
5. Cliquez sur **Valider**.

Paramètres système

Ces paramètres sont uniquement disponibles pour les déploiements sur site.

Pour accéder à ces paramètres, cliquez sur **Paramètres** > **Paramètres système**.

La section **Paramètres système** est visible uniquement par les administrateurs de l'organisation.

Notifications par courrier électronique

Vous pouvez configurer les paramètres généraux communs pour toutes les notifications par messagerie électronique envoyées par le serveur de gestion.

Dans les options de sauvegarde par défaut, vous pouvez ignorer ces paramètres exclusivement pour les événements qui se produisent pendant la sauvegarde. Dans ce cas, les paramètres généraux seront effectifs pour les opérations autres que la sauvegarde.

Lors de la création d'un plan de protection, vous pouvez choisir les paramètres qui seront utilisés : les paramètres généraux ou les paramètres définis dans les options de sauvegarde par défaut. Vous pouvez également les remplacer par des valeurs personnalisées qui seront spécifiques au plan.

Important
Lorsque les paramètres généraux relatifs aux notifications par e-mail sont modifiés, tous les plans de protection qui utilisent les paramètres généraux sont affectés.

Avant de configurer ces paramètres, assurez-vous que les paramètres du **serveur de messagerie** sont configurés.

Pour configurer les paramètres généraux relatifs aux notifications par messagerie électronique

1. Cliquez sur **Paramètres** > **Paramètres système** > **Notifications par messagerie électronique**.
2. Dans le champ **Adresses électroniques des destinataires**, indiquez l'adresse électronique de destination. Vous pouvez saisir plusieurs adresses séparées par des points-virgules.
3. [Facultatif] Dans le champ **Objet**, modifiez l'objet de la notification par messagerie électronique. Vous pouvez utiliser les variables suivantes :
   - `[Alerte]` - résumé des alertes.
   - `[Terminal]` - nom du terminal.
   - `[Plan]` - nom du plan ayant généré l'alerte.
   - `[Serveur de gestion]` - nom d'hôte de l'ordinateur sur lequel le serveur de gestion est installé.
   - `[Unité]` - nom de l'unité à laquelle l'ordinateur appartient.

   L'objet par défaut est `[Alerte]` **Terminal :** `[Terminal]` **Plan :** `[Plan]`
4. [Facultatif] Cochez la case **Résumé quotidien concernant les alertes actives**, puis procédez comme suit :

a. Précisez l'heure à laquelle le résumé sera envoyé.

b. [Facultatif] Cochez la case **Ne pas envoyer de message « Aucune alerte active »**.

5. [Facultatif] Sélectionnez la langue qui sera utilisée dans les notifications par messagerie électronique.
6. Sélectionnez les cases à cocher correspondant aux événements pour lesquels vous souhaitez recevoir des notifications. Vous pouvez choisir dans la liste contenant toutes les alertes possibles, regroupées par niveau de gravité.
7. Cliquez sur **Enregistrer**.

Serveur de messagerie

Vous pouvez spécifier un serveur de messagerie qui servira à envoyer des notifications par courrier électronique depuis le serveur de gestion.

Pour spécifier le serveur de messagerie

1. Cliquez sur **Paramètres** > **Paramètres système** > **Serveur de messagerie**.
2. Dans **Service de courrier électronique**, sélectionnez l'une des options suivantes :
   - **Personnalisée**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. [Uniquement pour un service de messagerie personnalisé] Spécifiez les paramètres suivants :
   - Dans le champ **Serveur SMTP**, saisissez le nom du serveur de messagerie sortant (SMTP).
   - Dans le champ **Port SMTP**, définissez le port du serveur de messagerie sortant. Par défaut, le port est défini sur 25.
   - Choisissez le chiffrement que vous souhaitez utiliser, SSL ou TLS. Sélectionnez **Aucun** pour désactiver le chiffrement.
   - Si le serveur SMTP requiert une authentification, sélectionnez la case à cocher **correspondante** et spécifiez les informations d'identification du compte qui sera utilisé pour envoyer les messages. Si vous n'êtes pas sûr que le serveur SMTP nécessite une authentification, contactez l'administrateur réseau ou votre fournisseur de service de messagerie pour assistance.
4. [Uniquement pour Gmail, Yahoo Mail et Outlook.com] Spécifiez les informations d'identification du compte qui sera utilisé pour envoyer les messages.
5. [Uniquement pour un service de messagerie personnalisé] Dans **Expéditeur**, saisissez le nom de l'expéditeur. Ce nom apparaîtra dans le champ **De** des notifications par messagerie électronique. Si vous laissez ce champ vide, le compte spécifié dans l'étape 3 ou 4 apparaîtra dans les messages.

6. [Facultatif] Cliquez sur **Envoyer un message de test** pour vérifier que les notifications par messagerie électronique fonctionnent avec les paramètres configurés. Saisissez l'adresse électronique à laquelle envoyer un message de test.

Sécurité

Utilisez ces options pour renforcer la sécurité du déploiement sur site de Acronis Cyber Protect.

Déconnecter les utilisateurs inactifs après

Cette option vous permet de spécifier un délai d'expiration pour la déconnexion automatique causée par l'inactivité de l'utilisateur. Lorsqu'il reste une minute avant l'expiration, le logiciel invite l'utilisateur à rester connecté. S'il ne réagit pas, l'utilisateur est déconnecté et toutes les modifications non enregistrées sont perdues.

Le préréglage est le suivant : **Activé. Délai expiré : 10 minutes.**

Afficher une notification sur la dernière connexion de l'utilisateur actuel

Cette option permet l'affichage de la date et de l'heure de la dernière connexion réussie de l'utilisateur, le nombre d'échecs d'authentification depuis la dernière connexion réussie, et l'adresse IP de la dernière connexion réussie. Ces informations s'affichent en bas de l'écran à chaque connexion de l'utilisateur.

