Acronis

acronis.com

Cyber Protect Cloud

25.10

Guía del usuario

REVISIÓN: 10/11/2025

Contenido

Cómo empezar a usar Cyber Protection **22**
Activación de la cuenta 22
Requisitos de contraseña 22
Autenticación de doble factor 22
Configuración de privacidad 25
Acceso a los servicios de Cyber Protection 25
Navegadores web compatibles 26
Mi bandeja de entrada 27
Información general 27
Comprobación de sus notificaciones 27
Búsqueda en Mi bandeja de entrada 27
Funciones de protección compatibles con el sistema operativo 28
Sistemas operativos y versiones compatibles 28
Instalación e implementación de los agentes de Cyber Protection **38**
Antes de empezar 38
Preparación 38
Copia de seguridad basada en agente y sin agente 41
¿Qué Agente necesito? 42
Requisitos del sistema para agentes 47
Descarga de agentes de protección 49
Paquetes de Linux necesarios para la instalación de agentes en Linux 50
Ajuste de la configuración del servidor proxy 53
Instalación dinámica de componentes 57
Conceder los permisos de sistema necesarios para el Agente de Connect 58
Modo compatible con FIPS 60
Instalación del Agente para Windows en modo compatible con FIPS 61
Instalación del Agente para Linux en el modo compatible con FIPS 64
Habilitación del modo compatible con FIPS para un dispositivo virtual 65
Instalación de agentes de protección utilizando la interfaz gráfica de usuario 65
Instalación de agentes de protección en Windows 65
Instalación de agentes de protección en Linux 70
Instalación de agentes de protección en macOS 72
Desinstalación de agentes 73
Instalación y desinstalación de agentes de protección utilizando la interfaz de línea de comandos 75

© Acronis International GmbH, 2003-2025

Instalación y desinstalación de agentes de protección en Windows ... 75
Ejemplos ... 76
Ejemplo ... 77
Ejemplos ... 78
Ejemplos ... 86
Ejemplo ... 87
Ejemplos ... 87
Instalación y desinstalación de agentes de protección en Linux ... 93
Instalación y desinstalación de agentes de protección en macOS ... 100
Registro de cargas de trabajo ... 109
Registro de cargas de trabajo utilizando la interfaz gráfica de usuario ... 110
Registro y anulación de registro de cargas de trabajo utilizando la interfaz de línea de comandos ... 115
Cambio de registro de una carga de trabajo ... 120
Traslado de cargas de trabajo a otro inquilino ... 121
Actualización de agentes de protección ... 121
Espacio libre en disco que se requiere para la actualización ... 121
Configuración del método predeterminado para actualizar agentes ... 122
Actualización manual de agentes de protección ... 128
Actualización de agentes de protección automática ... 130
Actualización de agentes de protección en cargas de trabajo cifradas con BitLocker ... 133
Despliegue de agentes de protección a través de la directiva de grupo ... 134
Requisitos previos ... 134
Creación del archivo de transformación y extracción de los paquetes de instalación ... 135
Configurar el objeto de directiva de grupo ... 135
Despliegue de dispositivos virtuales ... 137
Implementación de Agente para VMware (dispositivo virtual) ... 137
Implementación de Agent para Scale Computing HC3 (dispositivo virtual) ... 141
Implementación del Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual) ... 147
Ejemplos ... 150
Ejemplos ... 154
Implementando Agent para oVirt (dispositivo virtual) ... 159
Despliegue del agente para Azure ... 166
Despliegue de Agente para Nutanix AHV ... 171
Implementar Agente para Synology ... 176
Conexiones SSH a un dispositivo virtual ... 185
Detección de dispositivos ... 186

© Acronis International GmbH, 2003-2025

Detección de varios dispositivos ... 187
Detección de dispositivos mediante Device Sense ™ ... 194
Vista de la información sobre los dispositivos detectados ... 200
Instalación remota de agentes ... 201
Exclusión de dispositivos de la detección ... 209
Conexión remota a dispositivos descubiertos ... 210
Detección pasiva de la solución de problemas ... 211
Evitar la desinstalación o modificación de agentes no autorizadas ... 212
Cambiar la cuota de servicio de cargas de trabajo ... 214
Configuración de la protección ... 215
Actualizaciones automáticas de los componentes ... 215
Recopilación automática de datos de rendimiento ... 217
Actualización de las definiciones de Cyber Protection mediante la planificación ... 217
Actualización de las definiciones de Cyber Protection bajo demanda ... 218
Almacenamiento en caché ... 218
servicios de Cyber Protection instalados en su entorno ... 219
Servicios instalados en Windows ... 219
Servicios instalados en macOS ... 219
Guardar un archivo de registro del agente ... 219
Gestión de licencias para servidores de gestión locales ... 220
Trabajo con planes ... 221
Compresión de los planes ... 221
Planes integrados ... 224
Planes predeterminados ... 237
Planes favoritos ... 240
Planes preseleccionados ... 244
Planes en diferentes niveles de administración ... 246
Estado del plan ... 248
Planes de protección y módulos ... 249
Creación de un plan de protección ... 250
Acciones con planes de protección ... 251
Planes de protección individual para integraciones del panel de control de alojamiento ... 257
Problemas de compatibilidad con los planes ... 257
Resolver problemas de compatibilidad ... 258
Planes de protección de datos fuera del host ... 260
Réplica de copia de seguridad ... 261
Validación ... 264

© Acronis International GmbH, 2003-2025

Limpieza ... 272
Conversión a equipo virtual ... 273
Planes de análisis de copia de seguridad ... 277
Planes de copias de seguridad para aplicaciones en la nube ... 278
Protección de aplicaciones de colaboración y comunicación ... 279
Planes de reenvío de SIEM ... 279
Capacidades SIEM de Acronis ... 280
Listas de planes de reenvío SIEM ... 280
Creación de un plan de reenvío SIEM genérico para múltiples clientes ... 281
Creación de un plan SIEM para un cliente individual ... 283
Renombrar un plan de reenvío SIEM ... 285
Modificación de un plan de reenvío SIEM ... 285
Eliminación de un plan SIEM ... 286
Métodos de planes de reenvío SIEM ... 286
Cómo comprender el nivel de protección actual ... 288
Supervisión ... 288
Panel de control de Información general ... 288
Panel de control Actividades ... 289
Panel de control de Alertas ... 290
Cyber Protection ... 329
Estado de la protección ... 330
Widgets de Endpoint Detection and Response (EDR) ... 331
#CyberFit Score por equipo ... 335
Supervisión del estado del disco ... 336
Mapa de protección de datos ... 340
Widget de dispositivos detectados ... 342
Widgets de evaluación de vulnerabilidades ... 342
Widgets de instalación de parches ... 343
Detalles del análisis de copias de seguridad ... 345
Elementos afectados recientemente ... 345
Aplicaciones de Cloud ... 346
Widgets de software ... 347
Widgets de inventario de hardware ... 350
Widget de sesiones remotas ... 351
Protección inteligente ... 352
La pestaña Actividades ... 359
Cyber Protect Monitor ... 360

© Acronis International GmbH, 2003-2025

Configuración del servidor proxy en Cyber Protect Monitor ... 362
Chats en el Monitor ... 363
Informes ... 365
Acciones con informes ... 367
Datos informados según el tipo de widget ... 369
Gestión de cargas de trabajo en la consola de Cyber Protect ... 372
Consola de Cyber Protect ... 372
Novedades de la consola de Cyber Protect ... 373
Niveles de administración en la consola de Cyber Protect ... 373
Requisitos previos ... 378
Uso de comodines para definir exclusiones ... 382
Uso de variables para definir exclusiones ... 383
Cargas de trabajo ... 383
Adición de cargas de trabajo a la consola de Cyber Protect ... 385
Eliminación de cargas de trabajo de la consola de Cyber Protect ... 390
Tipos de recurso ... 394
Grupos de los dispositivos ... 406
Grupos integrados y grupos personalizados ... 407
Grupos dinámicos y estáticos ... 407
Grupos de nube a nube y grupos que no son de nube a nube ... 408
Creación de un grupo estático ... 409
Añadir cargas de trabajo a un grupo estático ... 411
Creación de un grupo dinámico ... 411
Edición de un grupo dinámico ... 431
Eliminar un grupo ... 432
Aplicar un plan a un grupo ... 433
Revocación de un plan desde un grupo ... 434
Cómo trabajar con el módulo de control de dispositivos ... 434
Uso del control de dispositivos ... 437
Configuración del acceso ... 445
Lista de tipos de dispositivo permitidos ... 450
Lista de dispositivos USB permitidos ... 452
Exclusión de procesos del control de acceso ... 456
Alertas de control de dispositivos ... 458
Borrado de datos de una carga de trabajo gestionada ... 462
Ver cargas de trabajo gestionados por integraciones RMM ... 463
Cargas de trabajo de CyberApp ... 464

© Acronis International GmbH, 2003-2025

Cargas de trabajo agregadas ... 464
Trabajar con cargas de trabajo de CyberApp ... 465
Trabajar con cargas de trabajo agregadas ... 465
Vinculación de cargas de trabajo a usuarios específicos ... 467
Viendo el último usuario que ha iniciado sesión ... 467
#CyberFit Score para equipos ... 468
Cómo funciona ... 468
Ejecución de un análisis #CyberFit Score ... 472
Secuencia de comandos cibernética ... 474
Requisitos previos ... 474
Limitaciones ... 475
Plataformas compatibles ... 475
Roles de usuario y derechos de la Programación cibernética ... 476
Secuencias de comandos ... 478
Depósito de secuencia de comandos ... 488
Planes de programación ... 489
Ejecución rápida de la secuencia de comandos ... 496
Gestión de la copia de seguridad y recuperación de cargas de trabajo y archivos ... 499
Sistemas operativos y entornos compatibles para la copia de seguridad y la recuperación ... 499
Agente para Windows ... 499
Agente para Windows (heredado) ... 500
Agente para SQL, Agente para Active Directory y Agente para Exchange (para copia de seguridad de bases de datos y copias de seguridad compatibles con la aplicación) ... 501
Agente para la prevención de la pérdida de datos ... 502
Agente para File Sync & Share ... 502
Agente para Exchange (para la copia de seguridad de buzones de correo) ... 503
Agente para Microsoft 365 ... 503
Agente para Oracle ... 504
Agente para MySQL/MariaDB ... 504
Agente para Linux ... 504
Agente para Mac ... 506
Agente para VMware (dispositivo virtual) ... 507
Agente para VMware (Windows) ... 507
Agente para Hyper-V ... 507
Agente para Virtuozzo ... 508
Agente para la Virtuozzo Hybrid Infrastructure ... 508
Agent para Scale Computing HC3 ... 508

© Acronis International GmbH, 2003-2025

Agente para oVirt ... 508
Agente para Synology ... 509
Agente para Azure ... 509
Agente para Nutanix ... 509
Cyber Protect Monitor ... 509
Versiones compatibles de Microsoft SQL Server ... 509
Versiones compatibles de Microsoft Exchange Server ... 510
Versiones de Microsoft SharePoint compatibles ... 510
Versiones de Oracle Database compatibles ... 511
Versiones de SAP HANA compatibles ... 511
Versiones de MySQL admitidas ... 511
Versiones de MariaDB admitidas ... 511
Plataformas de virtualización compatibles ... 511
Compatibilidad con almacenamientos Dell EMC Data Domain ... 524
Sistemas de archivos compatibles ... 525
Operaciones admitidas con volúmenes lógicos ... 529
Compatibilidad con software de cifrado ... 531
Compatibilidad con discos duros de formato avanzado (sector de 4 K) ... 532
Copia de seguridad ... 533
Hoja de referencia de la copia de seguridad ... 535
¿Cuánto tiempo se conservarán las copias de seguridad? ... 537
Seleccionar los datos que se incluirán en la copia de seguridad ... 538
Selección de todo el equipo ... 538
Seleccionar discos o volúmenes ... 538
Seleccionar archivos o carpetas ... 542
Seleccionar un estado del sistema ... 545
Selección de la configuración de ESXi ... 546
Seleccionar un destino ... 547
Opción de almacenamiento avanzada ... 548
Acerca de Secure Zone ... 549
Protección continua de datos (CDP) ... 552
Cómo funciona ... 552
Fuentes de datos compatibles ... 554
Destinos compatibles ... 555
Configuración de una copia de seguridad de CDP ... 555
Programación de copia de seguridad ... 556
Esquemas de copia de seguridad ... 557

© Acronis International GmbH, 2003-2025

Tipos de copia de seguridad 559
Ejecutar una copia de seguridad en una planificación 559
Ejecutar una copia de seguridad manualmente 574
Normas de retención 575
Consejos importantes 576
Reglas de retención según el esquema de copias de seguridad 577
Configuración de reglas de retención 580
Replicación 581
Ejemplos de uso 581
Ubicaciones compatibles 581
Cifrado 583
Configurar el cifrado en el plan de protección 584
Configurar el cifrado como una propiedad del equipo 584
Notarización 587
Cómo utilizar la notarización 588
Cómo funciona 588
Opciones de copia de seguridad predeterminadas 588
Opciones de copia de seguridad 589
Disponibilidad de las opciones de copia de seguridad 589
Alertas 592
Puntos de restauración de Azure 593
Consolidación de la copia de seguridad 595
Nombre del archivo de copia de seguridad. 596
Formato de la copia de seguridad 600
Validación de la copia de seguridad 602
Seguimiento de bloques modificados (CBT) 602
Modo de copia de seguridad de clústeres 603
Tasa de compresión 605
Control de errores 605
Copias de seguridad incrementales/diferenciales rápidas 607
Filtros de archivo (inclusiones y exclusiones) 607
Instantánea de la copia de seguridad a nivel de archivo 615
Datos forenses 616
Truncamiento de registros 625
Toma de instantáneas de LVM 626
Puntos de montaje 626
Instantánea multivolumen 627

© Acronis International GmbH, 2003-2025

Recuperación con un clic ... 628
Ventana de copia de seguridad y rendimiento ... 633
Envío de datos físicos ... 637
Comandos previos/posteriores ... 639
Comandos previos o posteriores a la captura de datos ... 642
Planificación ... 645
Copia de seguridad sector por sector ... 646
División ... 646
Manejo de fallos de la tarea ... 647
Condiciones de inicio de la tarea ... 647
Servicio de instantáneas de volumen (VSS) ... 648
Servicio de instantáneas de volumen (VSS) para equipos virtuales ... 650
Copia de seguridad semanal ... 652
Registro de eventos de Windows ... 653
Recuperación ... 653
Recuperación de apuntes ... 653
Recuperación multiplataforma ... 655
Recuperación de equipos físicos ... 663
Recuperación del equipos virtuales ... 678
Recuperar discos usando dispositivos de arranque ... 693
Recuperación de archivos ... 695
Recuperación del estado del sistema ... 703
Recuperación de la configuración de ESXi ... 703
Recuperación con reinicio ... 704
Uso de Universal Restore ... 707
Opciones de recuperación ... 710
Recuperación segura ... 719
Operaciones con copias de seguridad ... 720
Almacenamiento de copias de seguridad ... 720
Montaje de volúmenes desde una copia de seguridad ... 723
Validación de copias de seguridad ... 725
Exportación de copias de seguridad ... 725
Eliminación de copias de seguridad ... 727
Descripción de la detección de atascos ... 729
Hacer copias de seguridad de cargas de trabajo en nubes públicas ... 734
Definir una ubicación de copia de seguridad en Microsoft Azure ... 734
Definición de una ubicación de copia de seguridad en Amazon S3 ... 737

© Acronis International GmbH, 2003-2025

Definición de una ubicación de copia de seguridad en un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3 ... 742
Visualización y actualización de ubicaciones de copia de seguridad en la nube pública ... 747
Gestionar el acceso a la cuenta de la nube pública ... 748
Archivado de correos electrónicos ... 762
Limitaciones ... 763
Configuración del archivado de correos electrónicos ... 763
Planes de archivos comprimidos ... 766
Importando correos electrónicos desde archivos PST ... 769
Consultas de búsqueda ... 771
Normas de retención ... 779
Reglas de retención legales ... 783
Recuperación de datos de un archivo comprimido de correos electrónicos ... 787
Almacenamiento inmutable para el archivado de correos electrónicos ... 791
Protección de aplicaciones de Microsoft ... 792
Protección de Microsoft SQL Server y Microsoft Exchange Server ... 792
Protección de Microsoft SharePoint ... 793
Protección de un controlador de dominio ... 793
Recuperación de aplicaciones ... 793
Requisitos para copias de seguridad con información de aplicaciones ... 794
Copia de seguridad de la base de datos ... 797
Copia de seguridad compatible con la aplicación ... 803
Copia de seguridad de casillas de correo ... 807
Recuperación de bases de datos SQL ... 809
Recuperación de bases de datos de Exchange ... 817
Recuperación de elementos de buzón de correo y de buzones de correo de Exchange ... 821
Cambio de las credenciales de acceso de SQL Server o Exchange Server ... 828
Protección de dispositivos móviles ... 828
Dispositivos móviles compatibles ... 829
De qué puede realizar una copia de seguridad ... 829
Qué necesita saber ... 829
Dónde obtener la aplicación Acronis Cyber Protect ... 830
Cómo empezar a realizar copias de seguridad de los datos ... 830
Cómo recuperar los datos en un dispositivo móvil ... 831
Cómo revisar los datos a través de la consola de Cyber Protect ... 831
Protección de los datos de Microsoft 365 ... 833
Comparación de soluciones de copia de seguridad para datos de Microsoft 365 ... 833

© Acronis International GmbH, 2003-2025

Derechos de usuario necesarios ... 839
Cómo añadir una organización de Microsoft 365 ... 841
Administración de organizaciones de Microsoft 365 añadidas en diferentes niveles ... 843
Detección de recursos de Microsoft 365 ... 843
Cómo eliminar una organización de Microsoft 365 ... 845
Revocación de los derechos de acceso de la aplicación de servicio de copia de seguridad ... 846
Informe de licencia de usuarios de Microsoft 365 ... 846
Configuración de la frecuencia de las copias de seguridad de Microsoft 365 ... 847
Microsoft 365 Business (copia de seguridad) ... 848
Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365 ... 891
Agente instalado de forma local para Office 365 ... 902
Protección de los datos de Google Workspace ... 907
¿Qué implica la protección de Google Workspace? ... 907
Derechos de usuario necesarios ... 907
Acerca de la planificación de copia de seguridad ... 908
Limitaciones ... 908
Incorporación de una organización de Google Workspace ... 909
Cree un proyecto personal de Google Cloud ... 910
Detección de los recursos de Google Workspace ... 914
Configuración de la frecuencia de las copias de seguridad de Google Workspace ... 914
Protección de los datos de Gmail ... 915
Protección de archivos de Google Drive ... 920
Protección de archivos de unidades compartidas ... 925
Notarización ... 929
Búsqueda en copias de seguridad de nube a nube ... 931
Búsqueda en todo el texto ... 932
Índices de búsqueda ... 932
Comprobar el tamaño de un índice de búsqueda ... 933
Actualizar, reconstruir o eliminar índices ... 933
Habilitar la búsqueda mejorada en copias de seguridad cifradas ... 934
Deshabilitar la búsqueda de texto completo para las copias de seguridad de Gmail ... 935
Protección de base de datos de Oracle ... 936
Protección de SAP HANA ... 936
Protección de datos de MySQL y MariaDB ... 936
Configurar una copia de seguridad con información de aplicaciones ... 938
Recuperación de datos a partir de una copia de seguridad con información de aplicaciones ... 939
Protección de los equipos virtuales y contenedores Proxmox ... 943

© Acronis International GmbH, 2003-2025

Limitaciones para cargas de trabajo de Proxmox ... 944
Instalación de Agente para Proxmox ... 945
Copia de seguridad de cargas de trabajo de Proxmox ... 946
Recuperación de cargas de trabajo de Proxmox ... 946
Protección de sitios web y servidores de alojamiento ... 946
Protección de los sitios web ... 946
Protección de servidores de alojamiento web ... 950
Operaciones especiales con equipos virtuales ... 951
Ejecución de un equipo virtual desde una copia de seguridad (Instant Restore) ... 951
Trabajar en VMware vSphere ... 955
Copia de seguridad de equipos Hyper-V en clúster ... 979
Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo ... 980
Copia de seguridad basada en agente de máquinas virtuales de Microsoft Azure y Amazon EC2 ... 982
Creación de soportes de arranque para recuperar sistemas operativos ... 983
¿Un dispositivo de arranque personalizado o uno disponible? ... 983
¿Dispositivos de arranque basados en Linux o en WinPE/WinRE? ... 984
Creación de un dispositivo de arranque físico ... 984
Bootable Media Builder ... 985
Recuperación desde el almacenamiento en la nube ... 990
Recuperación desde un recurso compartido de red ... 990
Archivos de un script ... 991
Estructura de autostart.json ... 992
Objeto de nivel superior ... 992
Objeto de variable ... 992
Tipo de control ... 993
Conexión a un equipo que se inició desde un dispositivo de arranque ... 1001
Operaciones locales con dispositivos de arranque ... 1002
Operaciones remotas con soportes de arranque ... 1003
Soporte para agrupación de tarjetas NIC ... 1005
Startup Recovery Manager ... 1007
Implementación de la recuperación ante desastres ... 1010
Acerca de Acronis Disaster Recovery ... 1010
Disaster Recovery para Cyber Protect Cloud ... 1010
La funcionalidad clave ... 1010
Requisitos de software para Disaster Recovery para Cyber Protect Cloud ... 1011

© Acronis International GmbH, 2003-2025

Producto de prueba de Disaster Recovery 1014
Operaciones con máquinas virtuales de Microsoft Azure 1014
Limitaciones al usar el almacenamiento en la nube con redundancia geográfica 1015
Eliminación automática de entornos de clientes que no se usan en el sitio en la nube 1015
Trabajo con Disaster Recovery a Cyber Protect Cloud 1016
Creación de un plan de protección de recuperación ante desastres 1016
Conectividad y redes 1020
Requisitos previos 1023
Requisitos del sistema 1026
Puertos 1027
Requisitos previos 1046
Requisitos previos 1048
Servidores de nube 1060
Puntos de cálculo 1076
Conmutación por error de prueba 1078
Conmutación por error de prueba automatizada 1080
Conmutación por error de producción 1082
Conmutación por recuperación 1086
Organización (runbooks) 1099
Eliminar el sitio de recuperación ante desastres 1105
Disaster Recovery para Microsoft Azure 1106
Requisitos de software para Disaster Recovery en Microsoft Azure 1107
Licencia de Disaster Recovery para Microsoft Azure 1109
Trabajar con Disaster Recovery en Microsoft Azure 1109
Gestionar el acceso a su suscripción de Microsoft Azure 1110
Problemas de configuración entre suscripciones en Microsoft Azure 1111
Creación de un plan de protección de recuperación ante desastres con Microsoft Azure 1111
Gestión del sitio de recuperación ante desastres en Microsoft Azure 1112
Conectividad y redes en Microsoft Azure 1115
Servidores de recuperación en Microsoft Azure 1121
Conmutación por error en Microsoft Azure 1126
Conmutación tras recuperación en Microsoft Azure 1135
Runbooks en Microsoft Azure 1149
Recursos de Azure que se crean durante la configuración del sitio de DR y la conmutación por error 1154
Eliminación reversible de inquilinos que tienen un sitio de recuperación en Microsoft Azure 1154
Trabajadores en Microsoft Azure 1155

© Acronis International GmbH, 2003-2025

Panel de control de recuperación ante desastres ... 1155
Dispositivos elegibles para la recuperación ante desastres ... 1155
Comprobación del estado ... 1156
Conmutación por error de prueba automatizada ... 1156
Servidores de recuperación en modo de conmutación por error ... 1157
Servidores principales ... 1157
Alertas del servidor en la nube ... 1158
Uso de puntos de cálculo ... 1158
Compatibilidad de Disaster Recovery con el software de cifrado ... 1158
Configuración de la protección antivirus y antimalware ... 1160
Sistemas operativos compatibles para la protección antivirus y antimalware ... 1160
Funciones compatibles por plataforma ... 1161
Protección antivirus y antimalware ... 1164
Características de la protección antimalware ... 1164
Tipos de análisis ... 1164
Configuración de los ajustes de la protección antivirus y antimalware ... 1166
Active Protection en la edición Cyber Backup Standard ... 1183
Configuración de Active Protection en Cyber Backup Standard ... 1184
Filtrado de URL ... 1192
Cómo funciona ... 1193
Flujo de trabajo de la configuración del filtrado de URL ... 1195
Ajustes del filtrado de URL ... 1195
Antivirus Microsoft Defender y Microsoft Security Essentials ... 1203
Planificar análisis ... 1204
Acciones predeterminadas ... 1205
Protección en tiempo real ... 1205
Avanzado ... 1206
Exclusiones ... 1207
Gestión del cortafuegos ... 1207
Cuarentena ... 1208
¿Cómo llegan los archivos a la carpeta de cuarentena? ... 1209
Gestión de los archivos que están en cuarentena ... 1209
Ubicación de la carpeta Cuarentena en los equipos ... 1210
Carpeta personalizada de autoservicio bajo demanda ... 1210
Lista de permitidos corporativa ... 1210
Inclusión automática de aplicaciones en la lista blanca ... 1211
Inclusión manual de aplicaciones en la lista blanca ... 1211

© Acronis International GmbH, 2003-2025

Añadir archivos en cuarentena a la lista blanca ... 1211
Configuración de la lista blanca ... 1212
Visualización de detalles sobre elementos de la lista blanca ... 1212
Análisis antimalware de copias de seguridad ... 1212
Limitaciones ... 1214
Trabajar con funciones de protección avanzada ... 1215
Advanced Data Loss Prevention ... 1217
Creación de la directiva de flujo de datos y reglas de la directiva ... 1218
Habilitar Advanced Data Loss Prevention en los planes de protección ... 1228
Detección automatizada de destino ... 1231
Definiciones de datos confidenciales ... 1232
Eventos para la prevención de pérdida de datos ... 1238
Widgets de Advanced Data Loss Prevention en el panel de control Información general ... 1240
Categorías de confidencialidad personalizadas ... 1241
Detectores de contenido personalizados ... 1242
Mapa de la organización ... 1245
Problemas conocidos y limitaciones ... 1248
RMM ... 1249
Endpoint Detection and Response (EDR) ... 1250
Por qué necesita Endpoint Detection and Response (EDR) ... 1250
Habilitación de la funcionalidad Endpoint Detection and Response (EDR) ... 1254
Cómo se utiliza Endpoint Detection and Response (EDR) ... 1257
Ver qué incidentes no se han mitigado actualmente ... 1261
Entender el ámbito y el impacto de los incidentes ... 1262
Cómo agregar o quitar columnas en la vista de diseño de tabla ... 1268
Sintaxis ... 1271
Consultas de muestra ... 1273
Tipos de eventos y campos ... 1274
Tipos de eventos ... 1274
Tipos de datos de muestra ... 1275
Campos de eventos ... 1276
Cómo ir a las fases del ataque ... 1291
Habilitar el modo de supervisión para Endpoint Detection and Response (EDR) ... 1335
Cómo probar si Endpoint Detection and Response (EDR) funciona correctamente ... 1337
Extended Detection and Response (XDR) ... 1339
¿Por qué necesita Extended Detection and Response (XDR)? ... 1339
Activación de Extended Detection and Response (XDR) ... 1340

© Acronis International GmbH, 2003-2025

Trabajar con el gráfico XDR ... 1341
Gestión y supervisión del entorno de Microsoft 365 ... 1348
Configuración de conexiones de Microsoft 365 ... 1348
Conexión a una cuenta de Microsoft ... 1349
Asignación de clientes ... 1350
Definición del modo del producto ... 1351
Cómo deshabilitar el servicio de gestión de Microsoft 365 ... 1352
Revisión de la posición de seguridad ... 1352
Revisión del panel de control de riesgos ... 1353
Supervisión de líneas base ... 1355
Supervisión de líneas base de inquilinos ... 1355
Corrección de línea base de inquilinos de forma manual ... 1359
Habilitación o deshabilitación de la corrección automática de las desviaciones de línea base 1360
Gestión de usuarios de Microsoft 365 ... 1361
Incorporación de usuarios ... 1361
Corrección de riesgos de usuario ... 1362
Restablecimiento de contraseñas de usuario ... 1365
Dar de baja a usuarios ... 1365
Gestión del inventario de hardware ... 1367
Habilitar o deshabilitar el análisis de inventario de hardware ... 1367
Inicio manual de un análisis de inventario de hardware ... 1368
Búsqueda en el inventario de hardware ... 1369
Visualización del hardware de un solo dispositivo ... 1371
Gestión de software ... 1374
Gestión del inventario de software ... 1374
Habilitar o deshabilitar el análisis del inventario de software ... 1374
Inicio manual de un análisis de inventario de software ... 1375
Búsqueda en el inventario de software ... 1376
Visualización del inventario de software de un solo dispositivo ... 1378
Acceso a vulnerabilidades y gestión de parches ... 1379
Evaluación de vulnerabilidades ... 1379
Gestión de parches ... 1390
Trabajar con repositorios de software y paquetes de software ... 1410
Paquetes de software ... 1410
Repositorios de software ... 1410
Versiones de Windows compatibles ... 1411
Búsqueda en los repositorios de software ... 1412

© Acronis International GmbH, 2003-2025

Cómo agregar paquetes de software desde la biblioteca ... 1414
Cargando paquetes de software ... 1415
Edición de paquetes de software ... 1419
Eliminación de paquetes de software ... 1419
Instalación de software ... 1420
Desinstalación de software ... 1423
Planes de implementación de software ... 1427
Crear un plan de despliegue de software ... 1427
Adición de un recurso informático a un plan de despliegue de software ... 1436
Cómo quitar recursos informáticos de los planes de despliegue de software ... 1437
Acciones adicionales con planes de despliegue de software ... 1437
Conexión a cargas de trabajo para asistencia o escritorio remotos ... 1441
Funciones de asistencia y escritorio remotos ... 1442
Sistemas operativos compatibles con escritorio remoto y asistencia ... 1445
Protocolos de conexión remota ... 1446
NEAR ... 1446
RDP ... 1447
Uso compartido de pantalla de Apple ... 1447
Redireccionamiento de sonido remoto ... 1447
Conexiones a cargas de trabajo remotas para asistencia o escritorio remotos ... 1448
Planes de administración remota ... 1450
Creación de un plan de administración remota ... 1450
Adición de una carga de trabajo a un plan de administración remota ... 1460
Eliminación de cargas de trabajo de un plan de administración remota ... 1460
Acciones adicionales con planes de administración remota ... 1461
Credenciales de la carga de trabajo ... 1464
Agregar credenciales ... 1464
Asignación de credenciales a una carga de trabajo ... 1465
Eliminar credenciales ... 1466
Anular la asignación de credenciales de una carga de trabajo ... 1466
Trabajar con cargas de trabajo gestionadas ... 1466
Ajuste de la configuración de RDP ... 1467
Conexión a cargas de trabajo administradas para asistencia o escritorio remotos ... 1468
Conectar a una carga de trabajo gestionada a través del cliente web ... 1471
Transferir archivos ... 1472
Compartir contenido del portapapeles entre cargas de trabajo ... 1473
Llevar a cabo acciones de control en cargas de trabajo gestionadas ... 1475

© Acronis International GmbH, 2003-2025

Conexión a línea de comandos remota ... 1478
Supervisión de cargas de trabajo mediante la transmisión de captura de pantalla ... 1481
Observar varias cargas de trabajo gestionadas de manera simultánea ... 1483
Trabajar con cargas de trabajo sin gestionar ... 1485
Conectar a cargas de trabajo no administradas a través de Acronis Asistencia rápida ... 1485
Conectar a cargas de trabajo gestionadas mediante una dirección IP ... 1486
Transferir archivos mediante Acronis Asistencia rápida ... 1487
Uso de la barra de herramientas en la ventana del Visor ... 1488
Grabar y reproducir sesiones remotas ... 1491
Configuración de los ajustes de Cliente de Connect ... 1492
Los notificadores del escritorio remoto ... 1493
Seguimiento de geolocalización ... 1495
Método de seguimiento de geolocalización compatible por sistema operativo ... 1495
Habilitación de los servicios de ubicación en el sistema operativo ... 1496
Visualización de la ubicación de un dispositivo ... 1496
Chat de asistencia ... 1498
Iniciar un chat con un usuario remoto ... 1499
Asignar sesiones de chat a uno mismo ... 1500
Reasignar sesiones de chat ... 1501
Exportar chats ... 1501
Filtrar sesiones de chat ... 1502
Buscar mensajes en sesiones de chat ... 1502
Acciones adicionales con las sesiones de chat ... 1503
Acciones adicionales con los mensajes de chat ... 1505
Supervisión del estado y el rendimiento de las cargas de trabajo ... 1507
Planes de supervisión ... 1507
Tipos de supervisión ... 1507
Supervisión basada en anomalías ... 1508
Plataformas compatibles con la supervisión ... 1508
Monitores configurables ... 1508
Configuración del monitor de espacio en disco ... 1516
Configuración de la supervisión de temperatura de la CPU ... 1518
Configuración de la supervisión de temperatura de la GPU ... 1520
Configuración del monitor de cambios de hardware ... 1521
Configuración de la supervisión del uso de la CPU ... 1522
Configuración de la supervisión del uso de la memoria ... 1524
Configuración de la supervisión de la velocidad de transferencia del disco ... 1526

© Acronis International GmbH, 2003-2025

Configuración del monitor de uso de red ... 1529
Configuración del uso de la CPU por supervisión del proceso ... 1531
Configuración del uso de la memoria por supervisión del proceso ... 1532
Configuración de la supervisión de la velocidad de transferencia del disco por proceso ... 1533
Configuración del uso de la red por supervisión del proceso ... 1534
Configuración de la supervisión del estado del servicio de Windows ... 1536
Configuración del monitor de estado del proceso ... 1536
Configuración del monitor de Software instalado ... 1537
Configuración de la supervisión del último reinicio del sistema ... 1538
Configuración de la supervisión del registro de eventos de Windows ... 1538
Configuración de la supervisión del tamaño de archivos y carpetas ... 1539
Configuración de la supervisión del estado de actualización de Windows ... 1540
Configuración de la supervisión del estado del cortafuegos ... 1541
Configuración del monitor de inicios de sesión fallidos ... 1541
Configuración de la supervisión del estado del software antimalware ... 1541
Configuración de la supervisión del estado de la función AutoRun ... 1543
Configuración del monitor personalizado ... 1543
Planes de supervisión ... 1545
Crear un plan de supervisión ... 1545
Añadir cargas de trabajo a los planes de supervisión ... 1547
Revocación de planes de supervisión ... 1548
Configuración de las acciones de respuesta automática ... 1548
Acciones adicionales con planes de supervisión ... 1551
Restablecimiento de los modelos de aprendizaje automático ... 1555
Supervisión de alertas ... 1555
Configuración de alertas de supervisión ... 1555
Variables de alertas de supervisión ... 1556
Medidas de respuesta manuales ... 1559
Consultar las alertas de supervisión para una carga de trabajo ... 1562
Visualización del registro de alertas de supervisión ... 1563
Configurar directivas de notificaciones por correo electrónico ... 1563
Ver datos de supervisión ... 1564
Widgets de supervisión ... 1565
Herramientas de Cyber Protection adicionales ... 1568
Modo de cumplimiento ... 1568
Limitaciones ... 1568
Características no compatibles ... 1568

© Acronis International GmbH, 2003-2025

Definición de la contraseña de cifrado ... 1569
Cambio de contraseña de cifrado ... 1569
Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento ... 1570
Almacenamiento inmutable ... 1570
Modos de almacenamiento inmutables ... 1571
Almacenamientos y agentes admitidos ... 1571
Habilitación del almacenamiento inmutable ... 1571
Inhabilitación del almacenamiento inmutable ... 1572
Acceder a copias de seguridad eliminadas en el almacenamiento inmutable ... 1573
Visualización del uso del almacenamiento inmutable ... 1574
Almacenamiento redundante geográficamente ... 1574
Limitaciones ... 1574
Habilitar el almacenamiento con redundancia geográfica ... 1575
Deshabilitar el almacenamiento con redundancia geográfica ... 1576
Visualización del estado de georreplicación ... 1576
Panel de control de concienciación ... 1577
Funcionamiento del servicio de Formación en concienciación sobre seguridad ... 1577
OpenVPN de sitio a sitio: información adicional ... 1578
Glosario ... 1587
Índice ... 1592

© Acronis International GmbH, 2003-2025

Cómo empezar a usar Cyber Protection

Activación de la cuenta

Cuando el administrador le cree una cuenta, se le enviará un mensaje a su dirección de correo electrónico. El mensaje contiene la siguiente información:

- **Sus credenciales de inicio de sesión.** Este es el nombre de usuario que utiliza para iniciar sesión. Sus credenciales de inicio de sesión aparecen también en la página de activación de la cuenta.
- Botón **Activar cuenta**. Haga clic en el botón y establezca la contraseña de su cuenta. Asegúrese de que la contraseña tenga al menos nueve caracteres. Para obtener más información sobre la contraseña, consulte "Requisitos de contraseña" (p. 22).

Si el administrador ha activado la autenticación de doble factor, se le solicitará que la configure para su cuenta. Para obtener más información sobre este tema, consulte "Autenticación de doble factor" (p. 22).

Requisitos de contraseña

La complejidad de las contraseñas se comprueba durante el registro del usuario y se clasifican en una de las siguientes categorías:

- Débil
- Medio
- Fuerte

No puede guardar una contraseña débil, incluso aunque sea lo suficientemente larga. Las contraseñas que repiten el nombre de usuario, el inicio de sesión, el correo electrónico del usuario o el nombre del inquilino al que pertenece la cuenta de usuario siempre se consideran débiles. Las contraseñas más comunes también se consideran débiles.

Nota
Los requisitos de contraseña están sujetos a cambios.

Para reforzar una contraseña, añada más caracteres. No es obligatorio utilizar diferentes tipos de caracteres, como números, mayúsculas y minúsculas y caracteres especiales, pero se obtienen contraseñas más fuertes y más cortas.

Autenticación de doble factor

La autenticación de doble factor (2FA) proporciona protección adicional contra el acceso no autorizado a su cuenta. Cuando se establezca la autenticación de doble factor (2FA), tendrá que introducir su contraseña (el primer factor) y un código de un solo uso (el segundo factor) para iniciar sesión en la consola de Cyber Protect. Una aplicación especial, que deberá instalar en su teléfono

© Acronis International GmbH, 2003-2025

móvil u otro dispositivo que le pertenezca, genera el código de un solo uso. Incluso si alguien descubre su inicio de sesión y contraseña, no podrá iniciar sesión en su cuenta sin tener que acceder a su dispositivo de segundo factor.

Configuración de la autenticación de doble factor para su cuenta

Debe establecer la autenticación de doble factor (2FA) para su cuenta si el administrador la ha habilitado para su organización. Si el administrador habilita la autenticación de doble factor (2FA) mientras tiene la sesión iniciada en la consola de Cyber Protect, tendrá que configurarla cuando caduque esa sesión.

Requisitos previos

- Un administrador de su organización ha habilitado la autenticación de doble factor.

Configuración de la autenticación de doble factor para su cuenta

1. Escoja un dispositivo de segundo factor.
   Normalmente es un teléfono móvil, pero puede ser una tablet, un portátil o un equipo de escritorio.
2. Instale una app de autenticación en su dispositivo de segundo factor.
   Ejemplos de apps compatibles:
   - Microsoft Authenticator
   - Google Authenticator
   - Twilio Authy
3. Escanee el código QR con la app de autenticación e introduzca el código de 6 dígitos que aparece en su app de autenticación en la ventana **Configurar la autenticación de doble factor**.
4. Haga clic en **Siguiente**.
   Se mostrarán las indicaciones sobre cómo restaurar el acceso a su cuenta si pierde su dispositivo con autenticación de doble factor (2FA) o desinstala la app de autenticación.
5. Guarde o imprima el archivo PDF.

   Nota
   Asegúrese de guardar el archivo PDF en un lugar seguro o imprimirlo para futuras consultas. Es la mejor manera de restaurar el acceso.

6. Vuelva a la página de inicio de sesión de la consola de Cyber Protect e introduzca el código generado.
   Un código de un solo uso tiene una validez de 30 segundos. Si espera más de 30 segundos, use el siguiente código generado.

Nota
Si su app de autenticación admite copias de seguridad, le recomendamos que realice una copia de seguridad de su configuración en la nube.

© Acronis International GmbH, 2003-2025

La próxima vez que inicie sesión, puede seleccionar la casilla de verificación **Confiar en este navegador...**. En este caso, el código no será necesario para iniciar sesión más veces con este navegador en este equipo.

Nota
Le recomendamos que deje esta casilla de verificación sin marcar. De lo contrario, perderá el acceso a la configuración de la autenticación de doble factor (2FA) de su cuenta.

Pasos para configurar la autenticación de doble factor (2FA) en un nuevo dispositivo

Este procedimiento es aplicable si tiene acceso a la app de autenticación configurada anteriormente.

1. Instale un app de autenticación en su nuevo dispositivo.
2. Utilice el archivo PDF que ha guardado al configurar la autenticación de doble factor (2FA) en el dispositivo.
   El archivo contiene el código de 32 dígitos que debe introducir en la app de autenticación para enlazar de nuevo la app de autenticación con su cuenta de Acronis.

   Importante
   Si el código no funciona, asegúrese de que la hora en la app de autenticación para entorno móvil está sincronizada con su dispositivo.

Si no ha guardado el archivo PDF durante la instalación:

1. Haga clic en **Restablecer autenticación de doble factor (2FA)** e introduzca la contraseña de un solo uso mostrada en la app de autenticación para entorno móvil.
2. Siga las instrucciones que aparecen en pantalla.

Pasos para restaurar el acceso a su cuenta cuando la 2FA esté habilitada

Estas opciones son aplicables cuando no tiene acceso a la app de autenticación configurada anteriormente. Por ejemplo, ha perdido el dispositivo, se lo han robado o ha quedado destrozado.

- Para volver a configurar la app de autenticación TOTP, utilice el código 2FA que se proporcionó cuando configuró la 2FA inicialmente. El nombre predeterminado del archivo es `cyberprotect-2fa-backupcode.pdf`.
- Si tiene una copia de seguridad en la app de autenticación, restaure la configuración de la 2FA desde la copia de seguridad.
- Para restablecer la configuración de la 2FA, póngase en contacto con el administrador de la cuenta que tiene acceso al portal de administración en la nube.
- Solicite a su proveedor de servicios que restablezca su configuración de autenticación de doble factor (2FA).
- Póngase en contacto con el equipo de soporte del proveedor para obtener ayuda.

© Acronis International GmbH, 2003-2025

Configuración de privacidad

La configuración de privacidad le ayuda a indicar si da o no su consentimiento para la recopilación, uso y divulgación de su información personal.

En función del país en el que utilice Cyber Protect Cloud y del centro de datos de Cyber Protect Cloud que le preste servicios, es posible que, al iniciar Cyber Protect Cloud por primera vez, se le pida que confirme si acepta el uso de Google Analytics en Cyber Protect Cloud.

Google Analytics nos ayuda a comprender mejor el comportamiento de los usuarios y a mejorar su experiencia en Cyber Protect Cloud mediante la recopilación de datos anónimos.

Si ha habilitado o rechazado la habilitación de Google Analytics en el lanzamiento inicial de Cyber Protect Cloud, puede cambiar su decisión en cualquier momento.

Pasos para habilitar o deshabilitar Google Analytics

1. En la consola de Cyber Protect, haga clic en **Gestionar cuentas**.
2. Haga clic en el icono de la cuenta en la esquina superior derecha.
3. Seleccione **Mi configuración de privacidad**. Se mostrará la ventana **Mi configuración de privacidad**.
4. En la sección **Recopilación de datos de Google Analytics**, haga clic en uno de los siguientes botones:
   - **Encendido** para habilitar Google Analytics
   - **Apagado** para deshabilitar Google Analytics

En la sección **Cómo eliminar cookies** puede controlar y gestionar cookies directamente desde su navegador.