Le préréglage est le suivant : **Désactivé**.

Avertir de l'expiration du mot de passe du domaine ou local

Cette option permet l'affichage de la date d'expiration du mot de passe permettant à l'utilisateur d'accéder au serveur de gestion Acronis Cyber Protect. C'est le mot de passe local ou de domaine avec lequel l'utilisateur se connecte à la machine sur laquelle le serveur de gestion est installé. Le temps restant avant l'expiration du mot de passe s'affiche en bas de l'écran et dans le menu du compte dans le coin supérieur droit.

Le préréglage est le suivant : **Désactivé**.

Mises à jour

Cette option permet à Acronis Cyber Protect de vérifier si une nouvelle version est disponible à chaque fois qu'un administrateur de l'organisation se connecte sur la console Web Cyber Protect.

Le préréglage est le suivant : **Activé**.

Si cette option est désactivée, l'administrateur peut vérifier les mises à jour manuellement comme décrit dans « Vérification des mises à jour de logiciel ».

Options de sauvegarde par défaut

Les valeurs par défaut des options de sauvegarde sont communes pour tous les plans de protection du serveur de gestion. L'administrateur d'une organisation peut 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 après la mise en place 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. Connectez-vous à la console Web Cyber Protect en tant qu'administrateur de l'organisation.
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**.

Paramètres de protection

Pour configurer les paramètres de protection, dans la console Web Cyber Protect, accédez à **Paramètres** > **Protection**.

Pour en savoir plus sur des paramètres et procédures spécifiques, reportez-vous à la rubrique suivante de cette section.

Mise à jour des définitions de protection

Par défaut, tous les agents de protection peuvent se connecter à Internet et télécharger les mises à jour des composants suivants :

- Anti-malware
- Évaluation des vulnérabilités
- Gestion des correctifs

Agents ayant le rôle de Responsable de la mise à jour

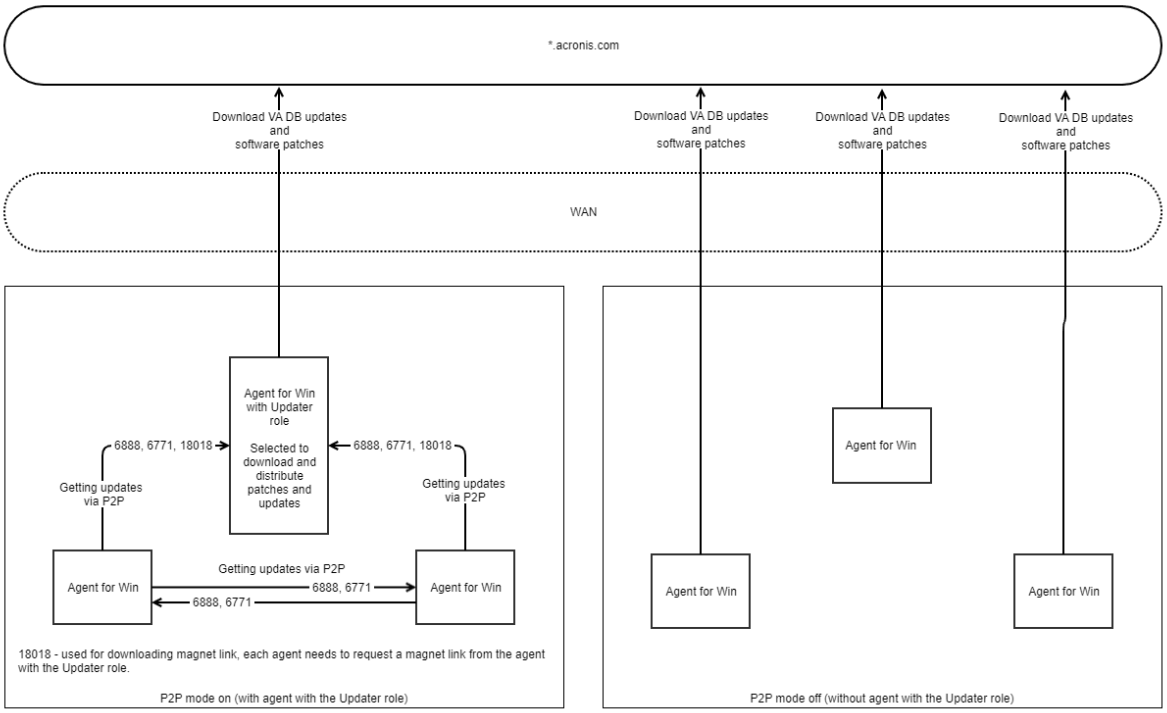
Un administrateur peut réduire le trafic sur la bande passante réseau en sélectionnant un ou plusieurs agents de protection dans l'environnement et en leur attribuant le rôle Responsable de la mise à jour. Les agents dédiés se connecteront donc à Internet et téléchargeront les mises à jour. Tous les 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.

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.

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 définitions de protection mises à jour.

Le diagramme suivant illustre les options de téléchargement des mises à jour de protection. A gauche, le rôle Responsable de la mise à jour est attribué à un agent. Cet agent se connecte à Internet pour télécharger les mises à jour de protection, et les autres agents se connectent à l'agent Responsable de la mise à jour pour obtenir les dernières mises à jour. A droite, le rôle Responsable de la mise à jour n'est attribué à aucun agent. Tous les agents se connectent donc à Internet pour télécharger les mises à jour de protection.



Pour préparer un ordinateur pour le rôle Responsable de la mise à jour

1. Sur la machine sur laquelle un agent ayant le rôle Responsable de la mise à jour s'exécutera, appliquez les règles de pare-feu suivantes :
   - Entrant « ports_tcp_entrants_responsable_mise_à_jour » : autoriser la connexion aux ports TCP 18018 et 6888 pour tous les profils de pare-feu (public, privé et domaine).
   - Entrant « ports_udp_entrants_responsable_mise_à_jour » : autoriser la connexion aux ports UDP 6888 pour tous les profils de pare-feu (public, privé et domaine).
2. Redémarrez le service Noyau agent Acronis.
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.

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

1. Dans la console Web 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.
3. Cliquez sur **Détails**, puis activez l'interrupteur **Utilisez cet agent pour télécharger et distribuer des correctifs et des mises à jour**.

Planification des mises à jour

Vous pouvez planifier des mises à jour automatiques des définitions de protection sur tous les agents ou les mettre à jour manuellement sur des objets sélectionnés.

Pour planifier des mises à jour automatiques

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Protection** > **Mise à jour des définitions de protection**.
2. Sélectionnez **Planifier**.
3. Dans **Type de planification**, sélectionnez l'une des options suivantes :
   - **Quotidienne**

     Sélectionnez des jours de la semaine pour mettre à jour les définitions de protection.

     Dans **Démarrage à :**, sélectionnez l'heure à laquelle les mises à jour seront exécutées.
   - **Par heure**

     Définissez une planification granulaire pour les mises à jour.

     Dans **Exécution chaque :**, définissez la périodicité des mises à jour.

     Dans **À partir de :** ... **Jusqu'à :**, définissez une plage de temps spécifique pour les mises à jour.

Pour mettre à jour manuellement les définitions de protection

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Agents**.
2. Sélectionnez les machines des agents sur lesquelles vous souhaitez mettre à jour les définitions de protection, puis cliquez sur **Mettre les définitions à jour**.

Modification de l'emplacement de téléchargement

Les définitions de protection sont téléchargées dans le dossier temporaire par défaut de votre machine avant d'être stockées dans le dossier du programme Acronis.

Pour modifier le dossier temporaire pour le téléchargement

1. Sur la machine du serveur de gestion, ouvrez le fichier `atp-database-mirror.json` pour le modifier.

   Vous pouvez trouver ce fichier à l'emplacement suivant :
   - Windows : `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux : `/var/lib/Acronis/AtpDatabaseMirror/`
2. Modifiez la valeur de `"enable_user_config"` en `true`.

```
{
"sysconfig":
{
...
```

```
"enable_user_config": true
}
...
}
```

3. Sur la machine du serveur de gestion, ouvrez le fichier `config.json` pour le modifier.
   Vous pouvez trouver ce fichier à l'emplacement suivant :
   - Windows : `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux : `/var/lib/Acronis/AtpDatabaseMirror/`
4. Ajoutez la ligne suivante : `"mirror_temp_dir": "<path_to_new_download_location>"`
   Par exemple :

   ```
   {
           "mirror_temp_dir": "C:\\temp"
   }
   ```

   Ce chemin d'accès peut être absolu ou relatif au dossier `AppData`.
   Si le dossier ne peut être créé ou si le serveur de gestion ne peut pas y écrire, l'emplacement par défaut sera utilisé.

Options de stockage de cache

Les données en cache sont stockées dans l'emplacement suivant :

- Windows : `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linux : `/opt/acronis/var/atp-downloader/Cache`
- macOS : `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Vous pouvez configurer un calendrier pour effacer les données en cache obsolètes et définir une limite de taille pour ces données. Vous pouvez définir différentes limites pour les machines, selon qu'elles contiennent des agents responsables de la mise à jour ou des agents non responsables de la mise à jour.

Source des dernières définitions de protection

Vous pouvez télécharger les dernières définitions de protection depuis les emplacements suivants :

- **Le Cloud**
  Les agents de protection se connectent à Internet et téléchargent les dernières définitions de protection depuis Acronis Cloud. Par défaut, tous les agents enregistrés dans le serveur de gestion cherchent des mises à jour et les distribuent. Pour plus d'informations sur les agents ayant le rôle de Responsable de la mise à jour, reportez-vous à la section "Mise à jour des définitions de protection" (p. 657).
- **Cyber Protect Serveur de gestion**

Grâce à cette option, les agents n'ont pas besoin d'accéder à Internet. Ils se connectent uniquement au serveur de gestion, dans lequel les définitions de protection sont stockées. Toutefois, le serveur de gestion doit être connecté à Internet afin de pouvoir télécharger les dernières définitions de protection.

- **Serveurs Web personnalisés**

  Cette option est prévue à des fins de dépannage et de test uniquement, ou pour être utilisée dans des environnements isolés par air gap. Pour obtenir plus d'informations, consultez l'article "Mise à jour des définitions de protection dans un environnement isolé par air gap" (p. 661). Vous devrez habituellement sélectionner cette option uniquement lorsque l'équipe de support Acronis vous invite à le faire.

Connexion à distance

Quand vous activez la connexion à distance, les options **Se connecter via un client RDP** et **Se connecter via un client HTML5** apparaissent dans le console Web Cyber Protect, sous **Bureau cyberprotection** dans le menu de droite. Le menu de droite s'ouvre quand vous sélectionnez une ressource dans l'onglet **Terminaux**.

Activer ou désactiver la connexion à distance affecte tous les utilisateurs de votre organisation.

Pour activer la connexion à distance

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Protection**.
2. Cliquez sur **Connexion à distance**, puis activez l'interrupteur **Connexion à distance au bureau**.

Vous pouvez également activer le partage de connexion à distance. Avec cette option, vous pouvez générer un lien qui permet d'accéder à distance à la ressource sélectionnée. Vous pouvez partager ces liens avec d'autres utilisateurs.

Pour activer le partage de connexion à distance

1. Dans la console Web Cyber Protect, accédez à **Paramètres** > **Protection**.
2. Cochez la case **Partager la connexion à distance au bureau**.

Par conséquent, l'option **Partager la connexion à distance** apparaît dans la console Web Cyber Protect, sous **Bureau cyberprotection** dans le menu de droite.