Nota
Si no ve la sección Google Analytics, significa que Google Analytics no se utiliza en su país.

En la sección **Incorporación del producto y ayuda interactiva** que se muestra al inicio durante el período de prueba, puede detener o mantener la recepción de información sobre las mejoras y las nuevas funciones del programa en el futuro. Esta función está habilitada de forma predeterminada, pero .puede deshabilitarla si cambia el conmutador a **Apagado**.

Acceso a los servicios de Cyber Protection

Cuando active su cuenta, podrá acceder al servicio de Cyber Protection si inicia sesión en la consola de Cyber Protect o a través del portal de administración.

Pasos para iniciar sesión en la consola de Cyber Protect

1. Vaya a la página de inicio de sesión del servicio Cyber Protection.
2. Escriba su usuario y haga clic en **Siguiente**.

© Acronis International GmbH, 2003-2025

3. Escriba su contraseña y haga clic en **Siguiente**.
4. [Si utiliza más de un servicio de Cyber Protect Cloud] Haga clic en **Cyber Protection**.
   Los usuarios que solo tienen acceso al servicio de Cyber Protection inician sesión en la consola de Cyber Protect directamente.
   Si **Cyber Protection** no es el único servicio al que tiene acceso, puede cambiar de un servicio a otro con el icono  de la esquina superior derecha. Los administradores también pueden usar este icono para cambiar al portal de gestión.

El tiempo de espera para la consola de Cyber Protect es de 24 horas en las sesiones activas y de 1 hora en las inactivas.

Puede cambiar el idioma de la interfaz web si hace clic en el icono de la cuenta que hay en la esquina superior derecha.

Pasos para acceder a la consola de Cyber Protect desde el portal de administración

1. En el portal de administración, vaya a **Supervisión** > **Uso**.
2. En **Cyber Protect**, seleccione **Protección** y haga clic en **Gestionar servicio**.
   De manera alternativa, en **Clientes**, seleccione un cliente y haga clic en **Gestionar servicio**.

Como resultado, se le dirigirá a la consola de Cyber Protect.

Importante
Si el cliente está en el modo de administración **Autoservicio**, no puede gestionar servicios en su nombre. Solo los administradores de clientes pueden cambiar el modo del cliente a **Gestionado por el proveedor de servicios** y luego gestionar los servicios.

Pasos para restablecer su contraseña

1. Vaya a la página de inicio de sesión del servicio Cyber Protection.
2. Escriba su usuario y haga clic en **Siguiente**.
3. Haga clic en **¿Olvidó su contraseña?**.
4. Haga clic en **Enviar** para confirmar que quiere obtener más instrucciones.
5. Siga las instrucciones del correo electrónico que ha recibido.
6. Establezca su nueva contraseña.

Navegadores web compatibles

La consola de Cyber Protect utiliza el protocolo TLS 1.2 y es compatible con los siguientes navegadores web:

- Google Chrome 109 o posterior
- Mozilla Firefox 115 o posterior
- Opera 95 o posterior (Chromium 109)

© Acronis International GmbH, 2003-2025

- Microsoft Edge 109 o posterior
- Apple Safari (para Mac OS X) 16 o posterior, ejecutándose en los sistemas operativos macOS e iOS

En otros navegadores web (incluido Safari para otros sistemas operativos), es posible que la interfaz de usuario no se muestre correctamente o que algunas funciones no estén disponibles.

No se admite el uso de navegadores móviles.

Mi bandeja de entrada

La página Mi bandeja de entrada está diseñada para agilizar su comunicación dentro de la aplicación. Con esta guía, puede gestionar sus mensajes de forma eficaz, mantenerse organizado y mejorar su productividad. La bandeja de entrada del producto es su centro de operaciones en el que recibir y gestionar comunicaciones dentro de la aplicación. Le permite mantenerse informado sobre actualizaciones importantes, mensajes y alertas dentro de su flujo de trabajo.

Información general

La pestaña **Mi bandeja de entrada** cuenta con una función de contador de notificaciones que muestra la cantidad de notificaciones sin leer. Al hacer clic en este contador, se muestran las notificaciones sin leer, lo que facilita el seguimiento de los elementos pendientes. Además, las funciones de contadores junto a cada filtro (categoría, importancia, acción) muestran la cantidad de notificaciones disponibles en ese filtro específico, lo que le ayuda a comprender cuántas notificaciones entran en cada categoría.

En su bandeja de entrada, recibirá varias notificaciones, cada una diseñada para fines específicos según su configuración de cuenta y contexto: anuncios de funciones, nuevos cursos de formación disponibles, invitaciones a eventos y seminarios web, recordatorios de vencimiento de certificados, promociones, avisos de mantenimiento, encuestas y otros.

Comprobación de sus notificaciones

Comprobación de la sección de notificaciones

1. Inicie la sesión en la consola de Cyber Protect Cloud.
2. En el panel de navegación, seleccione el elemento de menú **Mi bandeja de entrada**.

Búsqueda en Mi bandeja de entrada

Pasos para buscar mensajes no leídos

1. Haga clic en el elemento de menú **Mi bandeja de entrada**.
2. En la esquina superior derecha, cambie el interruptor **Mostrar solo no leídos**.

Pasos para buscar información importante en su bandeja de entrada

© Acronis International GmbH, 2003-2025

1. Acceda a **Mi bandeja de entrada** desde el panel de control de Cyber Protect Cloud.
2. En la vista de la bandeja de entrada, busque la barra de **búsqueda** en la parte superior.
3. Introduzca palabras clave o nombres de remitentes relevantes para filtrar los mensajes.
4. Pulse **Intro** para ver los resultados de la búsqueda.

Los resultados mostrarán todas las notificaciones que coincidan con los criterios de búsqueda.

Funciones de protección compatibles con el sistema operativo

Este tema contiene información acerca de las funciones de protección de Cyber Protect Cloud. Para ver la lista de sistemas operativos y entornos compatibles con la copia de seguridad y recuperación, consulte "Sistemas operativos y entornos compatibles para la copia de seguridad y la recuperación" (p. 499).

Las funciones de protección solo están disponibles en equipos en los que está instalado un agente de protección. No están disponibles para máquinas virtuales con copias de seguridad en el modo sin agente, por ejemplo, por Agente para Hyper-V, Agente para VMware, Agente para la Virtuozzo Hybrid Infrastructure, Agente para Scale Computing o Agente para oVirt.

Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Sistemas operativos y versiones compatibles

Windows

A menos que se indique lo contrario para un conjunto de funciones específico, las siguientes versiones de Windows son compatibles:

- Windows 7 Service Pack 1 y posteriores
- Windows Server 2008 R2 Service Pack 1 y posteriores

Nota
En Windows 7, debe instalar las siguientes actualizaciones de Microsoft antes de instalar el agente de protección:

- Actualizaciones de seguridad ampliadas de Windows 7 (ESU)
- KB4474419
- KB4490628

Consulte este artículo de la base de conocimientos para obtener más información sobre las actualizaciones requeridas.

Linux

© Acronis International GmbH, 2003-2025

Las distribuciones de Linux compatibles y sus versiones dependen de los conjuntos de funciones y se muestran al final de cada tabla.

macOS

Las versiones de macOS compatibles dependen de los conjuntos de funciones y se muestran al final de cada tabla.

Característica	Windows	Linux	macOS
Planes de protección predeterminados			
Trabajadores en remoto	Sí	No	No
Trabajadores en la oficina (antivirus de terceros)	Sí	No	No
Trabajadores en la oficina (antivirus Cyber Protect)	Sí	No	No
Cyber Protect Essentials (solo para la edición Cyber Protect Essentials)	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Copia de seguridad forense			
Recopilación de un volcado de memoria sin procesar	Sí	No	No
Instantánea de los procesos en ejecución	Sí	No	No
Certificación de copia de seguridad forense de imágenes locales	Sí	No	No
Certificación de copia de seguridad forense de imágenes en la nube	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Protección continua de datos (CDP)			
CDP para archivos y carpetas	Sí	No	No
CDP para archivos cambiados mediante el seguimiento de aplicaciones	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Autodetección e instalación remota			
Detección basada en la red	Sí	No	No
Detección basada en Active Directory*	Sí	No	No
Detección con base en la plantilla (importación de equipos desde un archivo)	Sí	No	No
Inclusión manual de dispositivos	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

* La detección basada en Active Directory no funciona como se espera con la configuración predeterminada de Windows Server 2025 porque aplica el cifrado LDAP de forma predeterminada. Consulte este artículo de la base de conocimientos.

Active Protection

Característica	Windows	Linux	macOS
Detección inserciones de procesos	Sí	No	No
Recuperación automática de archivos afectados de la caché local	Sí	Sí	Sí
Autodefensa de las copias de seguridad de Acronis	Sí	No	No
Autodefensa de las copias de seguridad del software Acronis	Sí	No	Sí (Solo Active Protection y componentes antimalware)
Gestión de procesos de confianza/bloqueados	Sí	No	Sí
Exclusiones de procesos/carpetas	Sí	Sí	Sí
Detección de ransomware basada en el comportamiento de un proceso (basada en IA)	Sí	Sí	Sí
Detección del proceso de criptominería basada en el comportamiento de procesos	Sí	No	No
Protección de unidades externas (discos duros, unidades flash y tarjetas SD)	Sí	No	Sí

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Protección de carpetas de red	Sí	No*	Sí
Protección del servidor	Sí	No	No
Protección de Zoom, Cisco Webex, Citrix Workspace y Microsoft Teams	Sí	No	No

*Las carpetas de red en Linux se tratan como carpetas locales, por lo que Active Protection protegerá automáticamente las carpetas de red en el sistema operativo Linux, como si fueran carpetas locales.

Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Protección contra malware y antivirus

Característica	Windows	Linux	macOS
Funcionalidad Active Protection integrada por completo	Sí	No	No
Protección contra malware en tiempo real	Sí	Sí	Sí
Protección contra malware en tiempo real avanzada con detección basada en firmas locales	Sí	Sí	Sí
Análisis estadístico para archivos ejecutables portátiles	Sí	No	Sí1
Análisis antimalware bajo demanda	Sí	Sí2	Sí
Protección de carpetas de red	Sí	No3	No
Protección del servidor	Sí	No	No
Análisis de archivos del archivo comprimido	Sí	No	Sí
Análisis de unidades extraíbles	Sí	No	Sí
Análisis únicamente de archivos nuevos y cambiados	Sí	No	Sí
Exclusiones de archivos/carpetas	Sí	Sí	Sí4
Exclusiones de procesos	Sí	No	Sí
Motor de análisis de comportamiento	Sí	Sí5	Sí
Prevención de vulnerabilidades	Sí	No	No
Cuarentena	Sí	Sí	Sí

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Limpieza automática en cuarentena	Sí	Sí	Sí
Filtrado de URL (http/https)	Sí	No	No
Lista blanca corporativa	Sí	No	Sí
Gestión del firewall6	Sí	No	No
Gestión del antivirus Microsoft Defender 7	Sí	No	No
Gestión de Microsoft Security Essentials	Sí	No	No
Registro y gestión de la protección antivirus y antimalware mediante Windows Security Center	Sí	No	No

1 El análisis estático de archivos ejecutables portátiles solo se admite para análisis programados en macOS.

2 En Linux, las condiciones para un análisis bajo demanda no están admitidas.

3 Las carpetas de red en Linux se tratan como carpetas locales, por lo que Active Protection protegerá automáticamente las carpetas de red en el sistema operativo Linux, como si fueran carpetas locales.

4 Las exclusiones de archivos/carpetas solo se admiten cuando se especifican archivos y carpetas que no se analizarán mediante la protección en tiempo real ni los análisis programados en macOS.

5 El motor de análisis de comportamiento es compatible con las siguientes versiones de Linux:
- CentOS 7.x
- Debian 10.x, 11.x
- CloudLinux 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.04 y 22.04

6 La gestión del cortafuegos es compatible con Windows 8 y versiones posteriores. Windows Server no es compatible.

7 La administración de Microsoft Defender Antivirus es compatible con Windows 8.1 y versiones posteriores.

Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Característica	Windows	Linux	macOS
Evaluación de vulnerabilidades			
Evaluación de vulnerabilidades del sistema operativo y sus aplicaciones nativas	Sí	Sí*	Sí
Evaluación de vulnerabilidades para aplicaciones de terceros	Sí	No	Sí

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Evaluación de vulnerabilidades			
Para obtener más información sobre los sistemas operativos admitidos y sus versiones, consulte "Productos de Microsoft y de terceros compatibles con la evaluación de vulnerabilidades" (p. 1380), "Productos de Linux compatibles para la evaluación de vulnerabilidades" (p. 1382) y "Productos de Apple y de terceros compatibles con la evaluación de vulnerabilidades" (p. 1381).			

* La evaluación de vulnerabilidades depende de la disponibilidad de asesores de seguridad oficiales para distribuciones específicas, como https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce, etc.

Característica	Windows	Linux	macOS
Gestión de parches			
Aprobación automática de parches	Sí	No	No
Instalación automática de parches	Sí	No	No
Prueba de parches	Sí	No	No
Instalación manual de parches	Sí	No	No
Programación de parches	Sí	No	No
Instalación de parches a prueba de fallos: realización de una copia de seguridad del equipo antes de instalar los parches como parte del plan de protección	Sí	No	No
Cancelación del reinicio de un equipo si se está ejecutando una copia de seguridad	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Mapa de protección de datos			
Definición regulable de archivos importantes	Sí	No	No
Análisis de equipos para encontrar archivos no protegidos	Sí	No	No
Información general de ubicaciones no protegidas	Sí	No	No
Capacidad de iniciar la acción de protección desde el widget del mapa de protección de datos (acción **Proteger todos los archivos**)	Sí	No	No

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Mapa de protección de datos			
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Estado del disco			
Control del estado del disco duro y SSD basado en IA	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Planes de protección inteligente basados en alertas del centro de operaciones de ciberprotección (CPOC) de Acronis			
Fuente de amenazas	Sí	No	No
Asistente de soluciones	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Análisis de copia de seguridad			
Análisis antimalware de copias de seguridad de imágenes como parte del plan de copias de seguridad	Sí	No	No
Análisis de copias de seguridad de imágenes para detectar si hay malware en la nube	Sí	No	No
Análisis de malware de copias de seguridad cifradas	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Recuperación segura			
Análisis antimalware con protección antivirus y antimalware durante el proceso de recuperación	Sí	No	No
Recuperación segura para copias de seguridad cifradas	Sí	No	No

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Recuperación segura			
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Conexión a escritorio remoto			
Conexión a través de NEAR	Sí	Sí	Sí
Conexión a través de RDP	Sí	No	No
Conexión a través del uso compartido de pantalla de Apple	No	No	Sí
Conexión a través del cliente web	Sí	No	No
Conexión a través de Asistencia rápida	Sí	Sí	Sí
Asistencia remota	Sí	Sí	Sí
Transferencia de archivos	Sí	Sí	Sí
Transmisión de captura de pantalla	Sí	Sí	Sí
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles con escritorio remoto y asistencia" (p. 1445).			

Característica	Windows	Linux	macOS
#CyberFit Score			
Estado de #CyberFit Score	Sí	No	No
Herramienta independiente de #CyberFit Score	Sí	No	No
Recomendaciones de #CyberFit Score	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Prevención de pérdida de datos			
Control de dispositivos	Sí	No	Compatible con equipos Mac con procesadores

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Prevención de pérdida de datos			
			Intel que ejecuten macOS 10.15 o posterior o macOS 11.2.3 o posterior. No es compatible con los procesadores de Apple Silicon basados en ARM, como Apple M1 o M2.
Advanced Data Loss Prevention	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)).			

Característica	Windows	Linux	macOS
Opciones de gestión			
Situaciones de venta de productos de gama superior para promocionar ediciones de Cyber Protect	Sí	Sí	Sí
Consola de gestión web centralizada y remota	Sí	Sí	Sí
Sistemas operativos y versiones compatibles: Independencia de la plataforma.			

Característica	Windows	Linux	macOS
Opciones de protección			
Borrado remoto	Sí	No	No
Se admite en Windows 10 y versiones posteriores.			

Característica	Windows	Linux	macOS
Cyber Protect Monitor			
App de Cyber Protect	Sí	No	Sí
Estado de la protección de Zoom	Sí	No	No

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Cyber Protect Monitor			
Estado de la protección de Cisco Webex	Sí	No	No
Estado de la protección de Citrix Workspace	Sí	No	No
Estado de la protección de Microsoft Teams	Sí	No	No
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)). En macOS, Cyber Protect Monitor es compatible con todas las versiones en las que pueda instalar Agente para Mac, excepto macOS 10.x. Para obtener más información, consulte "Agente para Mac" (p. 506).			

Característica	Windows	Linux	macOS
Inventario de software			
Análisis de inventario de software	Sí	No	Sí
Supervisión de inventario de software	Sí	No	Sí
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)). En macOS, el inventario del Software es compatible con las versiones 10.13.x − 13.x.			

Característica	Windows	Linux	macOS
Inventario de hardware			
Análisis del inventario de hardware	Sí	No	Sí
Supervisión de inventario de hardware	Sí	No	Sí
Consulte las versiones de Windows compatibles al principio de esta sección ("Sistemas operativos y versiones compatibles" (p. 28)). En macOS, el inventario del Hardware es compatible con las versiones 10.13.x − 13.x.			

© Acronis International GmbH, 2003-2025

Instalación e implementación de los agentes de Cyber Protection

Antes de empezar

Preparación

Paso 1

Elija un agente teniendo en cuenta los elementos que va a incluir en la copia de seguridad. Para obtener más información sobre las posibles opciones, consulte ¿Qué Agente necesito?

Paso 2

Asegúrese de que hay suficiente espacio libre en el disco duro para instalar un agente. Para obtener información detallada sobre el espacio requerido, consulte "Requisitos del sistema para agentes" (p. 47).

Paso 3

Descargar el programa de instalación. Para buscar los enlaces de descarga, haga clic en **Todos los dispositivos** > **Agregar**.

La página **Añadir dispositivos** proporciona instaladores web para cada uno de los agentes instalados en Windows. Un instalador web es un pequeño archivo ejecutable que descarga el programa principal de instalación de Internet y lo guarda como un archivo temporal. Este archivo se elimina inmediatamente después de que se haya instalado.

Si desea almacenar los programas de instalación localmente, descargue un paquete que contenga todos los agentes para la instalación en Windows por medio del enlace que hay en la parte inferior de la página **Añadir dispositivos**. Están disponibles los paquetes de 32 bits y 64 bits. Con estos paquetes se puede personalizar la lista de componentes que se instalarán. Estos paquetes también permiten la instalación sin interacción, por ejemplo, a través de la directiva de grupo. Se detalla este escenario avanzado en "Despliegue de agentes de protección a través de la directiva de grupo" (p. 134).

Para descargar el programa de instalación del agente para Microsoft 365, haga clic en el icono de la cuenta que hay en la esquina superior derecha y, a continuación, seleccione **Descargas** > **Agente para Microsoft 365**.

La instalación en Linux y macOS se realiza desde los programas de instalación habituales.

Todos los programas de instalación precisan conexión a Internet para registrar el equipo en el servicio Cyber Protection. Si no hay conexión a Internet, la instalación fallará.

© Acronis International GmbH, 2003-2025

Paso 4

Las funciones de Cyber Protect requieren Microsoft Visual C++ 2017 Redistributable. Asegúrese de que esté instalado en su equipo o hágalo antes de instalar el agente. Es posible que tenga que reiniciar el equipo después de instalar Microsoft Visual C++. Puede encontrar el paquete de Microsoft Visual C++ Redistributable aquí https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Paso 5

Asegúrese de que los cortafuegos y otros componentes del sistema de seguridad de red (como, por ejemplo, un servidor proxy) permiten conexiones de salida mediante los siguientes puertos TCP.

- Puertos **443** y **8443**

  Se usan estos puertos para acceder a la consola de Cyber Protect, registrar los agentes, descargar los certificados, obtener la autorización del usuario y descargar archivos desde el almacenamiento en la nube.
- Puertos en el rango de **7770** – **7800**

  Los agentes usan estos puertos para comunicarse con el servidor de gestión.
- Puerto **44445**

  Los agentes usan este puerto para transferir datos durante la realización de copias de seguridad y las recuperaciones.

Si hay un servidor proxy habilitado en la red, consulte "Ajuste de la configuración del servidor proxy" (p. 53) para saber si debe configurar estos ajustes en cada equipo que ejecute un agente de protección.

La velocidad de conexión a Internet mínima necesaria para gestionar un agente desde el cloud es de 1 Mbit/s (no se debe confundir con la velocidad de transferencia de datos aceptable para llevar a cabo copias de seguridad en la nube). Tenga en cuenta este aspecto si usa una tecnología de conexión de ancho de banda bajo, como el ADSL.

Se necesitan puertos TCP para realizar copias de seguridad y replicaciones de equipos virtuales VMware.

- Puerto **443**

  El agente para VMware (en Windows y dispositivo virtual) se conecta a este puerto del servidor ESXi o vCenter para llevar a cabo operaciones de gestión de máquinas virtuales, como crear, actualizar y eliminar máquinas virtuales en vSphere durante operaciones de copia de seguridad, recuperación y replicación de máquinas virtuales.
- Puerto **902**

  El agente para VMware (en Windows y dispositivo virtual) se conecta a este puerto del servidor ESXi para establecer conexiones NFC con el fin de poder leer o escribir datos en discos de

© Acronis International GmbH, 2003-2025

máquinas virtuales durante operaciones de copia de seguridad, recuperación y replicación de máquinas virtuales.

- Puerto **2029**

  El agente para VMware (dispositivo virtual) escucha en este puerto las solicitudes entrantes al servidor NFS, que se aloja en el agente. Las conexiones a través de este puerto son necesarias para ejecutar una máquina virtual desde una copia de seguridad (restauración instantánea).
- Puerto **3333**

  Si el agente para VMware (dispositivo virtual) se está ejecutando en el clúster o servidor ESXi que vaya a ser el destino de la replicación de la máquina virtual, el tráfico de esta replicación no va directamente al servidor ESXi en el puerto **902**. En su lugar, el tráfico se dirige desde el agente para VMware de origen al puerto TCP **3333** en el agente para VMware (dispositivo virtual) que se encuentra en el clúster o servidor ESXi de destino.