Mise à jour des définitions de protection dans un environnement isolé par air gap

Acronis Cyber Protect prend en charge les définitions de protection dans les environnements isolés par air gap.

Pour mettre à jour les définitions de protection dans un environnement isolé par air gap

1. Installez un second serveur de gestion pouvant accéder à Internet, en dehors de votre environnement isolé par air gap.

   Pour en savoir plus sur la façon de procéder, consultez "Installation du serveur d'administration" (p. 86).
2. Copiez les définitions de protection du serveur de gestion en ligne sur un lecteur amovible, puis transférez les définitions vers un serveur HTTP dans l'environnement isolé par air gap.

   Pour plus d'informations sur cette étape, reportez-vous à "Téléchargement des définitions vers un serveur de gestion en ligne" (p. 662) et "Transfert des définitions vers un serveur HTTP" (p. 663).
3. Sur le serveur de gestion isolé par air gap, configurez le server HTTP comme source des définitions de protection mises à jour.

   Pour plus d'informations sur cette étape, reportez-vous à "Configuration de la source des définitions dans le serveur de gestion isolé par air gap" (p. 664).

Téléchargement des définitions vers un serveur de gestion en ligne

Après avoir installé un second serveur de gestion pouvant se connecter à Internet, téléchargez les dernières définitions de protection et copiez-les sur un lecteur amovible, comme un lecteur flash USB ou un disque dur externe.

Pour télécharger et copier les définitions de protection

1. Sur la machine contenant le serveur de gestion en ligne, copiez le dossier `AtpDatabaseMirror` vers un emplacement de votre choix, par exemple le bureau ou le dossier `Temp`.

   Vous pouvez trouver le dossier `AtpDatabaseMirror` sous l'emplacement suivant :
   - Windows : `%ProgramData%\Acronis\`
   - Linux : `/usr/lib/Acronis/`
2. Ouvrez le fichier `atp_database_mirror.json` pour le modifier. Vous pouvez trouver le fichier sous l'emplacement suivant :
   - Windows : `%Program Files%\Acronis\AtpDatabaseMirror`

     Remarque
     Sous Windows, ce dossier n'est pas le même que le dossier de l'étape précédente.
   - Linux : `/usr/lib/Acronis/AppDatabaseMonitor`
3. Modifiez le fichier `atp_database_mirror.json` comme suit :
   a. Modifiez les valeurs de `"enable_appdata_as_root"` en `false`.
   b. Modifiez les valeurs de toutes les entrées de `"local_path"` en chemin d'accès absolu de l'emplacement vers lequel vous souhaitez enregistrer les définitions de protection.
4. Enregistrez les modifications dans le fichier `atp_database_mirror.json`.
5. Sur la machine contenant le serveur de gestion en ligne, arrêtez le service **Acronis Management Server** en utilisant la commande suivante :

- Windows (invite de commandes) :

```
sc stop AcrMngSrv
```

- Linux (terminal) :

```
sudo systemctl stop acronis_ams.service
```

6. Dans le dossier `AtpDatabaseMirror` que vous avez copié vers un emplacement de votre choix, lancez l'outil `AtpDatabaseMirror` à l'aide de la commande suivante :
   - Windows (invite de commandes) :

```
atp_database_mirror.exe -config atp_database_mirror.json
```

   - Linux (terminal) :

```
sudo ./atp_database_mirror -config atp_database_mirror.json
```

   Lorsque toutes les mises à jour ont été les téléchargées vers le dossier indiqué dans `"local_path"`, la ligne suivante apparaît dans l'invite de commande ou la fenêtre du terminal :

```
standing by for 1m0s
```

7. Arrêtez l'outil `AtpDatabaseMirror` en appuyant sur CTRL+C.
8. Copiez les fichiers depuis le dossier que vous avez précisé dans `"local_path"` vers un lecteur amovible.

Vous devez ensuite copier les fichiers depuis le lecteur amovible vers un serveur HTTP dans votre environnement isolé par air gap. Vous pouvez utiliser le serveur de gestion isolé par air gap en tant que serveur HTTP. Pour obtenir plus d'informations, consultez l'article "Transfert des définitions vers un serveur HTTP" (p. 663).

Transfert des définitions vers un serveur HTTP

Pour distribuer les définitions de protection dans votre environnement isolé par air gap, vous avez besoin d'un serveur HTTP dédié. Vous pouvez utiliser votre serveur de gestion isolé par air gap en tant que serveur HTTP.

Pour transférer des définitions de protection vers un serveur HTTP

1. Sur la machine sur laquelle vous exécuterez le serveur HTTP, copiez les définitions de protection vers un dossier de votre choix.
2. Depuis le dossier dans lequel vous avez copié les définitions de protection, lancez un serveur HTTP.

   Vous pouvez par exemple utiliser Python et exécuter la commande suivante :

```
python -m http.server 8080
```

Remarque
Vous pouvez utiliser le serveur HTTP que vous préférez.

3. Dans le dossier dans lequel vous avez copié les définitions de protection, ouvrez les fichiers `update-index.json` suivants pour modification :
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`
4. Dans les deux fichiers `update-index.json`, modifiez tous les champs `produits > os > arch > composants > versions > url`, comme suit :
   a. Pour les valeurs `IP` et `port`, définissez l'adresse IP et le port de votre serveur HTTP.
   b. Ne modifiez pas l'autre partie du chemin d'accès.

   Par exemple, `"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"`, où 192.168.1.10 est l'adresse IP du serveur HTTP, et 8080 est son port. Ne changez pas la partie `/ngmp/win64/ngmp.zip`.
5. Enregistrez vos modifications dans les deux fichiers `update-index.json`.

Vous devez ensuite configurer la source des définitions de protection dans le serveur de gestion isolé par air gap. Pour obtenir plus d'informations, consultez l'article "Configuration de la source des définitions dans le serveur de gestion isolé par air gap" (p. 664).

Configuration de la source des définitions dans le serveur de gestion isolé par air gap

Après avoir configuré le serveur HTTP, vous devez le configurer dans le serveur de gestion isolé par air gap comme source des définitions de protection.

Pour configurer la source des définitions de protection dans le serveur de gestion isolé par air gap

1. Dans la console Web Cyber Protect du serveur de gestion isolé par air gap, accédez à **Paramètres** > **Protection** > **Mise à jour des définitions de protection**.
2. Sélectionnez **Définitions**.
3. Sélectionnez **Personnalisé**, puis spécifiez les chemins d'accès suivants :

- Pour **Définitions d'antivirus et d'antimalware** :
  `http://<IP address of your HTTP server>:8080/scanner`
- Pour **Définitions de détection avancées** :
  `http://<IP address of your HTTP server>:8080/ngmp`
- Pour **Définitions de l'évaluation des vulnérabilités et de la gestion des correctifs** :
  `http://<IP address of your HTTP server>:8080/vapm`

Par conséquent, les agents de l'environnement isolé par air gap téléchargeront les définitions de protection depuis votre serveur HTTP.

Administration des comptes d’utilisateur et des unités de l’organisation

Déploiement sur site

La fonctionnalité décrite dans cette section n'est disponible que pour les administrateurs de l'organisation.

Pour accéder à ces paramètres, cliquez sur **Paramètres** > **Comptes**.

Unités et comptes d'administration

Pour gérer les unités et les comptes d'administration, dans la console Web Cyber Protect, accédez à **Paramètres** > **Comptes**. Le volet **Comptes** affiche le groupe **Organisation** avec l'arborescence des unités (le cas échéant), ainsi que la liste des comptes d'administration au niveau hiérarchique sélectionné.

Unités

Le groupe **Organisation** est créé automatiquement quand vous installez le serveur d'administration. Avec la licence Acronis Cyber Protect Advanced, vous pouvez créer des groupes enfant appelés unités, qui correspondent généralement à des unités ou des services de l'organisation, et y ajouter des comptes d'administration. Ainsi, vous pouvez déléguer la gestion de la protection à d'autres personnes dont les droits d'accès seront strictement limités aux unités correspondantes. Pour en savoir plus sur la manière de créer une unité, consultez "Création d'unités" (p. 670).

Chaque unité peut disposer d'unités enfant. Les comptes d'administration d'une unité parent disposent des mêmes droits dans toutes ses unités enfant. Le groupe **Organisation** est l'unité parent de plus haut niveau, et tous les comptes d'administration à ce niveau disposent des mêmes droits dans toutes ses unités.

Comptes d'administration

Tout compte pouvant se connecter à la console Web Cyber Protect est un compte d'administration.

Dans la console Web Cyber Protect, tout compte d'administration peut afficher ou gérer tous les éléments situés à un niveau hiérarchique inférieur ou égal à celui de son unité. Par exemple, un compte d'administration au niveau *organisation* a accès à ce premier niveau et donc à toutes les unités de cette organisation. Un compte d'administration dans une *unité* spécifique peut uniquement accéder à cette unité et à ses unités enfant.

Quels comptes peuvent être des comptes d'administration ?

Si le serveur de gestion est installé sur un ordinateur Windows inclus dans un domaine Active Directory, vous pouvez octroyer des droits d'administration à des utilisateurs locaux, ou à des utilisateurs et groupes d'utilisateurs au sein de la forêt du domaine Active Directory.

Par défaut, le serveur de gestion établit une connexion protégée par SSL/TSL avec le contrôleur de domaine Active Directory. Si c'est impossible, aucune connexion ne sera établie. Vous pouvez néanmoins autoriser les connexions non sécurisées en modifiant le fichier `auth-connector.json5`.

Pour utiliser une connexion sécurisée, assurez-vous que le LDAP sur SSL (LDAPS) est configuré pour votre Active Directory.

Pour configurer le LDAPS pour Active Directory

1. Sur le contrôleur de domaine, créez et installez un certificat LDAP qui répond aux exigences de Microsoft.
   Pour en savoir plus sur la façon de réaliser ces opérations, reportez-vous à Activer LDAP sur SSL avec une autorité de certification tierce dans la documentation Microsoft.
2. Sur le contrôleur de domaine, ouvrez la **Console de gestion Microsoft** et vérifiez que le certificat existe sous **Certificats (ordinateur local)** > **Personnel** > **Certificats**.
3. Redémarrez le contrôleur de domaine.
4. Vérifiez que le LDAPS est activé.

Pour autoriser les connexions non sécurisées au contrôleur de domaine

1. Connectez-vous à la machine sur laquelle le serveur de gestion est installé.
2. Ouvrez le fichier `auth-connector.json5` pour modification.
   Le fichier `auth-connector.json5` se situe dans `%APPDATA%\Acronis\AuthConnector`.
3. Accédez à la section **sync** et, à chaque ligne **« connectionMode »**, remplacez **« ssl_only »** par **« auto »**.
   Dans le mode **auto**, une connexion non sécurisée est établie si une connexion TLS est impossible.
4. Redémarrez le service **Acronis Service Manager** comme décrit dans "Pour redémarrer le service Acronis Service Manager" (p. 204).

Remarque
Si le serveur de gestion n'est pas inclus dans un domaine Active Directory ou s'il est installé sur une machine Linux, vous pouvez octroyer des droits d'administration uniquement à des utilisateurs locaux et à des groupes.

Pour savoir comment ajouter un compte d'administration au serveur de gestion, consultez la section "Ajout de comptes d'administration" (p. 669).