  El agente para VMware de origen que lee los datos de los discos del equipo virtual originales puede estar en cualquier otro lugar y puede ser de cualquier tipo: Dispositivo virtual o Windows.

  El servicio que tiene que aceptar los datos de la replicación del equipo virtual en el agente para VMware (dispositivo virtual) de destino se denomina "Servidor del disco de replicación". Este servicio es el responsable de llevar a cabo técnicas de optimización WAN, como la compresión y la deduplicación del tráfico durante la replicación del equipo virtual, incluida la recopilación de réplicas (véase "Recopilación de una réplica inicial" (p. 960)).Cuando no se está ejecutando ningún agente para VMware (dispositivo virtual) en el servidor ESXi de destino, este servicio no está disponible y, por lo tanto, la recopilación de réplicas no se puede llevar a cabo.

Puertos necesarios para el componente de descarga

El componente de descarga se encarga de realizar las actualizaciones de un ordenador y distribuirlas a otras instancias de descarga. Puede ejecutarse en modo agente, lo que convierte su ordenador en un agente de descarga. El agente descarga las actualizaciones de Internet y actúa como origen de distribución de actualizaciones para otros ordenadores. El agente de descarga necesita los siguientes puertos para operar.

- Puerto TCP y UDP (entrante) **6888**

  Lo utiliza el protocolo BitTorrent para actualizaciones P2P de torrent.
- Puerto UDP **6771**

  Se utiliza como puerto de descubrimiento de sistemas del mismo nivel locales. También se utiliza en actualizaciones P2P.
- Puerto TCP **18018**

  Se utiliza para la comunicación entre actualizadores que trabajan en diferentes modos: Actualizador y Agente actualizador.
- Puerto TCP **18019**

  Puerto local, se utiliza para la comunicación entre el actualizador y el agente de protección.

© Acronis International GmbH, 2003-2025

Paso 6

En el equipo en el que quiera instalar el agente de protección, compruebe que otros procesos no utilicen los siguientes puertos locales.

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

Nota
No tiene que abrirlos en el cortafuegos.

Cambio de los puertos utilizados por el agente de protección

Es posible que otras aplicaciones de su entorno estén utilizando alguno de los puertos que el agente de protección requiere. Para evitar conflictos, puede cambiar los puertos predeterminados que utiliza el agente de protección al modificar los archivos siguientes.

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

Copia de seguridad basada en agente y sin agente

La copia de seguridad basada en agentes requiere que se instale un agente de protección en cada máquina protegida. Esta copia es compatible con todas las máquinas físicas y virtuales. Para obtener más información sobre qué agente necesita y dónde instalarlo, consulte "¿Qué Agente necesito?" (p. 42)

La copia de seguridad sin agente es compatible con algunas plataformas de virtualización y no está disponible para máquinas físicas. Solo requiere un agente de protección, que se instala en una máquina dedicada en el entorno virtual. Este agente realiza copias de seguridad de todas las demás máquinas virtuales en este entorno. Para obtener más información sobre los tipos de copia de seguridad compatibles por plataforma de virtualización, consulte "Plataformas de virtualización compatibles" (p. 511).

Para algunas plataformas de virtualización, hay disponibles dispositivos virtuales. Un dispositivo virtual es una máquina virtual disponible que incluye un agente de protección. Los dispositivos virtuales están disponibles en formatos específicos de hipervisor, como .ovf, .ova o .qcow.

¿Qué tipo de copia de seguridad necesito?

Recomendamos la copia de seguridad basada en agentes si necesita lo siguiente:

- Funciones de protección adicional, como antivirus y antimalware, administración de parches o conexión de escritorio remoto. Para obtener más información sobre estas funciones, consulte "Funciones de protección compatibles con el sistema operativo" (p. 28).

© Acronis International GmbH, 2003-2025

- Máquinas virtuales separadas a nivel de inquilino. Por ejemplo, porque quiere proporcionar a los usuarios del inquilino acceso solo a sus propias copias de seguridad.
- Copias de seguridad a nivel de archivo que puede recuperar en los sistemas operativos invitados.

Recomendamos la copia de seguridad sin agente si necesita lo siguiente:

- Solo copia de seguridad, sin ninguna función de protección adicional.
- Gestión simplificada: puede hacer copias de seguridad de varias máquinas virtuales mediante la instalación y configuración de un solo agente.
- Uso mínimo de recursos: un agente dedicado utiliza menos CPU y RAM que varios agentes instalados en cada máquina virtual de su entorno.
- Configuraciones de copia de seguridad específicas, como la copia de seguridad sin LAN. Para obtener más información sobre esta función, consulte "Agente para VMware: copia de seguridad sin LAN" (p. 961).
- Menos sobrecarga de configuración. El agente dedicado hace copias de seguridad de las máquinas virtuales a nivel de hipervisor, independientemente del sistema operativo de los invitados.

¿Qué Agente necesito?

Para seleccionar un agente, se debe tener en cuenta los elementos que se van a incluir en la copia de seguridad. En la siguiente tabla se resume la información para ayudarle a decidir.

En Windows, Agente para Exchange, Agente para SQL, Agente para Active Directory y Agent for Oracle requieren que también se instale el agente para Windows. Por lo tanto, si instala, por ejemplo, el Agente para SQL, también podrá realizar copias de seguridad de todo el equipo donde se haya instalado el agente.

Le recomendamos que instale el agente para Windows donde se vaya a instalar el Agente para VMware (Windows) y el agente para Hyper-V.

En Linux, el Agente para Oracle, Agente para MySQL/MariaDB, Agente para Virtuozzo y Agente para Proxmox requieren que también esté instalado el Agente para Linux (64 bits). Estos agentes se incluyen en el archivo de instalación del Agente para Linux (64 bits).

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?
Equipos físicos		
Equipos físicos que ejecutan Windows	Agente para Windows	En el equipo del que se hará la copia de seguridad.
Equipos físicos que ejecutan Linux	Agente para Linux	
Equipos físicos que ejecutan macOS	Agente para Mac	

© Acronis International GmbH, 2003-2025

Bases de datos		
Bases de datos SQL	Agente para SQL	En el equipo que ejecuta Microsoft SQL Server.
Bases de datos MySQL	Agente para MySQL/MariaDB (Incluido en el archivo de instalación del agente para Linux (64 bits))	En el equipo que ejecuta MySQL Server.
Bases de datos de MariaDB	Agente para MySQL/MariaDB (Incluido en el archivo de instalación del agente para Linux (64 bits))	En el equipo que ejecuta MariaDB Server.
Bases de datos de Exchange	Agente para Exchange	En el equipo que realiza el rol de buzón de correo de Microsoft Exchange Server.*
Bases de datos de Oracle	Agente para Oracle (En Linux, incluido en el archivo de instalación del Agente para Linux (64 bits))	En el equipo que ejecuta la Base de datos de Oracle.
Cargas de trabajo de la nube a la nube		
Buzones de correo de Microsoft 365 (Agente en la nube o agente local)	Agente en la nube (No requiere instalación)	Esta funcionalidad está disponible con agentes en la nube desplegados en el centro de datos. Para obtener más información, consulte "Comparación de soluciones de copia

© Acronis International GmbH, 2003-2025

		de seguridad para datos de Microsoft 365" (p. 833).
	Agente para Office 365	En un equipo Windows conectado a Internet. Para obtener más información, consulte "Agente instalado de forma local para Office 365" (p. 902).
Archivos de Microsoft 365 y OneDrive y sitios de SharePoint Online	Agente en la nube (No requiere instalación)	Esta funcionalidad está disponible con agentes en la nube desplegados en el centro de datos. Para obtener más información, consulte "Comparación de soluciones de copia de seguridad para datos de Microsoft 365" (p. 833).
Buzones de correo de Gmail de Google Workspace Gmail, archivos de Google Drive y unidades compartidas.	Agente en la nube (No requiere instalación)	Esta funcionalidad está disponible con agentes en la nube desplegados en el centro de datos. Para obtener más información, consulte "Protección de los datos de Google Workspace" (p. 907).
Active Directory		
Equipos que ejecutan Servicios de dominio de Active Directory	Agente para Active Directory	En el controlador de dominio.
Equipos virtuales		
Máquinas virtuales VMware ESXi (Broadcom)	Agente para VMware (Windows)	En un equipo Windows con acceso

© Acronis International GmbH, 2003-2025

		de red a vCenter Server y al almacenamiento del equipo virtual.**
	Agente para VMware (dispositivo virtual)	En el servidor ESXi.
Máquinas virtuales Microsoft Hyper-V	Agente para Hyper-V	En el servidor Hyper-V.
Máquinas virtuales Scale Computing HyperCore	Agente para Scale Computing HC3 (dispositivo virtual)	En el host Scale Computing HyperCore.
Máquinas virtuales Nutanix	Agente para Nutanix AHV (dispositivo virtual)	En el host de Nutanix AHV.
Máquinas virtuales Proxmox	Agente para Proxmox (Incluido en el archivo de instalación del agente para Linux (64 bits))	En el host de Proxmox VE.
Máquinas virtuales de Red Hat Virtualization (gestionadas por oVirt)	Agente para oVirt (dispositivo virtual)	En el servidor de Red Hat Virtualization.
Máquinas virtuales y contenedores Virtuozzo Hybrid Server***	Agente para Virtuozzo (Incluido en el archivo de instalación del agente para Linux (64 bits))	En el servidor Virtuozzo Hybrid Server.
Equipos virtuales de la Virtuozzo Hybrid Infrastructure	Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual)	En el servidor de la Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2025

Equipos virtuales alojados en Amazon EC2	Ocurre lo mismo con los equipos físicos****	En el equipo del que se hará la copia de seguridad.
Equipos virtuales alojados en Windows Azure.		
Máquinas virtuales Citrix Hypervisor/XenServer		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Máquinas virtuales basadas en Kernel (KVM) no gestionadas por oVirt		
Máquinas virtuales de Oracle no gestionadas por oVirt		
Red Hat Virtualization (RHV/RHEV), gestionado por oVirt	Agente para oVirt (dispositivo virtual)	En el host de virtualización.
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt		
Máquinas virtuales de Oracle gestionadas por oVirt		
Almacenamiento conectado a red		
Synology	Agente para Synology (dispositivo virtual)	En el dispositivo NAS.
Dispositivos móviles		
Dispositivos móviles que ejecutan Android.	Aplicación para dispositivos móviles de Android	En el dispositivo móvil que se incluirá en la copia de seguridad.
Dispositivos móviles que ejecutan iOS	Aplicación para dispositivos móviles de iOS	

* Durante la instalación, Agente para Exchange comprueba si hay suficiente espacio libre en el equipo en que se ejecutará. Durante una recuperación granular, es necesario que el espacio libre coincida temporalmente con el 15 por ciento de la mayor base de datos de Exchange.

**Si su ESXi utiliza un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará copias de seguridad de las máquinas virtuales directamente desde el almacenamiento en lugar de a través del host ESXi y la LAN. Para obtener instrucciones detalladas, consulte "Agente para VMware: copia de seguridad sin LAN" (p. 961).

***Para Virtuozzo 7, solo se admiten los contenedores ploop. No se admiten equipos virtuales.

****Un equipo virtual se considera virtual si se le puede hacer copias de seguridad a través de un agente externo. Si se instala un agente en el sistema invitado, la copia de seguridad y las operaciones de recuperación son iguales que con un equipo físico. Sin embargo, si Cyber Protection puede identificar una máquina virtual utilizando la instrucción CPUID, se le asignará una cuota de

© Acronis International GmbH, 2003-2025

servicio de máquina virtual. Si utiliza un modo de paso directo u otra opción que enmascare el ID del fabricante de la CPU, solo se asignarán las cuotas de servicio para las máquinas físicas.

Requisitos del sistema para agentes

Agente	Espacio de disco necesario para la instalación
Agente para Windows	1,2 GB
Agente para Linux	2 GB
Agente para Mac	1 GB
Agente para SQL y Agente para Windows	1,2 GB
Agente para Exchange y Agente para Windows	1,3 GB
Agente para la prevención de la pérdida de datos	500 MB
Agente para Microsoft 365	500 MB
Agente para Active Directory y Agente para Windows	2 GB
Agente para VMware y Agente para Windows	1,5 GB
Agente para Hyper-V y Agente para Windows	1,5 GB
Agente para Virtuozzo y Agente para Linux	1 GB
Agente para la Virtuozzo Hybrid Infrastructure	700 MB
Agent for Oracle y Agente para Windows	2,2 GB
Agente para Oracle y Agente para Linux	2 GB
Agente para MySQL/MariaDB y Agente para Linux	2 GB

Las operaciones de copia de seguridad, incluido el borrado de copias de seguridad, requieren alrededor de 1 GB de RAM por cada 1 TB de tamaño de copia de seguridad. El consumo de memoria puede variar en función de la cantidad y el tipo de datos que sean procesados por los agentes.

Nota
El uso de la memoria RAM podría aumentar al realizar una copia de seguridad en conjuntos de copias de seguridad de gran tamaño (4 TB y más).

En sistemas x64, las operaciones con un soporte de arranque o una recuperación de disco con reinicio requiere al menos 2 GB de memoria.

© Acronis International GmbH, 2003-2025

En las cargas de trabajo con procesadores modernos, como Intel Core de 11.ª generación o AMD Ryzen 7, que son compatibles con la tecnología CET, se han deshabilitado algunas funciones del agente para la prevención de pérdida de datos a fin de evitar conflictos. En la siguiente tabla, se indica la disponibilidad de las funciones de control de dispositivos y Advanced DLP en sistemas con este tipo de CPU.

Funciones	Control de dispositivos	Advanced DLP
Canales locales		
Almacenamiento extraíble	n/d	Sí
Almacenamiento extraíble cifrado	Sí	n/d
Impresoras	n/d	No
Unidades asignadas redirigidas	n/d	Sí
Portapapeles redirigido	n/d	No
Comunicaciones en red		
Correo electrónico SMTP	n/d	Sí
Microsoft Outlook (MAPI)	n/d	Sí
IBM Notes	n/d	No
Correo web	n/d	Sí
Mensajería instantánea (ICQ)	n/d	No
Mensajería instantánea (Viber)	n/d	No
Mensajería instantánea (IRC, Jabber, Skype, Viber)	n/d	Sí
Servicios de archivos compartidos	n/d	Sí
Redes sociales	n/d	Sí
Uso compartido de archivos en red local (SMB)	n/d	Sí
Acceso web (HTTP/HTTPS)	n/d	Sí
Transferencias de archivos (FTP/FTPS)	n/d	Sí
Lista de permitidos para la transferencia de datos		
Lista de permitidos para tipos de dispositivos	n/d	Sí
Lista de permitidos para comunicaciones en red	n/d	Sí
Lista de permitidos para servidores remotos	n/d	Sí
Lista de permitidos para aplicaciones	n/d	Sí

© Acronis International GmbH, 2003-2025

Dispositivos periféricos		
Almacenamiento extraíble	Sí	Sí
Almacenamiento extraíble cifrado	Sí	Sí
Impresoras	No	No
Dispositivos móviles conectados por MTP	No	No
Adaptadores Bluetooth	Sí	Sí
Unidades ópticas	Sí	Sí
Unidades de disquetes	Sí	Sí
Portapapeles de Windows	No	No
Captura de pantalla	No	No
Unidades asignadas redirigidas	Sí	Sí
Portapapeles redirigido	No	No
Autoprotección de Cyber Protect Agent		
Protección frente a usuarios finales habituales	Sí	Sí
Protección frente a administradores del sistema local	Sí	Sí

Descarga de agentes de protección

Antes de instalar un agente, debe descargar el archivo de instalación de la consola de Cyber Protect.

Para descargar un agente mientras se añade una carga de trabajo para proteger

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Añadir dispositivo** en la esquina superior derecha.
3. Seleccione una versión del agente en el panel **Añadir dispositivos** del menú desplegable **Canal de publicación**.
   - **Más reciente**: descargue la versión más reciente disponible del agente.
   - **Anterior estable**: descargue la versión anterior del agente.
4. Seleccione el agente que corresponda al sistema operativo de la carga de trabajo que añada.
   Se abrirá el cuadro de diálogo **Guardar como**.
5. [Solo para Macs con procesadores Apple silicon (como M1 y M2)] Haga clic en **Cancelar**. En el panel **Añadir Mac** que se abre, pulse en **Descargue el instalador de ARM**.
6. Seleccione una ubicación para guardar el archivo de instalación del agente y haga clic en **Guardar**.

Para descargar un agente para utilizarlo más tarde

© Acronis International GmbH, 2003-2025

1. Haga clic en el icono **Usuario** en la esquina superior derecha de la consola de Cyber Protect.
2. Haga clic en **Descargas**.
3. Seleccione una versión del agente en el cuadro de diálogo **Descargas** del menú desplegable **Canal de publicación**.
   - **Más reciente**: descargue la versión más reciente disponible del agente.
   - **Anterior estable**: descargue la versión anterior del agente.
4. Desplácese por la lista de programas de instalación disponibles para localizar el programa de instalación del agente que necesita y haga clic en el icono de descarga al final de la fila.
   Se abrirá el cuadro de diálogo **Guardar como**.
5. Seleccione una ubicación para guardar el archivo de instalación del agente y haga clic en **Guardar**.

Paquetes de Linux necesarios para la instalación de agentes en Linux

Para agregar los módulos necesarios al kernel de Linux, el agente instalador necesita los siguientes paquetes de Linux:

- El paquete con los encabezados u orígenes de kernel. La versión del paquete debe coincidir con la versión de kernel.
- El sistema compilador GNU Compiler Collection (GCC). La versión GCC debe ser la versión con la que se compiló el kernel.
- La herramienta Make.
- El interpretador Perl.
- Las bibliotecas `libelf-dev`, `libelf-devel` o `elfutils-libelf-devel` para compilar kernel desde 4.15 y configuradas con CONFIG_UNWINDER_ORC=y. Para algunas distribuciones, como Fedora 28, se tienen que instalar de forma independiente a los encabezados de kernel.

Los nombres de estos paquetes pueden variar según su distribución Linux.

En Red Hat Enterprise Linux, CentOS y Fedora, el programa de instalación normalmente instalará los paquetes. En otras distribuciones, debe instalar los paquetes si no están instalados o si no tienen las versiones requeridas.

¿Los paquetes requeridos ya están instalados?

Para verificar si los paquetes ya están instalados, realice los siguientes pasos:

1. Ejecute el siguiente comando para encontrar la versión de kernel y la versión GCC requerida:

   ```
   cat /proc/version
   ```

   Este comando devuelve líneas similares a las siguientes: `Linux version 2.6.35.6` y `gcc version 4.5.1`

© Acronis International GmbH, 2003-2025

2. Ejecute el siguiente comando para verificar si la herramienta Make y el compilador GCC están instalados:

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

   Para **gcc**, asegúrese de que la versión que el comando devuelva sea la misma que en `gcc version` del paso 1. Para **make**, solo tiene que asegurarse de que el comando funcione.
3. Verifique si está instalada la versión apropiada de los paquetes para compilar los módulos de kernel:
   - En Red Hat Enterprise Linux, CentOS y Fedora, ejecute el siguiente comando:

     ```
     yum list installed | grep kernel-devel
     ```

   - En Ubuntu, ejecute los siguientes comandos:

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

   En cualquier caso, asegúrese de que las versiones del paquete sean las mismas que en la `Linux version` del paso 1.
4. Ejecute el siguiente comando para verificar si el interpretador Perl está instalado:

   ```
   perl --version
   ```

   Si ve información sobre la versión Perl, el interpretador está instalado.
5. En Red Hat Enterprise Linux, CentOS y Fedora, ejecute el siguiente comando para comprobar si `elfutils-libelf-devel` está instalado:

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

   Si ve información sobre la versión de la biblioteca, esta se encuentra instalada.

Instalación de los paquetes del repositorio

En la siguiente tabla, se muestra cómo instalar los paquetes requeridos en las diferentes distribuciones Linux.

Distribución Linux	Nombres de los paquetes	Cómo instalar el paquete
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	El programa de instalación descargará e instalará los paquetes de forma automática mediante su suscripción de Red Hat.
	perl	Ejecute el siguiente comando:

© Acronis International GmbH, 2003-2025

		`yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	El programa de instalación descargará e instalará los paquetes automáticamente.
	perl	Ejecute el siguiente comando: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Ejecute los siguientes comandos:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

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

Los paquetes se descargarán del repositorio de distribución y luego se instalarán.

Para otras distribuciones de Linux, consulte la documentación de distribución sobre los nombres exactos de los paquetes requeridos y las maneras de instalarlos.

Instalación manual de los paquetes

Posiblemente, deba instalar los paquetes **manualmente** en los siguientes casos:

- El equipo no tiene una suscripción activa de Red Hat o una conexión a Internet.
- El programa de instalación no puede encontrar la versión **kernel-devel** o **gcc** que corresponden a la versión de kernel. Si el **kernel-devel** disponible es más reciente que su kernel, deberá actualizar su kernel o instalar manualmente la versión **kernel-devel** coincidente.
- Cuenta con los paquetes requeridos en la red local y no desea destinar su tiempo en una búsqueda automática y descarga.

Obtiene los paquetes de su red local o un sitio web de terceros confiable y los instala de la siguiente manera:

- En Red Hat Enterprise Linux, CentOS o Fedora, ejecute el siguiente comando como el usuario raíz:

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


© Acronis International GmbH, 2003-2025

- En Ubuntu, ejecute el siguiente comando:

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

Ejemplo: Instalación manual de los paquetes en Fedora 14

Siga estos pasos para instalar los paquetes requeridos en un equipo Fedora de 14 o 32 bits:

1. Ejecute el siguiente comando para determinar la versión de kernel y la versión GCC requerida:

   ```
   cat /proc/version
   ```

   El resultado de este comando incluye lo siguiente:

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

2. Obtenga los paquetes **kernel-devel** y **gcc** que corresponden a esta versión de kernel:

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

3. Obtenga el paquete **make** para Fedora 14:

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

4. Para instalar los paquetes, ejecute los siguientes comandos como el usuario raíz:

   ```
   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
   ```

   Puede especificar todos estos paquetes en un solo comando `rpm`. Para instalar cualquiera de estos paquetes, es posible que se deban instalar paquetes adicionales para resolver las dependencias.