Rôles de compte d'administration

Un rôle est affecté à chaque compte d'administration, avec des droits d'accès prédéfinis, nécessaires à des tâches spécifiques. Les rôles de compte d'administration sont les suivants :

- **Administrateur**
  Ce rôle donne un accès administratif complet à l'organisation ou à une unité.
- **Lecture seule**
  Ce rôle donne un accès en lecture seule à la console Web Cyber Protect. Il permet uniquement de collecter des données de diagnostic, comme les rapports système. Le rôle lecture seule ne permet pas de consulter les sauvegardes ni de parcourir le contenu des boîtes aux lettres sauvegardées.
- **Auditeur**
  Ce rôle donne un accès en lecture seule à l'onglet **Activités** de la console Web Cyber Protect. Pour plus d'informations sur cet onglet, reportez-vous à la section "Onglet Activités" (p. 610). Ce rôle ne permet pas la collecte ni l'exportation de données, quelles qu'elles soient, notamment les informations système du serveur de gestion.

Toute modification apportée aux rôles s'affiche dans l'onglet **Activités**.

Héritage des rôles

Les rôles dans une unité parent sont hérités par ses unités enfant. Si le même compte utilisateur possède différents rôles attribués dans l'unité parent et dans une unité enfant, il disposera des deux rôles.

De même, les rôles peuvent être attribués explicitement à un compte utilisateur spécifique, ou bien hérités depuis un groupe d'utilisateurs. Par conséquent, un compte utilisateur peut disposer à la fois d'un rôle attribué de façon spécifique et d'un rôle hérité.

Si un compte utilisateur possède différents rôles (attribués et/ou hérités), il peut accéder effectuer les actions et accéder aux objets autorisés dans n'importe lequel de ces rôles. Par exemple, un compte utilisateur auquel le rôle lecture seule a été affecté et qui a hérité d'un rôle administrateur aura les droits d'un administrateur.

Important
Dans la console Web Cyber Protect, seuls les rôles explicitement attribués pour l'unité actuelle sont affichés. Toute différence potentielle par rapport aux rôles hérités n'est pas affichée. Nous vous recommandons fortement d'attribuer des rôles administrateur, lecture seule et auditeur à des comptes ou groupes séparés, afin d'éviter les problèmes potentiels avec les rôles hérités.

Administrateurs par défaut

Sous Windows

Lors de l'installation du serveur de gestion sur une machine, vous obtenez les résultats suivants :

- Le groupe d'utilisateurs **Acronis Centralized Admins** est créé sur l'ordinateur.
  Sur un contrôleur de domaine, le groupe est appelé *DCNAME* **$ Acronis Centralized Admins**. Ici, *DCNAME* représente le nom du NetBIOS du contrôleur de domaine.
- Tous les membres du groupe **Administrateurs** seront ajoutés au groupe **Acronis Centralized Admins**. Si la machine est dans un domaine mais n'est pas un contrôleur de domaine, les utilisateurs locaux (hors domaine) sont alors exclus. Dans un contrôleur de domaine, il n'y a pas d'utilisateurs hors domaine.
- Les groupes **Administrateurs centralisés Acronis** et **Administrateurs** seront ajoutés au serveur de gestion en tant qu'**administrateurs de l'organisation**. Si la machine est dans un domaine mais n'est pas un contrôleur de domaine, le groupe **Administrateurs** n'est pas ajouté, de sorte que les utilisateurs locaux (hors domaine) ne deviennent pas administrateurs de l'organisation.

Vous pouvez supprimer le groupe **Administrateurs** de la liste des administrateurs de l'organisation. Toutefois, le groupe **Acronis Centralized Admins** ne peut pas être supprimé. Dans le cas peu probable où tous les administrateurs de l'organisation auraient été supprimés, vous pouvez ajouter un compte au groupe **Acronis Centralized Admins** dans Windows, puis vous connecter à la console Web Cyber Protect à l'aide de ce compte.

Sous Linux

Lors de l'installation du serveur de gestion sur une machine, l'utilisateur **root** est ajouté au serveur de gestion comme un **administrateur de l'organisation**.

Vous pouvez ajouter d'autres utilisateurs Linux dans la liste des administrateurs du serveur de gestion comme décrit ultérieurement, puis supprimer l'utilisateur **root** de cette liste. Dans le cas peu probable où tous les administrateurs de l'organisation auraient été supprimés, vous pouvez redémarrer le service `acronis_asm`. En conséquence, l'utilisateur **root** sera automatiquement rajouté comme administrateur de l'organisation.

Compte d'administration dans plusieurs unités

Des droits d'administration peuvent être accordés à un compte dans n'importe quel nombre d'unités. Pour un tel compte, ainsi que pour les comptes d'administration au niveau de l'organisation, le sélecteur d'unité s'affiche dans la console Web Cyber Protect. Grâce à ce sélecteur, ce compte peut voir et gérer chaque unité indépendamment.

Un compte ayant les droits nécessaires pour toutes les unités d'une organisation n'a pas nécessairement les droits nécessaires pour l'organisation. Les comptes d'administration au niveau de l'organisation doivent être ajoutés explicitement au groupe **Organisation**.

Comment peupler les unités avec des machines

Quand un administrateur ajoute une machine via l'interface Web, elle est ajoutée à l'unité gérée par l'administrateur. Si l'administrateur gère plusieurs unités, la machine est ajoutée à l'unité choisie

dans le sélecteur d'unités. De ce fait, l'administrateur doit choisir l'unité avant de cliquer sur **Ajouter**.

Lors de l'installation locale d'agents, l'administrateur fournit ses accréditations. La machine est ajoutée à l'unité gérée par l'administrateur. Si l'administrateur gère plusieurs unités, le programme d'installation invite à choisir une unité à laquelle la machine sera ajoutée.

Ajout de comptes d'administration

Remarque
Cette fonctionnalité n'est pas disponible dans les éditions Standard Edition et Essentials Edition.