Ajuste de la configuración del servidor proxy

Los agentes de protección de pueden transferir datos a través de un servidor proxy HTTP o HTTPS. El servidor debe operar a través de un túnel HTTP sin analizar el tráfico HTTP ni interferir con este. No se admiten los proxy de tipo "Man in the middle".

Puesto que el agente se registra en la nube durante la instalación, debe configurar los ajustes del servidor proxy antes o durante la instalación.

Para Windows

Si se configura un servidor proxy en **Panel de control** > **Opciones de Internet** > **Conexiones**, el programa de instalación lee la configuración del servidor proxy del registro y la usa automáticamente.

© Acronis International GmbH, 2003-2025

Utilice este procedimiento si desea ejecutar las siguientes tareas.

- Configure los ajustes de proxy antes de la instalación del agente.
- Actualice los ajustes de proxy después de la instalación del agente.

Para configurar los ajustes de proxy durante la instalación del agente, consulte "Instalación de agentes de protección en Windows" (p. 65).

Nota
Este procedimiento solo es válido cuando el archivo `http-proxy.yaml` no existe en el equipo. Si el archivo `http-proxy.yaml` existe en el equipo, debe actualizar la configuración del proxy en el archivo, ya que sobrescribirá la configuración del archivo `aakore.yaml`.

El archivo `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` se crea cuando configura los ajustes del servidor proxy mediante Cyber Protection Monitor. Para obtener más información, consulte "Configuración del servidor proxy en Cyber Protect Monitor" (p. 362).

Para abrir el archivo `http-proxy.yaml`, debe formar parte del grupo de Administradores en Windows.

Pasos para configurar los ajustes de proxy

1. Cree un nuevo documento de texto y ábralo con un editor de texto, como por ejemplo, Bloc de notas.
2. Copie y pegue las siguientes líneas en el archivo.

```
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. Sustituya `proxy.company.com` por el nombre/dirección IP de su servidor proxy y `000001bb` por el valor hexadecimal del número de puerto. Por ejemplo, `000001bb` es el puerto 443.
4. Si su servidor proxy necesita que se autentifique, sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.
5. Guarde el documento como `proxy.reg`.
6. Ejecute el archivo como administrador.
7. Confirme que desea editar el registro de Windows.
8. Si el agente todavía no está instalado en esta carga de trabajo, ahora puede instalarlo. Si el agente ya está instalado en la carga de trabajo, vaya al siguiente paso.
9. Abra el archivo `%programdata%\Acronis\Agent\etc\aakore.yaml` en un editor de texto.
   Para abrir este archivo, debe formar parte del grupo de Administradores en Windows.

© Acronis International GmbH, 2003-2025

10. Busque la sección **env** o créela y añada las siguientes líneas:

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

11. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.
12. En el menú **Inicio**, haga clic en **Ejecutar**, escriba **cmd** y, a continuación, haga clic en **Aceptar**.
13. Reinicie el servicio aakore con los siguientes comandos:

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

14. Reinicie el agente con los siguientes comandos:

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

Para macOS

Utilice este procedimiento si desea ejecutar las siguientes tareas.

- Configure los ajustes de proxy antes de la instalación del agente.
- Actualice los ajustes de proxy después de la instalación del agente.

Para configurar los ajustes de proxy durante la instalación del agente, consulte "Instalación de agentes de protección en macOS" (p. 72).

Pasos para configurar los ajustes de proxy

1. Cree el archivo `/Library/Application Support/Acronis/Registry/Global.config` y ábralo con un editor de texto, como Text Edit.
2. Copie y pegue las siguientes líneas en el archivo.

```
<?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. Sustituya `proxy.company.com` por el nombre/dirección IP de su servidor proxy y `443` por el valor decimal del número de puerto.
4. Si su servidor proxy necesita que se autentifique, sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.

© Acronis International GmbH, 2003-2025

5. Guarde el archivo.
6. Si el agente todavía no está instalado en esta carga de trabajo, ahora puede instalarlo. Si el agente ya está instalado en la carga de trabajo, vaya al siguiente paso.
7. Abra el archivo `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` en un editor de texto:
8. Busque la sección **env** o créela y añada las siguientes líneas:

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

9. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.
10. Vaya a **Aplicaciones** > **Utilidades** > **Terminal**.
11. Reinicie el servicio aakore con los siguientes comandos:

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

12. Reinicie el agente con los siguientes comandos:

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

Para Linux

Ejecute el archivo de instalación con estos parámetros: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Use el siguiente procedimiento para actualizar los ajustes de proxy después de la instalación del agente de protección.

Pasos para configurar los ajustes de proxy

1. Abra el archivo `/etc/Acronis/Global.config` en un editor de texto:
2. Realice uno de los siguientes procedimientos:
   - Si especificó la configuración del servidor proxy durante la instalación del agente, localice la sección siguiente:

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

   - Si no especificó la configuración de proxy durante la instalación del agente, copie las siguientes líneas y péguelas en el archivo entre las etiquetas `<registry`

© Acronis International GmbH, 2003-2025

name="Global">...</registry>.

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

3. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.
4. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` Y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.
5. Guarde el archivo.
6. Abra el archivo `/opt/acronis/etc/aakore.yaml` en un editor de texto.
7. Busque la sección **env** o créela y añada las siguientes líneas:

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

8. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.
9. Reinicie el servicio aakore con el siguiente comando:

```
sudo service aakore restart
```

10. Reinicie el agente ejecutando el comando que se ejecuta en cualquier directorio.

```
sudo service acronis_mms restart
```

Para el dispositivo de arranque

Cuando trabaje con dispositivos de arranque, es posible que necesite acceder al almacenamiento en la nube a través de un servidor proxy. Para configurar los ajustes del servidor proxy, haga clic en **Herramientas** > **Servidor proxy** y, a continuación, configure el nombre de servidor/dirección IP, el puerto y las credenciales del servidor proxy.

Instalación dinámica de componentes

Para las cargas de trabajo de Windows protegidas con el agente de la versión 15.0.26986 (lanzado en mayo de 2021) o posteriores, los siguientes componentes se instalan dinámicamente, es decir, solo cuando lo requiere un plan de protección:

- Agente de protección antimalware y filtrado de URL: requerido para que funcionen la protección antimalware y el filtrado de URL.

© Acronis International GmbH, 2003-2025

- Agente para la prevención de pérdida de datos: necesario para el control de dispositivos.

De forma predeterminada, no se instalarán estos componentes. El correspondiente componente se instala automáticamente si una carga de trabajo se protege con un plan en el cual está habilitado el módulo de **Protección antivirus y antimalware**.

De forma predeterminada, no se instalarán estos componentes. El correspondiente componente se instala automáticamente si una carga de trabajo se protege con un plan en el cual están habilitados cualquiera de los siguientes módulos:

- **Protección antivirus y antimalware**
- **Filtrado de URL**
- **Control de dispositivos**

De manera similar, si ningún plan de protección requiere protección antimalware, filtrado de URL ni control de dispositivos, el correspondiente componente se desinstalará automáticamente.

De manera similar, si ningún plan de protección requiere protección antimalware, el correspondiente componente se desinstalará automáticamente.

La instalación o desinstalación dinámica de componentes puede tardar hasta 10 minutos después de aplicar, revocar, editar o eliminar un plan de protección. Si se está ejecutando alguna de las siguientes operaciones, la instalación o desinstalación dinámica comenzará después de que se complete la operación:

- Copia de seguridad
- Recuperación
- Réplica de copia de seguridad
- Réplica de máquina virtual
- Realización de pruebas en una réplica
- Ejecución de una máquina virtual desde una copia de seguridad (con finalización)
- Conmutación por error de la recuperación ante desastres
- Conmutación por recuperación de la recuperación ante desastres
- Ejecución de una secuencia de comandos (para la funcionalidad de Secuencia de comandos cibernética)
- Instalación del parche
- Copia de seguridad de configuración de ESXi

Conceder los permisos de sistema necesarios para el Agente de Connect

Para habilitar todas las funciones desde la funcionalidad del escritorio remoto de las cargas de trabajo de macOS, además del permiso de acceso completo al disco, debe otorgar los siguientes

© Acronis International GmbH, 2003-2025

permisos al Agente de Connect:

- **Grabación de pantalla**: habilita la grabación de pantalla del recurso informático de macOS mediante NEAR. Hasta que no se otorgue este permiso, se niegan todas las conexiones de control remoto.
- **Accesibilidad**: habilita las conexiones remotas en el modo de control mediante NEAR.
- **Micrófono**: habilita el redireccionamiento de sonido desde el recurso informático remoto de macOS al recurso inforático local mediante NEAR. Para habilitar la función de redireccionamiento del sonido, se debe instalar un controlador de captura del sonido en el recurso informático. Para obtener más información, consulte "Redireccionamiento de sonido remoto" (p. 1447).
- **Automatización**: habilita la acción de vaciar papelera de reciclaje.
- **Servicios de ubicación**: habilita los servicios de ubicación en el recurso informático. Hasta que se conceda este permiso, el agente no puede rastrear la ubicación del recurso informático.

Después de iniciar el agente en la carga de trabajo de macOS, comprobará si el agente tiene estos derechos y le pedirá que otorgue permisos si es necesario.

Pasos para otorgar permiso de grabación de pantalla

1. En el cuadro de diálogo **Otorgar permisos de sistema obligatorios al agente de Cyber Protect**, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos del sistema**, en la fila **Grabación de pantalla**, haga clic en **Adquirir**.
3. Haga clic en **Abrir configuración del sistema**.
4. Para **Agente de Connect**, active el interruptor.

Si el agente no tiene permiso cuando intente acceder a la carga de trabajo de forma remota, se mostrara el cuadro de diálogo de solicitud de permiso de grabación de pantalla. Solo el usuario local puede responder al cuadro de diálogo.

Pasos para otorgar el permiso de accesibilidad

1. En el cuadro de diálogo **Otorgar permisos de sistema obligatorios al agente de Cyber Protect**, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos del sistema**, en la fila **Accesibilidad**, haga clic en **Adquirir**.
3. Haga clic en **Abrir configuración del sistema**.
4. Haga clic en el icono del candado en la esquina inferior izquierda de la ventana para que cambie a un icono desbloqueado. El sistema le pedirá una contraseña de administrador para hacer cambios.
5. Seleccione **Agente de Connect**.

Pasos para otorgar el permiso de micrófono

1. En el cuadro de diálogo **Otorgar permisos de sistema obligatorios al agente de Cyber Protect**, haga clic en **Configurar permisos del sistema**.

© Acronis International GmbH, 2003-2025

2. En el cuadro de diálogo **Permisos del sistema**, en la fila **Micrófono**, haga clic en **Adquirir**.
3. En la ventana de confirmación, haga clic en **Permitir**.

Nota
Para permitir que el agente utilice el permiso dado y realice el redireccionamiento del sonido del recurso informático, también debe instalar un controlador de captura de sonido en el recurso informático de macOS. Para obtener más información, consulte "Redireccionamiento de sonido remoto" (p. 1447).

Pasos para otorgar el permiso de automatización

1. En el cuadro de diálogo **Otorgar permisos de sistema obligatorios al diálogo Agente de Connect**, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos del sistema**, en la fila **Automatización**, haga clic en **Adquirir**.
3. En la ventana de confirmación, haga clic en **Permitir**.

Pasos para conceder el permiso de Servicios de ubicación

1. En el cuadro de diálogo **Otorgar permisos de sistema obligatorios al diálogo Agente de Connect**, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos del sistema**, en la fila **Servicios de ubicación**, haga clic en **Adquirir**.
3. En la ventana de confirmación, haga clic en **Permitir**.

Modo compatible con FIPS

Para ajustarse a los requisitos de cumplimiento, puede instalar y utilizar agentes de protección en el modo compatible con FIPS.

Este modo utiliza únicamente algoritmos y bibliotecas de criptografía que están certificados de acuerdo con los estándares federales de procesamiento de la información 140-2, de la siguiente manera:

- [Windows] API de criptografía de Microsoft con certificación FIPS: Next Generation (CNG).
- [Linux] Biblioteca BoringCrypto con certificación FIPS.
- [Windows y Linux] Módulo OpenSSL 3 con certificación FIPS.

El modo compatible con FIPS es compatible con los siguientes agentes:

- Agente para Windows (en sistemas operativos de 64 bits)
  Consulte las versiones compatibles en "Agente para Windows" (p. 499).

  Nota
  El Agente para Windows (heredado) no es compatible con el modo compatible con FIPS.

- Agente para Linux

© Acronis International GmbH, 2003-2025

Consulte las versiones compatibles en "Agente para Linux" (p. 504).

- Dispositivos virtuales
  - Agente para VMware (dispositivo virtual)
  - Agente para la Virtuozzo Hybrid Infrastructure
  - Agent para Scale Computing HC3
  - Agente para oVirt

Limitaciones

- Los siguientes componentes o servicios no son compatibles con FIPS:
  - File Sync & Share
  - Endpoint Detection and Response (EDR)
  - Recuperación ante desastres
  - Prevención de pérdida de datos (DLP)
  - Aplicación de Acronis Cyber Protect(copia de seguridad de dispositivos móviles)
  - Envío de datos físicos
  - Consola de Web Restore
- Los dispositivos virtuales en modo compatible con FIPS no admiten recursos compartidos de pymes.
- El dispositivo de arranque que se crea con el Agente para Windows compatible con FIPS o el Agente para Linux compatible con FIPS no admite recursos compartidos de pymes.
- Puede seleccionar el modo FIPS para el Agent para Windows y Agente para Linux solo durante la instalación. Para cambiar el modo FIPS más adelante, ejecute el archivo de instalación nuevamente y modifique la instalación.

Instalación del Agente para Windows en modo compatible con FIPS

Puede instalar el Agente para Windows en el modo compatible con FIPS mediante la interfaz gráfica de usuario o la interfaz de línea de comandos.

Requisitos previos

- Su recurso informático tiene un sistema operativo Windows de 64 bits.
- El sistema operativo del recurso informático está funcionando en modo FIPS.
  Para obtener más información, consulte Criptografía del sistema: use algoritmos compatibles con FIPS para el cifrado, el hash y la firma en la documentación de Microsoft.
- Ha descargado el archivo de instalación del Agente para Windows.
  Para obtener más información, consulte "Descarga de agentes de protección" (p. 49).

Pasos para instalar el Agente para Windows en modo compatible con FIPS

Interfaz gráfica de usuario

© Acronis International GmbH, 2003-2025

1. Ejecute Símbolo del sistema como administrador en el equipo en el que desee instalar el agente.
2. En Símbolo del sistema, navegue hasta el archivo de instalación.
3. Para ejecutar el procedimiento de instalación en modo compatible con FIPS y continuar en la interfaz gráfica de usuario, ejecute el siguiente comando:

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

   Por ejemplo:

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

4. [Opcional] Haga clic en **Personalizar la configuración de instalación** y, a continuación, configure los ajustes de instalación.

   Las siguientes opciones están disponibles:

   - Cambiar los componentes que se deben instalar (por ejemplo, deshabilitar la instalación de Cyber Protection Monitor o la herramienta de línea de comandos o instalar el agente de protección antimalware y el filtrado de URL).

     Nota
     En equipos Windows, las funciones de protección antimalware y filtrado de URL requieren la instalación del agente de protección antimalware y del filtrado de URL. Este agente se instalará automáticamente para los recursos informáticos protegidos si la **Protección antivirus y antimalware** y/o las opciones de **Filtrado de URL** están habilitadas en sus planes de protección.

   - Cambiar el método de registro del recurso informático en el servicio de Cyber Protection. Puede cambiar de **Usar la consola de servicio** (opción predeterminada) a **Usar credenciales** o **Usar token de registro**.
   - Cambio de la ruta de acceso de instalación.
   - Cambiar la cuenta de usuario con la que se ejecutará el servicio de agente. Para obtener más información, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 67).
   - Verificar o cambiar el nombre del host o la dirección IP de un servidor proxy, el puerto, el nombre de usuario y la contraseña para acceder a él.

     La contraseña puede incluir caracteres alfanuméricos en minúsculas y mayúsculas, y los siguientes caracteres especiales:

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

     Nota
     Si hay un servidor proxy habilitado en Windows, se detectará y usará automáticamente.

5. Haga clic en **Instalar**.

© Acronis International GmbH, 2003-2025

6. [Solo al instalar Agente para VMware] Especifique la dirección y las credenciales de acceso del servidor vCenter Server o del host ESXi independiente del que quiera hacer una copia de seguridad y recuperar las máquinas virtuales. Después, haga clic en **Listo**.
   Recomendamos que utilice una cuenta dedicada para acceder al servidor vCenter o al host ESXi, en lugar de usar una cuenta existente con el rol de Administrador. Para obtener más información, consulte "Privilegios necesarios para el agente para VMware" (p. 971).
7. [Solo al instalar en un controlador de dominio] Especifique la cuenta de usuario en la que se ejecutará el servicio de agente. Después, haga clic en **Listo**. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

   Nota
   A la cuenta de usuario que especifique se le debe conceder el privilegio `Iniciar sesión como un servicio`. Esta cuenta ya debe haberse usado en el controlador de dominio para que se cree su carpeta de perfiles en dicho equipo.

   Para obtener más información sobre la instalación del agente en un controlador de dominio de solo lectura, consulte este artículo de la base de conocimientos.
8. [Si ha seleccionado el método de registro predeterminado **Usar la consola de servicio**] Espere hasta que aparezca la pantalla de registro.
9. Registre al agente bajo una cuenta de usuario en un inquilino de cliente. Para obtener más información sobre el registro, consulte "Registro de cargas de trabajo utilizando la interfaz gráfica de usuario" (p. 110).
10. [Si ha registrado el agente en un inquilino que utiliza el modo cumplimiento] Establezca la contraseña de cifrado.

Interfaz de la línea de comandos

1. Ejecute Símbolo del sistema como administrador en el equipo en el que desee instalar el agente.
2. En Símbolo del sistema, navegue hasta el archivo de instalación.
3. Ejecute el siguiente comando:

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

   Utilice espacios para separar los parámetros y comas sin espacios para separar los valores de un parámetro. Por ejemplo:

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

   Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (EXE)" (p. 78).

© Acronis International GmbH, 2003-2025

Nota
Para instalar agentes compatibles con FIPS en varios equipos, puede utilizar un archivo MSI que se crea mediante un agente compatible con FIPS. Para obtener más información sobre la instalación de agentes con un archivo MSI, consulte "Instalación desatendida y desinstalación con un archivo MSI" (p. 84).

Instalación del Agente para Linux en el modo compatible con FIPS

Puede instalar el Agente para Linux en el modo compatible con FIPS mediante la interfaz de línea de comandos.

Requisitos previos

- Ha descargado el paquete de instalación del Agente para Linux.

Pasos para instalar el Agente para Linux en modo compatible con FIPS

1. Abra el Terminal.
2. Realice uno de los siguientes procedimientos:
   - Para instalar el agente especificando los parámetros de la línea de comando, ejecute el siguiente comando:

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

     Aquí, <package name> es el nombre del paquete de instalación (un archivo .i686 o .x86_64). Consulte los parámetros disponibles y sus valores se describen en "Parámetros de instalación o desinstalación sin supervisión" (p. 95).
   - Para instlalar el agente con los parámetros que se especifican en un archivo de texto independiente, ejecute el siguiente comando:

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

     Este enfoque puede ser útil si no desea introducir información confidencial en la línea de comandos. En este caso, puede especificar los parámetros de configuración en un archivo de texto independiente y asegurarse de que solo usted pueda acceder al mismo. Coloque cada parámetro en una nueva línea, seguido del valor correspondiente para cada parámetro. Por ejemplo:

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

     o

     ```
     -C
     https://cloud.company.com
     ```


© Acronis International GmbH, 2003-2025

```
-g
johndoe
-w
johnspassword
-a
--language
en
```

Si se especifica el mismo parámetro en la línea de comando y en el archivo de texto, precede el valor de la línea de comando.

3. Si el arranque UEFI seguro está habilitado en el equipo, se le pedirá que reinicie el sistema después de la instalación. Cuando se le pida una contraseña, use la contraseña para el usuario root. Si esta contraseña no es aceptada, use la palabra "acronis" como contraseña. Durante el reinicio del sistema, elija la gestión de MOK (clave del propietario del equipo), seleccione **Registrar MOK** y, a continuación, registre la clave usando la contraseña recomendada.
   Si habilita el arranque seguro UEFI después de instalar el agente, repita la instalación, incluido este paso. En caso contrario, las copias de seguridad fallarán.

Habilitación del modo compatible con FIPS para un dispositivo virtual

Puede habilitar el modo compatible con FIPS en la consola del dispositivo.

Requisitos previos

- Un dispositivo virtual se despliega y configura.

Pasos para habilitar el modo FIPS en un dispositivo virtual

1. Inicie sesión en la interfaz del hipervisor como administrador.
2. Abra la consola del dispositivo virtual.
3. En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Como resultado, el dispositivo virtual se reinicia. Después del reinicio, este opera en modo compatible con FIPS.

Instalación de agentes de protección utilizando la interfaz gráfica de usuario

Instalación de agentes de protección en Windows

Requisitos previos

© Acronis International GmbH, 2003-2025

- Se descarga un archivo de instalación del agente de protección en el recurso informático que desea proteger. Consulte "Descarga de agentes de protección" (p. 49).
- El recurso informático que desea proteger está conectada a Internet.

Pasos para instalar Agente para Windows

1. Inicie sesión como administrador en el recurso informático que desea proteger y, a continuación, abra el archivo del programa de instalación.
2. [Opcional] Haga clic en **Personalizar la configuración de instalación** y, a continuación, configure los ajustes de instalación.

   Las siguientes opciones están disponibles:

   - Cambiar los componentes que se deben instalar (por ejemplo, deshabilitar la instalación de Cyber Protection Monitor o la herramienta de línea de comandos o instalar el agente de protección antimalware y el filtrado de URL).

     Nota
     En equipos Windows, las funciones de protección antimalware y filtrado de URL requieren la instalación del agente de protección antimalware y del filtrado de URL. Este agente se instalará automáticamente para los recursos informáticos protegidos si la **Protección antivirus y antimalware** y/o las opciones de **Filtrado de URL** están habilitadas en sus planes de protección.

   - Cambiar el método de registro del recurso informático en el servicio de Cyber Protection. Puede cambiar de **Usar la consola de servicio** (opción predeterminada) a **Usar credenciales** o **Usar token de registro**.
   - Cambio de la ruta de acceso de instalación.
   - Cambiar la cuenta de usuario con la que se ejecutará el servicio de agente. Para obtener más información, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 67).
   - Verificar o cambiar el nombre del host o la dirección IP de un servidor proxy, el puerto, el nombre de usuario y la contraseña para acceder a él.

     La contraseña puede incluir caracteres alfanuméricos en minúsculas y mayúsculas, y los siguientes caracteres especiales:

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

     Nota
     Si hay un servidor proxy habilitado en Windows, se detectará y usará automáticamente.
3. Haga clic en **Instalar**.
4. [Solo al instalar Agente para VMware] Especifique la dirección y las credenciales de acceso del servidor vCenter Server o del host ESXi independiente del que quiera hacer una copia de seguridad y recuperar las máquinas virtuales. Después, haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Recomendamos que utilice una cuenta dedicada para acceder al servidor vCenter o al host ESXi, en lugar de usar una cuenta existente con el rol de Administrador. Para obtener más información, consulte "Privilegios necesarios para el agente para VMware" (p. 971).

5. [Solo al instalar en un controlador de dominio] Especifique la cuenta de usuario en la que se ejecutará el servicio de agente. Después, haga clic en **Listo**. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

   Nota
   A la cuenta de usuario que especifique se le debe conceder el privilegio `Iniciar sesión como un servicio`. Esta cuenta ya debe haberse usado en el controlador de dominio para que se cree su carpeta de perfiles en dicho equipo.

   Para obtener más información sobre la instalación del agente en un controlador de dominio de solo lectura, consulte este artículo de la base de conocimientos.
6. [Si ha seleccionado el método de registro predeterminado **Usar la consola de servicio**] Espere hasta que aparezca la pantalla de registro.
7. Registre al agente bajo una cuenta de usuario en un inquilino de cliente. Para obtener más información sobre el registro, consulte "Registro de cargas de trabajo utilizando la interfaz gráfica de usuario" (p. 110).
8. [Si ha registrado el agente en un inquilino que utiliza el modo cumplimiento] Establezca la contraseña de cifrado.

Cómo cambiar la cuenta de inicio de sesión en equipos Windows

En la pestaña **Seleccionar componentes del agente**, defina la cuenta en la que se ejecutarán los servicios especificando **Cuenta de inicio de sesión para el servicio de agente**. Puede seleccionar una de las siguientes opciones:

- **Usar cuentas de usuario del servicio** (opción predeterminada para el servicio de agente)
  Las cuentas de usuario del servicio son cuentas de sistema de Windows que se utilizan para ejecutar servicios. La ventaja de este ajuste es que las directivas de seguridad de dominios no afectan a los derechos de usuario de estas cuentas. De forma predeterminada, el agente se ejecuta desde la cuenta **Sistema local**.
- **Crear una cuenta nueva**
  El nombre de cuenta del agente será Agent User.
- **Utilice la siguiente cuenta**
  Si instala el agente en un controlador de dominios, el sistema le pedirá que especifique las cuentas actuales (o una misma cuenta) para cada agente. Por razones de seguridad, el sistema no crea automáticamente nuevas cuentas en un controlador de dominio.
  A la cuenta de usuario que especifique cuando el programa de instalación se ejecute en un controlador de dominio se le debe conceder el privilegio `Iniciar sesión como un servicio`. Esta cuenta ya debe haberse usado en el controlador de dominio para que se cree su carpeta de perfiles en dicho equipo.

© Acronis International GmbH, 2003-2025

Consulte también "Uso de cuentas gMSA con el agente de Cyber Protection" (p. 69).

Para obtener más información sobre la instalación del agente en un controlador de dominio de solo lectura, consulte este artículo de la base de conocimientos.

Nota
Si selecciona la opción **Crear una cuenta nueva** o **Utilice la siguiente cuenta**, asegúrese de que las directivas de seguridad de dominio no afecten a los derechos de las cuentas relacionadas. Si se niegan los derechos de usuario para una cuenta durante la instalación, el componente podría no funcionar correctamente o no funcionar en absoluto.

Importante
No es recomendable cambiar las cuentas de inicio de sesión manualmente una vez que ha terminado la instalación.

Privilegios necesarios para la cuenta de inicio de sesión

El agente de Cyber Protection se ejecuta como un Servicio de equipo administrado (MMS) para Windows. La cuenta con la que se ejecutará el agente debe tener derechos específicos para que el agente funcione correctamente. Por lo tanto, debería configurarse el usuario MMS de la siguiente manera:

1. Incluirlo en los grupos **Operadores de copia de seguridad** y **Administradores**. En un controlador de dominio, el usuario debe incluirse en el grupo **Administradores del dominio**.
2. Se le concede el permiso de **Control total** en la carpeta `%PROGRAMDATA%\Acronis` y en sus subcarpetas.

   Para Windows XP y Server 2003, se deben conceder permisos en la carpeta `%ALLUSERSPROFILE%\Application Data\Acronis` y sus subcarpetas.
3. Cada una de las tres cuentas tiene permiso de **Control total** en las claves de registro en la siguiente clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Asignarle los siguientes derechos de usuario:
   - Inicio de sesión como un servicio
   - Ajustar cantidades máximas de memoria para un proceso
   - Reemplazar símbolo de nivel de un proceso
   - Modificar los valores del entorno de firmware

Cómo asignar derechos de usuario

Siga las instrucciones que aparecen a continuación para asignar los derechos de usuario (en este ejemplo se usa el derecho de usuario **Iniciar sesión como servicio**; los pasos son los mismos para el resto de derechos de usuario):

1. Inicie sesión en el equipo con una cuenta con privilegios administrativos.
2. Desde el **Panel de control** de Windows, abra **Herramientas administrativas** y, a continuación, abra **Directiva de seguridad local**.

© Acronis International GmbH, 2003-2025

3. Despliegue **Directivas locales** y haga clic en **Asignación de derechos de usuario**.
4. En el panel de la derecha, haga clic derecho en **Iniciar sesión como un servicio** y seleccione **Propiedades**.
5. Haga clic en el botón **Añadir usuario o grupo...** para agregar un nuevo usuario.
6. En la ventana **Seleccionar usuarios, ordenadores, cuentas de servicio o grupos**, busque la cuenta a la que desea asignar este privilegio y haga clic en **Aceptar**.
7. Haga clic en **Aceptar** en las **propiedad de Iniciar sesión como un servicio** para guardar los cambios.

Importante
Asegúrese de que el usuario que ha añadido al derecho de usuario **Inicio de sesión como un servicio** no aparezca en la política **Rechazar inicio de sesión como servicio** en **Política de seguridad local**.

Uso de cuentas gMSA con el agente de Cyber Protection

Las cuentas de servicio administradas de grupo (gMSA) se pueden utilizar para ejecutar servicios en varios servidores sin tener que gestionar la contraseña.

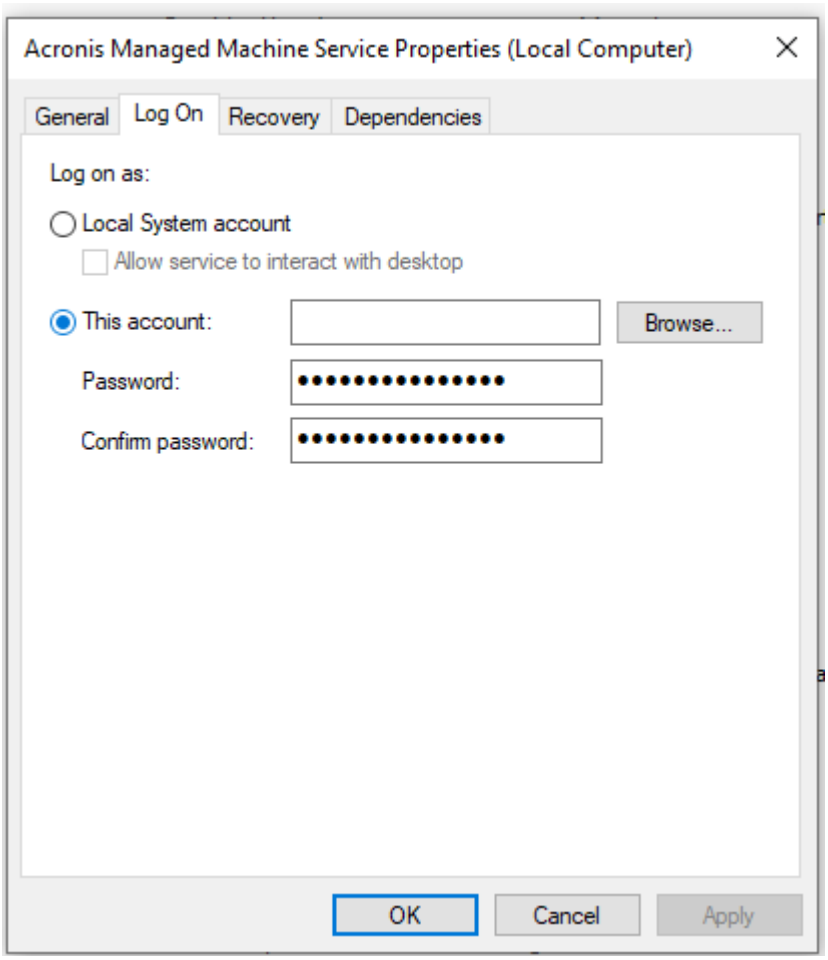
El siguiente procedimiento es aplicable si desea cambiar la cuenta de usuario utilizada por el agente de Acronis Cyber Protection después de la instalación, para que el agente pueda utilizar una gMSA.

Importante
Todos los planes de protección que se hayan asignado previamente al equipo en el que está cambiando la cuenta de inicio de sesión dejarán de funcionar y tendrá que revocarlos y volver a aplicarlos después de haber cambiado la cuenta.

Para habilitar el uso de una gMSA para el agente de Cyber Protection

1. Cree una gMSA siguiendo el procedimiento estándar documentado en la base de conocimientos de Microsoft.
2. Configure la gMSA como se describe en la sección "Privilegios necesarios para la cuenta de inicio de sesión" (p. 68).
3. Asigne la gMSA como la cuenta de inicio de sesión para el servicio MMS en el equipo donde se ejecuta el agente.
   a. Abra el menú de inicio de Windows y escriba `services.msc` para abrir la lista de servicios locales.
   b. Haga clic derecho en **Acronis Managed Machine Service** y haga clic en **Propiedades**.
   c. En la pestaña **Inicio de sesión**, seleccione **Esta cuenta** y haga clic en **Examinar** para buscar la gMSA que desea usar.

© Acronis International GmbH, 2003-2025



d. Haga clic en **Aceptar**.

4. Aplique los planes de protección según sea necesario.
   - Si tenía planes de protección aplicados al equipo antes de cambiar la cuenta de inicio de sesión, revoque esos planes y aplíquelos de nuevo.
   - Si no tenía planes de protección aplicados al equipo, cree nuevos o seleccione los existentes y aplíquelos.

Instalación de agentes de protección en Linux

Puede instalar el Agente para Linux al ejecutar su archivo de instalación en un equipo local.

Requisitos previos

- Ha descargado el archivo de instalación para el Agente para Linux. Consulte "Descarga de agentes de protección" (p. 49).

  El paquete de instalación de 64 bits contiene agentes adicionales, como Agente para Virtuozzo, Agente para Oracle, Agente para MySQL/MariaDB y Agente para Proxmox. Estos agentes dependen del Agente para Linux y se instalan junto con él.
- Ha instalado los paquetes de Linux necesarios.
- En el equipo en el que desee instalar el agente, debe haber al menos 2 GB de espacio libre en el disco.

© Acronis International GmbH, 2003-2025

- Cuando instale el agente en SUSE Linux, asegúrese de usar `su -` en lugar de `sudo`. De lo contrario, se producirá el siguiente error al intentar registrar el agente a través de la consola de Cyber Protect: "Error al iniciar el navegador web. No hay ninguna pantalla disponible". Algunas distribuciones de Linux, como SUSE, no pasan la variable DISPLAY al usar `sudo` y el programa de instalación no puede abrir el navegador en la interfaz gráfica de usuario (GUI).

Limitaciones

- Algunas distribuciones de Linux no permiten la instalación de paquetes firmados con SHA-1. En tales casos, la instalación falla con el siguiente mensaje: "No se puede encontrar el paquete Agente de copia de seguridad y recuperación". Para obtener más información sobre cómo resolver este problema, consulte este artículo de la base de conocimiento.

Para instalar Agente para Linux

1. Asegúrese de que el equipo está conectado a Internet.
2. Como el usuario raíz, vaya al directorio con el archivo de instalación, haga el archivo ejecutable y ejecútelo.

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

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

   Si hay un servidor proxy habilitado en la red, al ejecutar el archivo de instalación, especifique el nombre del host o la dirección IP del servidor y el puerto en el formato siguiente: `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD`.

   Si desea cambiar el método predeterminado de registro del equipo en el servicio de Cyber Protection, ejecute el archivo de instalación con uno de los parámetros siguientes:

   - `--register-with-credentials`: para que se solicite un nombre de usuario y una contraseña durante la instalación
   - `--token=STRING`: para que se utilice un token de registro
   - `--skip-registration`: para omitir el registro
3. Seleccione las casillas de verificación de los agentes que desea instalar. En el paquete de instalación de 64 bits, los agentes disponibles son los siguientes:
   - Agente para Linux
   - Agente para Virtuozzo
   - Agente para Oracle
   - Agente para MySQL/MariaDB
   - Agente para Proxmox
4. Si ha seguido el método de registro predeterminado en el paso 2, continúe con el paso siguiente. En caso contrario, introduzca el nombre de usuario y la contraseña para el servicio de Cyber Protection o espere hasta que el equipo se registre mediante el token.

© Acronis International GmbH, 2003-2025

5. Registre al agente bajo una cuenta de usuario en un inquilino de cliente. Para obtener más información sobre el registro, consulte "Registro de cargas de trabajo utilizando la interfaz gráfica de usuario" (p. 110).
6. [Si ha registrado el agente en un inquilino que utiliza el modo cumplimiento] Establezca la contraseña de cifrado.
7. Si el arranque UEFI seguro está habilitado en el equipo, se le informará de que debe reiniciar el sistema después de la instalación. Cuando se le solicite una contraseña, utilice la contraseña para el usuario root. Si esta contraseña no es aceptada, utilice la palabra "acronis" como contraseña.

   Nota
   La instalación genera una nueva clave que se utiliza para firmar módulos de kernel. Deberá registrar esta nueva clave en la lista de Machine Owner Key (MOK) mediante el reinicio del equipo. Si no se registra la nueva clave, su agente no estará operativo. Si habilita el arranque seguro UEFI después de la instalación del agente, deberá reinstalar el agente.

8. Una vez finalizada la instalación, lleve a cabo una de las siguientes acciones:
   - Haga clic en **Reiniciar**, si en el paso anterior se le ha pedido que reinicie el sistema.
     Durante el reinicio del sistema, opte por la gestión de MOK (clave del propietario del equipo), seleccione **Registrar MOK** y, a continuación, registre la clave por medio de la contraseña recomendada en el paso anterior.
   - En caso contrario, haga clic en **Salir**.

Encontrará información sobre la solución de problemas en el siguiente archivo:
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Instalación de agentes de protección en macOS

Requisitos previos

- Se descarga un archivo de instalación del agente de protección en el recurso informático que desea proteger. Consulte "Descarga de agentes de protección" (p. 49).
- El recurso informático que desea proteger está conectada a Internet.

Pasos para instalar Agente para Mac (x64 o ARM64)

1. Asegúrese de que el equipo está conectado a Internet.
2. Haga doble clic sobre el archivo de instalación (.dmg).
3. Espere mientras el sistema operativo monta la imagen del disco de instalación.
4. Haga doble clic en **Instalar**.
5. Si en la red hay un servidor proxy habilitado, haga clic en **Agente de protección**, en la barra de menú, y luego en **Configuración del servidor proxy**. A continuación, especifique el nombre del host, la dirección IP, el puerto y las credenciales del servidor proxy.

© Acronis International GmbH, 2003-2025

6. Si se le pide, proporcione las credenciales del administrador.
7. Haga clic en **Continuar**.
8. Espere a que se muestre la pantalla de registro.
9. Registre al agente bajo una cuenta de usuario en un inquilino de cliente. Para obtener más información sobre el registro, consulte "Registro de cargas de trabajo utilizando la interfaz gráfica de usuario" (p. 110).
10. [Si ha registrado el agente en un inquilino que utiliza el modo cumplimiento] Establezca la contraseña de cifrado.
11. Si su versión de macOS es Mojave 10.14.x o más reciente, conceda acceso completo al disco al agente de protección para habilitar las operaciones de copia de seguridad.
    Para obtener instrucciones, consulte Otorgar el permiso "Acceso a todo el disco" al agente de ciberprotección (64657).
12. Para utilizar la funcionalidad del escritorio remoto, conceda los permisos de sistema necesarios para el Agente de Connect. Para obtener más información, consulte "Conceder los permisos de sistema necesarios para el Agente de Connect" (p. 58).

Desinstalación de agentes

Al desinstalar un agente desde una carga de trabajo, se elimina automáticamente la carga de trabajo de la consola de Cyber Protect. Si la carga de trabajo se sigue mostrando después de desinstalar el agente, por ejemplo, debido a un problema de red, elimine manualmente esta carga de trabajo de la consola. Para obtener más información sobre cómo hacerlo, consulte "Eliminación de cargas de trabajo de la consola de Cyber Protect" (p. 390).

Nota
Al desinstalar un agente, no se eliminan los planes ni las copias de seguridad.

Pasos para desinstalar un agente

Windows

Nota
[Para planes de protección creados después de noviembre de 2024] La desinstalación y modificación de los agentes de protección para Windows está prohibida de forma predeterminada. El Agente para Windows solo se puede modificar durante una ventana de mantenimiento o a través de la funcionalidad de actualización automática del agente. Para obtener instrucciones sobre cómo habilitar la desinstalación o modificación de un solo uso de un agente, consulte "Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada" (p. 213). Para deshabilitar la protección de desinstalación del agente, consulte "Pasos para deshabilitar la protección de desinstalación del agente" (p. 214).

© Acronis International GmbH, 2003-2025

1. Inicie sesión como administrador en el equipo con el agente.
2. En el **Panel de control** vaya a **Programas y características** (**Añadir o quitar programas** en Windows XP).
3. Haga clic con el botón derecho en **Acronis Cyber Protect** y seleccione **Desinstalar**.
4. [Para agentes protegidos por contraseña] Especifique la contraseña necesaria para desinstalar el agente y haga clic en **Siguiente**.
5. [Opcional] Seleccione la casilla de verificación **Eliminar los registros y las opciones de configuración**.

   Si tiene previsto volver a instalar el agente, deje esta casilla de verificación sin marcar. Si selecciona la casilla de verificación e instala el agente de nuevo, esta carga de trabajo podría duplicarse en la consola de Cyber Protect y sus copias de seguridad antiguas podrían no asociarse a ella.
6. Haga clic en **Desinstalar**.

Linux

1. En el equipo con el agente, ejecute `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` como usuario root.
2. [Opcional] Seleccione la casilla de verificación **Limpiar todos los rastros del producto (Eliminar los registros, tareas, bóvedas y opciones de configuración del producto)**.

   Si tiene previsto volver a instalar el agente, deje esta casilla de verificación sin marcar. Si selecciona la casilla de verificación e instala el agente de nuevo, esta carga de trabajo podría duplicarse en la consola de Cyber Protect y sus copias de seguridad antiguas podrían no asociarse a ella.
3. Confirme su decisión.

macOS

1. En el equipo con el agente, haga doble clic en el archivo de instalación .dmg.
2. Espere hasta que el sistema operativo monte la imagen del disco de instalación.
3. Dentro de la imagen, haga doble clic en **Desinstalar**.
4. Si se le pide, proporcione las credenciales del administrador.
5. Confirme su decisión.

Pasos para desinstalar componentes en paquetes con Agente para Windows

Puede desinstalar componentes individuales en paquetes con Agente para Windows, como Cyber Protect Monitor, Agente para la prevención de pérdida de datos o Bootable Media Builder, sin instalar Agente para Windows.

1. Inicie sesión como administrador en el equipo con el agente.
2. Ejecute el programa de instalación y, a continuación, haga clic en **Modificar componentes instalados**.

© Acronis International GmbH, 2003-2025

3. Desmarque las casillas de verificación junto a los componentes que quiere desinstalar y, a continuación, haga clic en **Listo**.

Pasos para eliminar Agent para VMware (dispositivo virtual)

1. Inicie sesión en vCenter Server mediante vSphere Client.
2. [Si el dispositivo virtual está encendido] Haga clic con el botón derecho en el dispositivo virtual y luego en **Activar** > **Apagar**. Confirme su decisión.
3. [Si el dispositivo virtual utiliza un almacenamiento conectado localmente en un disco virtual, y desea conservar los datos en ese disco] Elimine el almacenamiento virtual del dispositivo virtual.
   a. Haga clic con el botón derecho en el dispositivo virtual y, a continuación, haga clic en **Editar configuración**.
   b. Seleccione el disco con el almacenamiento y después haga clic en **Eliminar**.
   c. En **Opciones de eliminación**, haga clic en **Eliminar del equipo virtual**.
   d. Haga clic en **Aceptar**.