Pour ajouter des comptes

1. Cliquez sur **Paramètres** > **Comptes**.
   Le logiciel affiche la liste des administrateurs de serveur de gestion et l'arborescence des unités (le cas échéant).
2. Sélectionnez **Organisation** ou sélectionnez l'unité dans laquelle vous souhaitez ajouter un administrateur.
3. Cliquez sur **Ajouter un compte**.
4. Dans **Domaine**, sélectionnez le domaine qui contient les comptes d'utilisateur que vous désirez ajouter. Si le serveur de gestion n'est pas inclus dans un domaine Active Directory ou installé sur Linux, seuls les utilisateurs locaux peuvent être ajoutés.
5. Cherchez le nom d'utilisateur ou du groupe d'utilisateurs.
6. Cliquez sur « + » à côté du nom de l'utilisateur ou du groupe.
7. Sélectionnez le rôle du compte.
8. Répétez les étapes 4 à 6 pour tous les utilisateurs ou groupes que vous souhaitez ajouter.
9. Lorsque vous avez terminé, cliquez sur **Terminé**.
10. [Uniquement sur Linux] Ajoutez les noms d'utilisateur à la configuration du Module d'Authentification Enfichable (PAM) pour les modules Acronis comme décrit ci-dessous.

Pour ajouter des noms d'utilisateur à la configuration du PAM pour Acronis

Cette procédure s'applique au serveur de gestion exécuté sur les ordinateurs Linux et dans l'appliance tout-en-un Acronis Cyber Protect.

1. Sur la machine exécutant le serveur de gestion, en tant qu'utilisateur root, ouvrez le fichier **/etc/security/acronisagent.conf** avec un éditeur de texte.
2. Dans ce fichier, saisissez les noms d'utilisateur que vous avez ajoutés en tant qu'administrateurs du serveur de gestion, un par ligne.
3. Enregistrez et fermez le fichier.

Création d'unités

1. Cliquez sur **Paramètres** > **Comptes**.
2. Le logiciel affiche la liste des administrateurs de serveur de gestion et l'arborescence des unités (le cas échéant).
3. Sélectionnez **Organisation** ou l'unité parente pour la nouvelle unité.
4. Cliquez sur **Créer une unité**.
5. Spécifiez un nom pour la nouvelle unité, puis cliquez sur **Créer**.

Déploiement Cloud

L'administration des comptes d'utilisateur et des unités de l'organisation est disponible dans le portail de gestion. Pour accéder au portail de gestion, cliquez sur **Portail de gestion** lorsque vous vous connectez au service de cyberprotection ou cliquez sur l'icône  dans le coin supérieur droit, puis sur **Portail de gestion**. Seuls les utilisateurs possédants les droits d'administrateur peuvent accéder à ce portail.

Pour plus d'informations sur l'administration des comptes d'utilisateur et des unités de l'organisation, veuillez consulter le Guide de l'administrateur du portail de gestion. Pour accéder à ce document, cliquez sur l'icône en forme de point d'interrogation dans le portail de gestion.

Cette section fournit des informations complémentaires sur la gestion du service de cyber protection.

Quotas

Les quotas vous permettent de limiter la capacité de l'utilisateur à utiliser le service. Pour définir les quotas, sélectionnez l'utilisateur dans l'onglet **Utilisateurs**, puis cliquez sur l'icône en forme de crayon dans la section **Quotas**.

Lorsqu'un quota est dépassé, une notification est envoyée à l'adresse e-mail de l'utilisateur. Si vous ne définissez pas un dépassement de quota, le quota est considéré comme « souple ». Cela signifie que les restrictions d'utilisation du service de cyber protection ne sont pas activées.

Vous pouvez également spécifier les dépassements de quota. Un dépassement permet à un utilisateur de dépasser le quota, selon la valeur indiquée. Lorsque le dépassement est atteint, des restrictions sont appliquées à l'utilisation du service de cyber protection.

Sauvegarde

Indiquez le quota de stockage dans le Cloud, le quota de sauvegarde au niveau local et le nombre maximum de machines/terminaux/boîtes aux lettres/ qu'un utilisateur est autorisé à protéger. Les quotas suivants sont disponibles :

- **Stockage dans le Cloud**
- **Postes de travail**
- **Serveurs**
- **Windows Server Essentials**
- **Hôtes virtuels**
- **Universelle**
  Ce quota peut être utilisé à la place d'un des quatre quotas répertoriés ci-dessus : Stations de travail, serveurs, Windows Server Essentials, hôtes virtuels.
- **Terminaux mobiles**
- **Boîtes aux lettres Microsoft 365**
- **Sauvegarde locale**

Un ordinateur, un terminal ou une boîte aux lettres sont considérés comme protégés tant qu'au moins un plan de protection leur est appliqué. Un terminal mobile devient protégé après la première sauvegarde.

Lorsque le dépassement de quota de stockage dans le Cloud est dépassé, la sauvegarde échoue. Lorsque le dépassement du quota de périphériques est atteint, l'utilisateur ne peut plus activer de plans de protection sur d'autres périphériques.

Le quota **Sauvegarde locale** limite la taille totale des sauvegardes locales créées à l'aide de l'infrastructure Cloud. Aucun dépassement ne peut être défini pour ce quota.

Reprise d'activité après sinistre

Ces quotas sont appliqués par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs de l'entreprise peuvent afficher les quotas et l'utilisation dans le portail de gestion, mais ne peuvent pas définir de quotas pour un utilisateur.

- **Stockage pour la reprise d'activité après sinistre**
  Ce stockage est utilisé par les serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible de créer des serveurs primaires et de restauration, ou d'ajouter/étendre des disques à des serveurs primaires existants. Si le quota est dépassé, il n'est pas possible d'initier un basculement ni de simplement démarrer un serveur arrêté. Les serveurs en cours d'exécution continuent à fonctionner.
  Lorsque le quota est désactivé, tous les serveurs sont supprimés. L'onglet **Site de restauration dans le Cloud** disparaît de la console Web Cyber Protect.
- **Points de calcul**
  Ce quota limite les ressources processeur et les ressources RAM utilisées par les serveurs primaires et de restauration pendant une période de facturation. Si le quota est atteint, tous les serveurs primaires et de restauration sont coupés. Ces serveurs ne pourront plus être utilisés avant le début de la prochaine période de facturation. La période de facturation par défaut est un mois complet.