   Como resultado, el disco permanece en el almacén de datos. Puede conectar el disco a otro dispositivo virtual.
4. Haga clic con el botón derecho en el dispositivo virtual y haga clic en **Eliminar del disco**. Confirme su decisión.
5. [Opcional] [Si no planea utilizar este dispositivo de nuevo] En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad** > **Ubicaciones** y, después, elimine la ubicación correspondiente al almacenamiento conectado localmente.

Instalación y desinstalación de agentes de protección utilizando la interfaz de línea de comandos

Instalación y desinstalación de agentes de protección en Windows

En Windows, puede ejecutar una instalación o desinstalación desatendida de las siguientes formas:

- Al utilizar el archivo EXE del programa de instalación y especificar los parámetros de instalación en la línea de comandos.
- Al utilizar un archivo MSI que extraiga del programa de instalación y especificar los parámetros de instalación en una de las siguientes formas:
  - En un archivo MST
  - Directamente en la línea de comandos

Instalación desatendida y desinstalación con un archivo EXE

Para este tipo de instalación desatendida, descargue el programa de instalación y luego inícielo desde la línea de comandos con los parámetros de instalación necesarios. Para ver los parámetros que puede utilizar, consulte "Parámetros para una instalación desatendida (EXE)" (p. 78).

© Acronis International GmbH, 2003-2025

No necesita extraer los paquetes de instalación, los archivos MSI y MST de antemano.

Instalación y desinstalación de agentes y componentes (EXE)

Para llevar a cabo una instalación desatendida con un archivo EXE, ejecute el programa de instalación y especifique los parámetros de instalación en la línea de comandos.

Para descargar el programa de instalación, en la consola de Cyber Protect, haga clic en el icono de la cuenta en la esquina superior derecha y, a continuación, haga clic en **Descargas**. El enlace de descarga también está disponible en el panel **Añadir dispositivos**.

Para instalar agentes y componentes

1. Inicie la interfaz de la línea de comandos como administrador y vaya al archivo EXE del programa de instalación.
2. Para iniciar el programa de instalación y especificar los parámetros de instalación, ejecute el siguiente comando:

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

   Utilice espacios para separar los parámetros y comas sin espacios para separar los valores de un parámetro. Por ejemplo:

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

   Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (EXE)" (p. 78).

Ejemplos

- Instalación del Agente para Windows, Agente para protección antimalware y filtrado de URL, la herramienta de línea de comandos y Cyber Protect Monitor. Registro de la carga de trabajo en el servicio de Cyber Protection con un nombre de usuario y una contraseña.

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

- Instalación del Agente para Windows, la herramienta de línea de comandos y Cyber Protect Monitor. Creación de una cuenta de inicio de sesión nueva para el servicio de agente en Windows. Registro de la carga de trabajo en el servicio de Cyber Protection con un token.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
  ```


© Acronis International GmbH, 2003-2025

```
Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
-reg-token=34F6-8C39-4A5C
```

- Instalación del Agente para Windows, la herramienta de línea de comandos, Agente para Oracle y Cyber Protect Monitor. Registro del equipo en el servicio Cyber Protection empleando un nombre de usuario y una contraseña.

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

- Instalación del Agente para Windows, la herramienta de línea de comandos y Cyber Protect Monitor. Configuración del idioma de la interfaz de usuario al alemán. Registro del equipo en el servicio Cyber Protection empleando un token. Configuración de un proxy HTTP.

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

Para eliminar un componente instalado

1. Inicie la interfaz de línea de comandos como administrador y vaya a `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Ejecute el siguiente comando:

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

   Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (EXE)" (p. 78).

Ejemplo

- Desinstalación del Cyber Protect Monitor.

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

Pasos para desinstalar un agente

1. Inicie la interfaz de línea de comandos como administrador y vaya a `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Ejecute el siguiente comando:

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


© Acronis International GmbH, 2003-2025

Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (EXE)" (p. 78).

Ejemplos

- Desinstalación del Agente para Windows y todos sus componentes. Eliminación de todos los registros, tareas y ajustes de configuración.

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

- Desinstalación de un agente para Windows protegido por contraseña y todos sus componentes. Eliminación de todos los registros, tareas y ajustes de configuración.

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

Parámetros para una instalación desatendida (EXE)

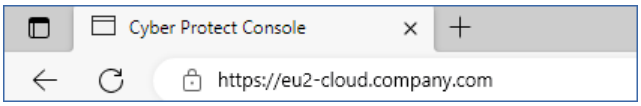
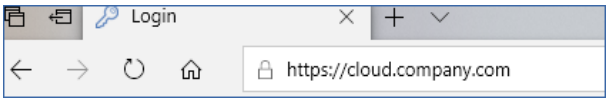
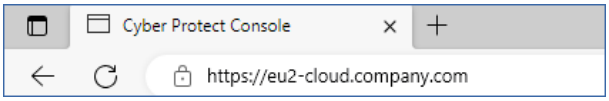
La tabla siguiente resume los parámetros para una instalación desatendida con un archivo EXE.

Parámetros	Descripción
Parámetros generales	
`--add-components=` <component1,component2,...,componentN>	Los componentes que se instalarán. Consulte la lista completa de los componentes disponibles en "Componentes para una instalación desatendida (EXE)" (p. 83). Si especifica varios componentes, sepárelos con comas. No añada espacios antes o después de la coma. Si especifica componentes que ya están instalados, dichos componentes se repararán o actualizarán según la versión del programa de instalación y la de los componentes instalados. Si no especifica este parámetro, se instalará un conjunto de componentes predeterminado, según el equipo en el que se lleve a cabo la instalación. Por ejemplo, Agente para SQL solo se instala en equipos que ejecutan MS SQL Server.
`--install-dir=`<path>	La carpeta en la que se instalarán los componentes seleccionados. Si la carpeta especificada no existe, se creará. Si no especifica este parámetro, se utilizará una carpeta predeterminada: `C:\Program Files\BackupClient`.

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
`--log-dir=`<path>	La carpeta en la que se guardarán los registros de la instalación. Si no especifica este parámetro, se utilizará una carpeta predeterminada: `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<code>	El idioma del producto. Los valores disponibles son los siguientes: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Si no especifica este parámetro y el idioma del sistema del equipo en el que se lleva a cabo la instalación aparece arriba, se utilizará el idioma del sistema. En todos los demás casos, el valor se establece en en.
`--quiet`	Utilice este parámetro para ejecutar el programa de instalación sin mostrar la interfaz gráfica de usuario. No lo utilice junto con el parámetro `--register-only`.
`--help`	Utilice este parámetro para ver una lista de todos los parámetros disponibles que puede utilizar en la línea de comandos y sus descripciones.
`--fss-onboarding-auto-start`	Utilice este parámetro junto con el parámetro `--quiet` para mostrar el asistente de incorporación de File Sync & Share después de una instalación desatendida.
`--fips={enabled | disabled}`	Use este parámetro con el valor `enabled` para instalar el agente en el modo compatible con FIPS.
Parámetros de registro	
`--registration={skip | by-credentials | by-token | device-flow}`	Utilice este parámetro para elegir cómo se registrará el agente cuando finalice la instalación. Para omitir el registro, especifique `skip`. Puede registrar el agente más adelante mediante el parámetro `--register-only`. Para registrar el agente con credenciales, especifique `by-credentials` y utilice los parámetros `--reg-login` y `--reg-password`. Asimismo, solo puede utilizar los parámetros `--reg-login` y `--reg-password`, lo cual hace que especificar `--registration=by-credentials` sea opcional. Para registrar el agente con un token de registro, especifique `by-token` y utilice el parámetro `--reg-token`.

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
	Asimismo, solo puede utilizar el parámetro `--reg-token`, lo cual hace que especificar `--registration=by-token` sea opcional. Para registrar el agente mediante el protocolo OAuth 2.0, especifique `device-flow`. Cuando haya terminado la instalación, la página de registro se abrirá automáticamente. Cuando use `--registration=device-flow`, especifique la dirección exacta del centro de datos como un valor para el parámetro `--reg-address`. Esta es la URL que ve **al iniciar sesión en el** servicio de Cyber Protection. Por ejemplo, `https://eu2-cloud.company.com`.  No use `--registration=device-flow` con el parámetro `--quiet`.
`--reg-address=`<url>	URL del servicio Cyber Protection. Puede usar este parámetro junto con los parámetros `--reg-login` y `--reg-password`, o bien junto con el parámetro `--reg-token`. • Cuando lo use con los parámetros `--reg-login` y `--reg-password`, especifique la dirección que usa **para iniciar sesión en** el servicio de Cyber Protection. Por ejemplo, `https://cloud.company.com`:  • Cuando lo use con el parámetro `--reg-token`, especifique la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión en el** servicio de Cyber Protection. Por ejemplo, `https://eu2-cloud.company.com`.  No utilice `https://cloud.company.com` con el parámetro `--reg-token`.
`--reg-login=`<login> `--reg-password=`<password>	Las credenciales para la cuenta con la que se registrará el agente en el servicio de Cyber Protection. No puede ser una cuenta de administrador de partners. Cuando use estos parámetros, especificar el parámetro `--registration` es opcional.

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
	No utilice estos parámetros con el parámetro `--reg-token`.
`--reg-token=`<token>	El token de registro. El token de registro es una serie de 12 caracteres, agrupados en tres segmentos que se separan por guiones. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112). Cuando use este parámetro, especificar el parámetro `--registration` es opcional. Puede usar este parámetro con los parámetros `--reg-login` y `--reg-password`.
`--register-only`	Utilice este parámetro para omitir la instalación y registrar el agente mediante el protocolo OAuth 2.0 (device-flow). Cuando haya terminado la instalación, la página de registro se abrirá automáticamente. No use `--register-only` con el parámetro `--quiet`.
Cuenta de inicio de sesión para el servicio de agente	
`--agent-account={system | new | custom}` o `--agent-account-login=`<login> `--agent-account-password=`<password>	Use este parámetro para especificar la cuenta de inicio de sesión en la que se ejecutará el servicio de agente. Para obtener más información sobre las cuentas de inicio de sesión, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 67). Para utilizar la cuenta **Sistema local**, especifique `--agent-account=system` o no utilice el parámetro `--agent-account` en su comando. Para que el servicio del agente se ejecute en una nueva cuenta de inicio de sesión, **Acronis Agent User**, que se crea automáticamente, especifique `new`. Para hacer que el servicio del agente se ejecute en una cuenta existente, especifique las credenciales de la cuenta mediante los parámetros `--agent-account-login` y `--agent-account-password`. En este caso, especificar el parámetro `--agent-account=custom` es opcional.
Parámetros de vCenter/ESXi	
`--esxi-address=`<host>	El nombre del host o la dirección IP del vCenter Server o

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
	host ESXi. Utilice este parámetro al instalar Agente para VMware.
`--esxi-login=`<login> `--esxi-password=`<password>	Las credenciales de acceso al vCenter Server o al host ESXi. Utilice estos parámetros al instalar Agente para VMware.
Parámetros del proxy	
`--http-proxy={none | system | custom}`	Utilice este parámetro para especificar el servidor proxy HTTP que desea utilizar para la copia de seguridad y la recuperación del almacenamiento en la nube. Si deshabilita las conexiones del servidor proxy, especifique `--http-proxy=none`. Para usar un servidor proxy en todo el sistema, especifique `--http-proxy=system` o no utilice el parámetro `--http-proxy` en el comando. Para usar otro servidor proxy, especifique la dirección del servidor proxy y las credenciales mediante los parámetros `--http-proxy-address`, `--http-proxy-login` y `--http-proxy-password`. En este caso, especificar el parámetro `--http-proxy=custom` es opcional.
`--http-proxy-address=`<host>:<port>	El nombre y la dirección IP del host y el puerto del servidor proxy HTTP personalizado.
`--http-proxy-login=`<login>	Inicio de sesión del servidor proxy HTTP personalizado.
`--http-proxy-password=`<password>	Contraseña del servidor proxy HTTP personalizado.
Parámetros de desinstalación	
`--remove-components=`<component1,component2,...,componentN>	Los componentes que se desinstalarán. Consulte la lista completa de los componentes disponibles en "Componentes para una instalación desatendida (EXE)" (p. 83). Si especifica varios componentes, sepárelos con comas. No añada espacios antes o después de la coma. **Importante** Al utilizar este parámetro, solo puede desinstalar componentes. Para desinstalar el producto completamente, vaya a Panel de Control de Windows > Programas y características, seleccione el producto y haga clic en **Desinstalar**.

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
`--delete-all-settings`	Utilice este parámetro opcional cuando utilice el parámetro `--remove-components` para eliminar todos los registros de productos, tareas y ajustes de configuración.
`--anti-tamper-password=`<password>	La contraseña requerida para desinstalar o modificar los componentes de un agente para Windows protegido por contraseña.

Componentes para una instalación desatendida (EXE)

La siguiente tabla resume los componentes que puede usar para la instalación desatendida mediante un archivo EXE. Utilice los nombres del valor para especificar los valores del parámetro `--add-components`.

Para obtener más información, consulte "Parámetros para una instalación desatendida (EXE)" (p. 78).

Nombre del valor	Descripción de componentes
`agentForWindows`	Agente para Windows
`agentForSas`	Agente para File Sync & Share
`agentForAd`	Agente para Active Directory
`agentForAmp`	Agente para protección antimalware y filtrado de URL
`agentForDlp`	Agente para la prevención de la pérdida de datos
`agentForEsx`	Agente para VMware (Windows)
`agentForExchange`	Agente para Exchange
`agentForHyperV`	Agente para Hyper-V
`agentForOffice365`	Agente para Office 365
`agentForOracle`	Agente para Oracle
`agentForSql`	Agente para SQL
`commandLine`	Herramienta de línea de comandos
`mediaBuilder`	Bootable Media Builder
`trayMonitor`	Cyber Protect Monitor
`all`	Este valor combina todos los componentes.
`allAgents`	Este valor combina todos los agentes.

© Acronis International GmbH, 2003-2025

Instalación desatendida y desinstalación con un archivo MSI

Para este tipo de instalación desatendida, utilice el instalador de Windows (el programa `Msiexec`). Extraiga los paquetes de instalación y el archivo MSI de antemano. Para ello, utilice la interfaz gráfica de usuario del programa de instalación.

Cuando instale componentes con un archivo MSI, puede usar un archivo de transformación MST para personalizar los parámetros de instalación. Para obtener más información sobre cómo usar la combinación de archivos MSI y MST, consulte "Instalación de agentes y componentes (combinación de MSI y MST)" (p. 85). Puede utilizar este método de instalación en un dominio de Active Directory para instalar agentes de protección mediante la directiva de grupo de Windows. Para obtener más información, consulte "Despliegue de agentes de protección a través de la directiva de grupo" (p. 134).

Como alternativa, puede especificar los parámetros de instalación manualmente en la línea de comandos. En este caso, no necesita un archivo MST. Para obtener más información, consulte "Ejemplos" (p. 86).

Extracción de archivos MSI, MST y CAB

Extraiga los archivos MSI, MST y CAB con los paquetes de instalación. Para ello, ejecute la interfaz gráfica de usuario del programa de instalación.

Pasos para extraer archivos MSI, MST y CAB

1. Ejecute la interfaz gráfica de usuario del programa de instalación y, a continuación, haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión**.
2. En **Qué instalar**, seleccione los componentes que desea instalar y haga clic en **Listo**.

   Nota
   Cuando modifique una instalación existente, seleccione los componentes que ya están instalados y los componentes que desee añadir.

   Los paquetes de instalación de estos componentes se extraerán del programa de instalación como archivos CAB.
3. En **Ajustes de registro**, seleccione **Usar credenciales** o **Usar token de registro**. Según lo que elija, especifique las credenciales o el token de registro y haga clic en **Listo**.

   Para obtener más información sobre cómo generar un token de registro, consulte "Generar un token de registro" (p. 112).
4. [Solamente cuando instale en un controlador de dominio] En **Cuenta de inicio de sesión para el servicio de agente**, seleccione **Utilice la siguiente cuenta**. Especifique la cuenta de usuario en la que se ejecutará el servicio de agente. Después, haga clic en **Listo**. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

© Acronis International GmbH, 2003-2025

Nota
A la cuenta de usuario que especifique se le debe conceder el privilegio `Iniciar sesión como un servicio`. Esta cuenta ya debe haberse usado en el controlador de dominio para que se cree su carpeta de perfiles en dicho equipo.

Para obtener más información sobre la instalación del agente en un controlador de dominio de solo lectura, consulte este artículo de la base de conocimientos.

5. Revise o modifique otros ajustes de la instalación que se añadirá al archivo MST y haga clic en **Continuar**.
6. Seleccione la carpeta en la que se extraerán los archivos MSI, MST y CAB y haga clic en **Generar**.

Instalación de agentes y componentes (combinación de MSI y MST)

Utilice el archivo MST para personalizar la configuración de la instalación del archivo MSI. Utilice la combinación de MSI y MST al instalar agentes en varios equipos a través de la directiva de grupo de Windows. Para obtener más información, consulte "Despliegue de agentes de protección a través de la directiva de grupo" (p. 134).

Pasos para instalar componentes con archivos MSI y MST

1. Extraiga los archivos MSI y MST como se describe en "Extracción de archivos MSI, MST y CAB" (p. 84).
2. En la interfaz de la línea de comandos del equipo en el que desea instalar los componentes, ejecute el siguiente comando:

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

Por ejemplo:

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

Instalación y desinstalación de agentes y componentes (MSI y selección directa)

Ejecute el archivo MSI, seleccione manualmente los componentes a instalar y especifique sus parámetros de instalación en la línea de comandos. En este caso, no necesita el archivo MST.

Para instalar agentes y componentes

1. Extraiga el archivo MSI y los paquetes de instalación (archivos CAB) como se describe en "Extracción de archivos MSI, MST y CAB" (p. 84).

   Para este método de instalación, solo necesita los archivos MSI y CAB. No necesita el archivo MST.
2. En la interfaz de línea de comandos del equipo, ejecute el siguiente comando:

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


© Acronis International GmbH, 2003-2025

Utilice espacios para separar los parámetros y comas sin espacios para separar los valores de un parámetro. Por ejemplo:

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

Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (MSI)" (p. 88).

Ejemplos

- Instalación del Agente para Windows, Agente para antimalware y filtrado de URL, la herramienta de línea de comandos y Cyber Protect Monitor. Registro de la carga de trabajo en el servicio de Cyber Protection con un nombre de usuario y una contraseña.

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

- Instalación del Agente para Windows, la herramienta de línea de comandos y Cyber Protect Monitor. Creación de una cuenta de inicio de sesión nueva para el servicio de agente en Windows. Registro de la carga de trabajo en el servicio de Cyber Protection con un token.

  ```
  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
  ```

- Instalación del Agente para Windows, la herramienta de línea de comandos, Agente para Oracle y Cyber Protect Monitor. Registro del equipo en el servicio Cyber Protection empleando un nombre de usuario y una contraseña codificada base64. Puede que necesite cifrar su contraseña si contiene caracteres especiales o espacios en blanco. Consulte "Uso de contraseñas con caracteres especiales o espacios en blanco" (p. 116) para obtener más información sobre cómo cifrar una contraseña.