Lorsque le quota est désactivé, les serveurs ne peuvent pas être utilisés, quelle que soit la période de facturation.

- **Adresses IP publiques**

  Ce quota limite le nombre d'adresses IP publiques qui peuvent être attribuées à des serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible d'activer des adresses IP publiques pour d'autres serveurs. Vous pouvez interdire à un serveur d'utiliser une adresse IP publique en désactivant la case à cocher **Adresse IP publique** dans les paramètres du serveur. Après cela, vous pouvez autoriser un autre serveur à utiliser une adresse IP publique, qui ne sera généralement pas la même.

  Lorsque le quota est désactivé, tous les serveurs cessent d'utiliser des adresses IP publiques et ne sont donc plus accessibles depuis Internet.
- **Serveurs Cloud**

  Ce quota limite le nombre total de serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible de créer des serveurs primaires ou de restauration.

  Lorsque le quota est désactivé, les serveurs sont visibles dans la console Web Cyber Protect, mais seule l'option **Supprimer** est disponible.
- **Accès Internet**

  Ce quota active ou désactive l'accès à Internet à partir de serveurs primaires ou de restauration.

  Lorsque ce quota est désactivé, les serveurs primaires ou de restauration sont immédiatement déconnectés d'Internet. Le commutateur **Accès Internet** présent dans les propriétés du serveur est décoché et désactivé.

Notifications

Pour modifier les paramètres de notifications pour un utilisateur, sélectionnez l'utilisateur dans l'onglet **Utilisateurs**, puis cliquez sur l'icône en forme de crayon dans la section **Paramètres**. Les paramètres de notifications suivants sont disponibles :

- **Notifications relatives aux dépassements de quotas** (activé par défaut)

  Les notifications relatives aux dépassements de quotas.
- **Rapports d'utilisation planifiés**

  Les rapports d'utilisation décrits ci-dessous sont envoyés le premier jour de chaque mois.
- **Notifications d'échec**, **Notifications d'avertissement** et **Notifications de réussite** (désactivées par défaut)

  Les notifications relatives aux résultats d'exécution des plans de protection et aux résultats des opérations de reprise d'activité après sinistre pour chaque appareil.
- **Résumé quotidien concernant les alertes actives** (activé par défaut)

  Ce résumé vous tient informé des échecs de sauvegarde, des sauvegardes manquées et des autres problèmes éventuels. Le résumé est envoyé à 10 h (heure du centre de données). Si il n'y a aucun problème, aucun résumé n'est envoyé.

Toutes les notifications sont envoyées à l'adresse e-mail de l'utilisateur.

Rapports

Le rapport sur l'utilisation du service de cyber protection comprend les informations suivantes à propos de l'organisation ou d'une unité :

- Le volume des sauvegardes par unité, par utilisateur et par type de périphérique.
- Le nombre de périphériques protégés par unité, par utilisateur et par type de périphérique.
- La valeur par unité, par utilisateur et par type de périphérique.
- Le volume total de sauvegardes.
- Le nombre total de périphériques protégés.
- La valeur totale.

Référence pour la ligne de commande

La référence pour la ligne de commande est un document séparé disponible sur https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html.

Dépannage

Cette section décrit comment enregistrer le journal d'un 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.

Pour rassembler les journaux

1. Effectuez l'une des actions suivantes :
   - Dans **Périphériques**, sélectionnez la machine depuis laquelle vous voulez collecter les journaux, puis cliquez sur **Activités**.
   - Dans **Paramètres** > **Agents**, sélectionnez la machine depuis laquelle vous voulez collecter les journaux, puis cliquez sur **Détails**.
2. Cliquez sur **Collecter les informations système**.
3. Si vous y êtes invité par votre navigateur Web, indiquez où enregistrer le fichier.

Glossaire

E

Emplacement géré

Un emplacement de sauvegarde géré par un nœud de stockage. Physiquement, des emplacements gérés peuvent se trouver sur un partage réseau, SAN, NAS, sur un disque dur local du nœud de stockage ou sur une bibliothèque de bandes connectée localement au nœud de stockage. Le nœud de stockage effectue un nettoyage et une validation (s'ils sont inclus dans un plan de protection) pour chaque sauvegarde stockée dans l'emplacement géré. Vous pouvez spécifier des opérations supplémentaires que le nœud de stockage effectuera (déduplication, chiffrement).

F

Format de sauvegarde sous forme d'un fichier unique

Nouveau format de sauvegarde, pour lequel les sauvegardes complètes et incrémentielles subséquentes sont enregistrées sous forme d'un fichier .tib unique, plutôt que d'une suite de fichiers. 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, par exemple les serveurs SFTP.

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 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.

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.

Startup Recovery Manager

Une modification de l'agent de démarrage, résidant sur le disque du système et configuré pour démarrer lors du démarrage en pressant F11. Startup Recovery Manager supprime le besoin de connexion réseau ou de support de secours pour démarrer l'utilitaire de démarrage de secours.
Startup Recovery Manager est particulièrement utile pour les utilisateurs mobiles. Si une défaillance se produit, l'utilisateur redémarre l'ordinateur, appuie sur F11 à l'invite « Appuyer sur F11 pour Startup Recovery Manager... » et effectue la récupération de données de la même manière que pour un support de démarrage ordinaire. Limite : nécessite la réactivation des chargeurs autres que les chargeurs Windows et GRUB.

Index

B

C

E

H

I

J

L

M

P

Q

R

S

T

U

V

W