  ```
  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==
  ```

- Instalación del Agente para Windows, la herramienta de línea de comandos y Cyber Protect Monitor. Registro del equipo en el servicio Cyber Protection empleando un token. Configuración de un proxy HTTP.

© Acronis International GmbH, 2003-2025

```
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
```

Para eliminar un componente instalado

1. Extraiga el archivo MSI y los paquetes de instalación (archivos CAB) como se describe en "Extracción de archivos MSI, MST y CAB" (p. 84).

   Para este método de instalación, solo necesita los archivos MSI y CAB. No necesita el archivo MST.
2. En la interfaz de línea de comandos del equipo, ejecute el siguiente comando:

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

   Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (MSI)" (p. 88).

Ejemplo

- Eliminación del monitor Cyber Protect.

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

Pasos para desinstalar un agente

1. Extraiga el archivo MSI y los paquetes de instalación (archivos CAB) como se describe en "Extracción de archivos MSI, MST y CAB" (p. 84).

   Para este método de instalación, solo necesita los archivos MSI y CAB. No necesita el archivo MST.
2. En la interfaz de línea de comandos del equipo, ejecute el siguiente comando:

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

   Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (MSI)" (p. 88).

Ejemplos

- Desinstalación del Agente para Windows y todos sus componentes. Eliminación de todos los registros, tareas y ajustes de configuración.

© Acronis International GmbH, 2003-2025

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

- Desinstalación de un agente para Windows protegido por contraseña y todos sus componentes. Eliminación de todos los registros, tareas y ajustes de configuración.

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

Parámetros para una instalación desatendida (MSI)

La tabla siguiente resume los parámetros para una instalación desatendida cuando utiliza un archivo MSI.

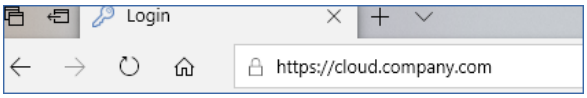
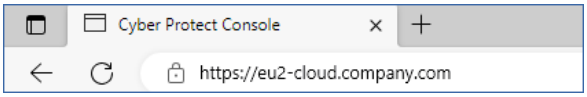
También puede utilizar otros parámetros `msiexec`. Por ejemplo, utilice `/qn` para evitar que se muestren los elementos de interfaz. Para obtener más información sobre los parámetros `msiexec`, consulte la documentación acerca de Microsoft.

Parámetros	Descripción
Parámetros generales	
`ADDLOCAL=` <component1,component2,...,componentN>	Los componentes que se instalarán. Consulte la lista completa de los componentes disponibles en "Componentes para una instalación desatendida (MSI)" (p. 92). Si especifica varios componentes, sepárelos con comas. No añada espacios antes o después de la coma. **Nota** Debe extraer los archivos de instalación para todos los componentes que desea instalar. Para obtener más información sobre cómo extraerlos, consulte "Extracción de archivos MSI, MST y CAB" (p. 84).
`TARGETDIR=`<path>	La carpeta en la que se instalarán los componentes seleccionados. Si la carpeta especificada no existe, se creará. Si no especifica este parámetro, se utilizará una carpeta predeterminada: `C:\Program Files\BackupClient`.
`REBOOT=ReallySuppress`	Especifique este parámetro si desea instalar componentes sin reiniciar el equipo.
`/l*v` <log file>	Especifique este parámetro para guardar un registro detallado. Este registro es necesario si tiene que

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
	investigar problemas de instalación.
CURRENT_LANGUAGE=<language ID>	El idioma del producto. Los valores disponibles son los siguientes: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Si no especifica este parámetro y el idioma del sistema del equipo en el que se lleva a cabo la instalación aparece arriba, se utilizará el idioma del sistema. En todos los demás casos, el valor se establece en en.
SKIP_SHA2_KB_CHECK={0,1}	Use este parámetro para comprobar o para omitir la verificación de la instalación de la actualización de Microsoft para el soporte de firma de código SHA2 (KB4474419) en un equipo. La verificación solo se ejecuta en sistemas operativos que requieren esta actualización. Para ver si es necesario para su sistema operativo, consulte "Sistemas operativos y entornos compatibles para la copia de seguridad y la recuperación" (p. 499). Para omitir la verificación, establezca el valor del parámetro en 1. Si no especifica el parámetro o establece su valor a 0 y la actualización de soporte de firma de código SHA2 no se encuentra en el equipo, la instalación falla.
FSS_ONBOARDING_AUTO_START={0,1}	Utilice este parámetro con el valor establecido 1 para mostrar el asistente de incorporación de File Sync & Share después de una instalación desatendida. Si no especifica este parámetro o establece su valor en 0, no se mostrará el asistente de incorporación.
ENABLE_FIPS_COMPLIANCE_MODE={0,1}	Use este parámetro con el valor establecido en 1 para instalar el agente en el modo compatible con FIPS.
Parámetros de registro	
REGISTRATION_ADDRESS	URL del servicio Cyber Protection. Puede usar este parámetro con los parámetros REGISTRATION_LOGIN y REGISTRATION_PASSWORD o bien con REGISTRATION_TOKEN. • Cuando lo use con los parámetros REGISTRATION_LOGIN y REGISTRATION_PASSWORD, especifique la dirección que usa **para iniciar sesión** en el servicio de Cyber Protection. Por ejemplo,

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
	`https://cloud.company.com`:  • Cuando lo use con el parámetro `REGISTRATION_TOKEN`, especifique la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión en el** servicio de Cyber Protection. Por ejemplo, `https://eu2-cloud.company.com`.  No utilice `https://cloud.company.com` con el parámetro `REGISTRATION_TOKEN`.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	Las credenciales para la cuenta con la que se registrará el agente en el servicio de Cyber Protection. No puede ser una cuenta de administrador de partners.
	
	No utilice estos parámetros con el parámetro `REGISTRATION_TOKEN`.

`REGISTRATION_PASSWORD_ENCODED`	La contraseña para la cuenta con la que se registrará el agente en el servicio Cyber Protection, codificada como base64. Para obtener más información sobre cómo codificar su contraseña, consulte "Uso de contraseñas con caracteres especiales o espacios en blanco" (p. 116).
`REGISTRATION_TOKEN`	El token de registro. El token de registro es una serie de 12 caracteres, agrupados en tres segmentos que se separan por guiones. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112). No utilice este parámetro con los parámetros `REGISTRATION_LOGIN` y `REGISTRATION_PASSWORD`.
`REGISTRATION_REQUIRED={0,1}`	Utilice este parámetro para elegir qué ocurre si el registro falla. Si establece el valor en `1`, la instalación también falla. Si establece el valor en `0` o no especifica el parámetro, la instalación se completa correctamente, aunque el registro falle.

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
Cuenta de inicio de sesión para el servicio de agente	
MMS_USE_SYSTEM_ACCOUNT={0,1}	Utilice este parámetro con el valor 1 para ejecutar el servicio con la cuenta de inicio de sesión **Sistema local**. Para obtener más información sobre las cuentas de inicio de sesión, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 67).
MMS_CREATE_NEW_ACCOUNT={0,1}	Utilice este parámetro con el valor 1 para que el servicio del agente se ejecute en una nueva cuenta de inicio de sesión, **Acronis Agent User**, que se crea automáticamente.
MMS_SERVICE_USERNAME=<user name> MMS_SERVICE_PASSWORD=<password>	Use estos parámetros para especificar una cuenta de inicio de sesión existente en la que se ejecutará el servicio de agente.
Parámetros de vCenter/ESXi	
SET_ESX_SERVER={0,1}	Utilice este parámetro al instalar Agente para VMware. Si establece el valor en 0, el Agent for VMware no se conectará al vCenter Server ni al servidor ESXi. Si establece el valor en 1, especifique los siguientes parámetros: ESX_HOST, EXI_USER, ESX_PASSWORD.
ESX_HOST=<host name>	El nombre del host o la dirección IP del vCenter Server o host ESXi.
ESX_USER=<user name> ESX_PASSWORD=<password>	Las credenciales de acceso al vCenter Server o al host ESXi.
Parámetros del proxy	
HTTP_PROXY_ADDRESS=<IP address> HTTP_PROXY_PORT=<port>	Use estos parámetros para especificar el servidor proxy HTTP en el que se usará el agente. Si no utiliza un servidor proxy, no especifique estos parámetros.
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	Credenciales del servidor proxy HTTP. Utilice estos parámetros si el servidor proxy necesita autenticación.
Parámetros de desinstalación	
REMOVE=	Los componentes que se desinstalarán.

© Acronis International GmbH, 2003-2025

Parámetros	Descripción
{<component1,component2,...,componentN>|ALL}	Si especifica varios componentes, sepárelos con comas. No añada espacios antes o después de la coma. Para eliminar todos los componentes de producto, establezca el valor ALL.
DELETE_ALL_SETTINGS={0,1}	Para eliminar todos los registros de productos, tareas y ajustes de configuración, establezca el valor en 1. Utilice este parámetro opcional cuando utilice el parámetro REMOVE.
ANTI_TAMPER_PASSWORD=<password>	La contraseña requerida para desinstalar o modificar los componentes de un agente para Windows protegido por contraseña.

Componentes para una instalación desatendida (MSI)

La siguiente tabla resume los componentes que puede usar para la instalación desatendida mediante un archivo MSI. Utilice los nombres del valor para especificar los valores del parámetro ADDLOCAL.

Para obtener más información, consulte "Parámetros para una instalación desatendida (MSI)" (p. 88).

Nombre del valor	Descripción de componentes	Debe instalarse junto con	Número de bits
AgentFeature	Componentes fundamentales de los agentes		32 bits / 64 bits
MmsMspComponents	Componentes principales para copia de seguridad	AgentFeature	32 bits / 64 bits
BackupAndRecoveryAgent	Agente para Windows	MmsMspComponents	32 bits / 64 bits
AmpAgentFeature	Agent for Antimalware protection and URL filtering	BackupAndRecoveryAgent	32 bits / 64 bits
DlpAgentFeature	Agente para la prevención de la pérdida de datos	BackupAndRecoveryAgent	32 bits / 64 bits

© Acronis International GmbH, 2003-2025

SasAgentFeature	Agente para File Sync & Share	TrayMonitor	32 bits / 64 bits
ArxAgentFeature	Agente para Exchange	MmsMspComponents	32 bits / 64 bits
ArsAgentFeature	Agente para SQL	BackupAndRecoveryAgent	32 bits / 64 bits
ARADAgentFeature	Agente para Active Directory	BackupAndRecoveryAgent	32 bits / 64 bits
ArxOnlineAgentFeature	Agente para Microsoft 365	MmsMspComponents	32 bits / 64 bits
OracleAgentFeature	Agente para Oracle	BackupAndRecoveryAgent	32 bits / 64 bits
AcronisESXSupport	Agente para VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64 bits
HyperVAgent	Agente para Hyper-V	BackupAndRecoveryAgent	32 bits / 64 bits
CommandLineTool	Herramienta de línea de comandos		32 bits / 64 bits
TrayMonitor	Cyber Protect Monitor	AgentFeature	32 bits / 64 bits
BackupAndRecoveryBootableComponents	Bootable Media Builder		32 bits / 64 bits

Instalación y desinstalación de agentes de protección en Linux

En esta sección se describe cómo instalar o desinstalar los agentes de protección en el modo de interacción en un equipo que ejecute Linux mediante una línea de comando.

Requisitos previos

- Ha descargado el archivo de instalación para el Agente para Linux. Consulte "Descarga de agentes de protección" (p. 49).

  El paquete de instalación de 64 bits contiene agentes adicionales, como Agente para Virtuozzo, Agente para Oracle, Agente para MySQL/MariaDB y Agente para Proxmox. Estos agentes dependen del Agente para Linux y se instalan junto con él.
- Ha instalado los paquetes de Linux necesarios.
- En el equipo en el que desee instalar el agente, debe haber al menos 2 GB de espacio libre en el disco.

© Acronis International GmbH, 2003-2025

- Cuando instale el agente en SUSE Linux, asegúrese de usar `su -` en lugar de `sudo`. De lo contrario, se producirá el siguiente error al intentar registrar el agente a través de la consola de Cyber Protect: "Error al iniciar el navegador web. No hay ninguna pantalla disponible". Algunas distribuciones de Linux, como SUSE, no pasan la variable DISPLAY al usar `sudo` y el programa de instalación no puede abrir el navegador en la interfaz gráfica de usuario (GUI).

Limitaciones

- Algunas distribuciones de Linux no permiten la instalación de paquetes firmados con SHA-1. En tales casos, la instalación falla con el siguiente mensaje: "No se puede encontrar el paquete Agente de copia de seguridad y recuperación". Para obtener más información sobre cómo resolver este problema, consulte este artículo de la base de conocimiento.

Cómo instalar un agente

1. Abra el Terminal.
2. Realice uno de los siguientes procedimientos:
   - Para iniciar la instalación especificando los parámetros de la línea de comando, ejecute el siguiente comando:

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

     Aquí, `<package name>` es el nombre del paquete de instalación (32 bits o 64 bits). Consulte los parámetros disponibles y sus valores se describen en "Parámetros de instalación o desinstalación sin supervisión" (p. 95).
   - Para iniciar la instalación con los parámetros que se especifican en un archivo de texto independiente, ejecute el siguiente comando:

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

     Este enfoque puede ser útil si no desea introducir información confidencial en la línea de comandos. En este caso, puede especificar los parámetros de configuración en un archivo de texto independiente y asegurarse de que solo usted pueda acceder al mismo. Coloque cada parámetro en una nueva línea, seguido del valor correspondiente para cada parámetro. Por ejemplo:

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

     o

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


© Acronis International GmbH, 2003-2025

```
-a
--language
en
```

Si se especifica el mismo parámetro tanto en la línea de comando como en el archivo de texto, precede el valor de la línea de comando.

3. Si el arranque UEFI seguro está habilitado en el equipo, se le pedirá que reinicie el sistema después de la instalación. Cuando se le pida una contraseña, use la contraseña para el usuario root. Si esta contraseña no es aceptada, use la palabra "acronis" como contraseña. Durante el reinicio del sistema, elija la gestión de MOK (clave del propietario del equipo), seleccione **Registrar MOK** y, a continuación, registre la clave usando la contraseña recomendada.
   Si habilita el arranque seguro UEFI después de instalar el agente, repita la instalación, incluido este paso. En caso contrario, las copias de seguridad fallarán.

Pasos para desinstalar un agente

1. Abra el Terminal.
2. Realice uno de los siguientes procedimientos:
   - Para desinstalar el agente y eliminar todos los registros, tareas y ajustes de configuración, ejecute el siguiente comando:

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

   - Para desinstalar el agente pero mantener su ID (por ejemplo, si planea instalar el agente más tarde), ejecute el siguiente comando:

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

   - Para desinstalar el agente mediante el archivo de instalación, ejecute el siguiente comando:

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

     Aquí, `<package name>` es el nombre del paquete de instalación (32 bits o 64 bits). Consulte los parámetros disponibles y sus valores se describen en "Parámetros de instalación o desinstalación sin supervisión" (p. 95).

     Nota
     Utilice este comando solo cuando el paquete de instalación sea de la misma versión que el agente instalado y si `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` está dañado o es inaccesible.

Parámetros de instalación o desinstalación sin supervisión

Esta sección describe parámetros que se utilizan en una instalación o desinstalación sin supervisión en Linux.

© Acronis International GmbH, 2003-2025

La configuración mínima para una instalación de interacción incluye `-a` y parámetros de registro (por ejemplo, los parámetros `--login` y `--password`; `--rain` y `--token`). Puede usar más parámetros para personalizar su instalación.

Parámetros de instalación

Parámetros básicos

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

Los componentes que se van a instalar, separados con comas y sin espacios. Los siguientes componentes están disponibles para el paquete de instalación de 64 bits (x86_64):

Componente	Descripción de componentes
`BackupAndRecoveryAgent`	Agente para Linux
`AgentForPCS`	Agente para Virtuozzo
`OracleAgentFeature`	Agente para Oracle
`MySQLAgentFeature`	Agente para MySQL/MariaDB
`AgentForProxmox`	Agente para Proxmox

Sin este parámetro, se instalarán todos los componentes anteriores.

El Agente para Virtuozzo, Agente para Oracle, Agente para MySQL/MariaDB y Agente para Proxmox requieren que el Agente para Linux también esté instalado.

El paquete de instalación de 32 bits contiene únicamente BackupAndRecoveryAgent.

`{-a|--auto}`

El proceso de instalación y registro se completará sin que el usuario tenga que llevar a cabo ninguna otra acción. Cuando use este parámetro, debe especificar la cuenta en la que se registrará el agente en el servicio Cyber Protection, ya sea mediante el parámetro `--token` o los parámetros `--login` y `--password`.

`{-t|--strict}`

Si se especifica el parámetro, cualquier advertencia que ocurra durante la instalación dará como resultado un error de instalación. Sin este parámetro, la instalación finaliza correctamente aunque haya advertencias.

`{-n|--nodeps}`

Se omitirá la ausencia de paquetes de Linux requeridos durante la instalación.

`{-d|--debug}`

Escribe el registro de instalación en modo detallado.

`--options-file=<location>`

© Acronis International GmbH, 2003-2025

Los parámetros de instalación se leerán de un archivo de texto, en lugar de la línea de comando.

`--language=<language ID>`

El idioma del producto. Los valores disponibles son los siguientes: `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, vi, zh, zh_TW`.
Si no se especifica este parámetro, el idioma del producto estará definido por el idioma de su sistema siempre que esté en la lista anterior. De lo contrario, el idioma del producto establecido será el inglés (`en`).

Parámetros de registro

Especifique alguno de los parámetros siguientes:

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

  Credenciales para la cuenta con la que se registrará el agente en el servicio Cyber Protection. No puede ser una cuenta de administrador de partners.

- `--token=<token>`

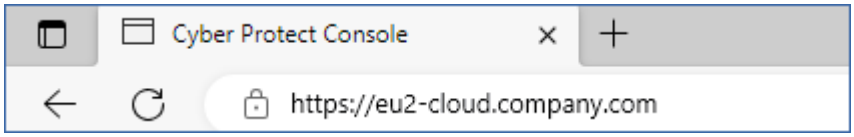
  El token de registro es una serie de 12 caracteres separados en tres segmentos por guiones. Para obtener más información, consulte "Generar un token de registro" (p. 112).

  Nota
  Cuando utilice el parámetro `--token`, también debe incluir el parámetro `{-C|--rain=}` y especificar la dirección exacta del centro de datos.
  No puede usar el parámetro `--token` junto con los parámetros `--login`, `--password` y `--register-with-credentials`.

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

    URL del servicio Cyber Protection.

    Debe utilizar el parámetro `{-C|--rain=}` y especificar la dirección exacta del centro de datos cuando utilice el parámetro `--token`. La dirección exacta del centro de datos es la URL que ve **después de iniciar sesión en** la consola de Cyber Protection. Por ejemplo:

    Puede omitir el parámetro `{-C|--rain=}` cuando utilice los parámetros `--login` y `--password` para el registro, ya que el programa de instalación utiliza la dirección correcta de forma predeterminada.

- `--register-with-credentials`

  Si se especifica este parámetro, se iniciará la interfaz gráfica del programa de instalación. Para finalizar el registro, introduzca el nombre de usuario y la contraseña de la cuenta con la que se

© Acronis International GmbH, 2003-2025

registrará el agente en el servicio Cyber Protection. No puede ser una cuenta de administrador de partners.

- `--skip-registration`

  Utilice este parámetro si desea instalar el agente pero tiene pensado registrarlo en el servicio Cyber Protection más tarde. Para obtener más información sobre cómo hacerlo, consulte "Registro y anulación de registro de cargas de trabajo utilizando la interfaz de línea de comandos" (p. 115).

Parámetros adicionales

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

El servidor proxy HTTP que el agente usará para realizar la copia de seguridad y la recuperación desde la nube y para establecer la conexión al servidor de gestión. Sin estos parámetros, no se utilizará ningún servidor proxy.

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

Credenciales del servidor proxy HTTP. Utilice estos parámetros si el servidor necesita autenticación.

`--tmp-dir=<location>`

Especifique la carpeta en la que se guardan los archivos temporales durante la instalación. La carpeta predeterminada es **/var/tmp**.

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

Durante la instalación, se utilizarán bibliotecas redistribuibles, a pesar de que es posible que ya se encuentran en su sistema.

`--skip-prereq-check`

No se comprobará si ya están instalados los paquetes necesarios para la compilación del módulo "snapapi".

`--force-weak-snapapi`

El programa de instalación no compilará ningún módulo "snapapi". En su lugar, usará un módulo preparado que es posible que no coincida exactamente con el kernel Linux. No le recomendamos utilizar esta opción.

`--skip-svc-start`

Los servicios no se iniciarán automáticamente después de la instalación. Este parámetro se utiliza con `--skip-registration` en más ocasiones.

Parámetros de información

`{-?|--help}`

Muestra descripción de los parámetros.

© Acronis International GmbH, 2003-2025

`--usage`

Muestra una breve descripción del uso del comando.

`{-v|--version}`

Muestra la versión del paquete de instalación.

`--product-info`

Muestra el nombre del producto y la versión del paquete de instalación.

`--snapapi-list`

Muestra los módulos "snapapi" preparados disponibles.

`--components-list`

Muestra los componentes del programa de instalación.

Parámetros para funciones heredadas

Estos parámetros están relacionados con un componente heredado, agent.exe.

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

Especifica la ruta al archivo de un certificado para establecer una comunicación SSL.

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

Especifica el puerto en el que agent.exe escucha para conexiones. El puerto predeterminado es 9876.

Parámetros de desinstalación

`{-u|--uninstall}`

Desinstala el producto.

`--purge`

Desinstala el producto y elimina los registros, tareas y ajustes de configuración. No es necesario que especifique el parámetro `--uninstall` de manera explícita cuando use `--purge`.

Ejemplos

- Instalación del Agente para Linux sin registrarlo.

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

- Instalación del Agente para Linux, Agente para Virtuozzo y Agent for Oracle, y su correspondiente registro mediante credenciales.

© Acronis International GmbH, 2003-2025

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

- Instalación de Agent for Oracle y Agente para Linux, y su correspondiente registro mediante un token de registro.

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

- Instalación del Agente para Linux, Agente para Virtuozzo y Agent for Oracle con ajustes de configuración en un archivo de texto independiente.

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

- Desinstalación del Agente para Linux, Agente para Virtuozzo y Agente para Oracle y eliminación de todos sus registros, tareas y ajustes de configuración.

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

Instalación y desinstalación de agentes de protección en macOS

En esta sección se describe cómo instalar y desinstalar el agente de protección en el modo sin interacción en un equipo que ejecute macOS mediante una línea de comando.

Permisos obligatorios

Antes de iniciar una instalación desatendida en una carga de trabajo de Mac, debe modificar el Control de políticas de preferencias de privacidad para permitir tanto el acceso a la app como las extensiones del sistema y del kernel en el sistema operativo macOS de la carga de trabajo con el fin de llevar a cabo la instalación del agente de Cyber Protection. Consulte "Permisos obligatorios para la instalación sin supervisión en macOS" (p. 102).

Después de implementar la carga útil de PPPC, puede continuar con los procedimientos siguientes.

Pasos para descargar el archivo de instalación (.dmg)

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar** y luego en **Mac**.

Cómo instalar un agente

1. Abra el Terminal.
2. Cree un directorio temporal para montar el archivo de instalación (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Aquí, `<dmg_root>` es un nombre de su elección.

© Acronis International GmbH, 2003-2025

3. Monte el archivo .dmg.

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

Aquí, `<dmg_file>` es el nombre del archivo de instalación. Por ejemplo, **Cyber_Protection_Agent_for_MAC_x64.dmg**.

4. Ejecute el programa de instalación.
   - Si utiliza un programa de instalación completo para Mac, como `CyberProtect_AgentForMac_x64.dmg` o `CyberProtect_AgentForMac_arm64.dmg`, ejecute el siguiente comando.

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

     Nota
     Si necesita habilitar la incorporación automática para File Sync & Share, en su lugar, ejecute el siguiente comando. Esta opción le pedirá la contraseña del administrador.

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

   - Si utiliza un programa de instalación universal para Mac, como `CyberProtect_AgentForMac_web.dmg`, ejecute el siguiente comando.

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```

5. Desconecte el archivo de instalación (.dmg).

```
hdiutil detach <dmg_root>
```

Ejemplo

```
mkdir mydirectory
```

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

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

```
hdiutil detach mydirectory
```

Pasos para desinstalar un agente

© Acronis International GmbH, 2003-2025

1. Abra el Terminal.
2. Realice uno de los siguientes procedimientos:
   - Para desinstalar el agente, ejecute el siguiente comando:

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

   - Para desinstalar el agente y eliminar todos los registros, tareas y ajustes de configuración, ejecute el siguiente comando:

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

Permisos obligatorios para la instalación sin supervisión en macOS

Antes de iniciar una instalación desatendida en una carga de trabajo de Mac, debe modificar el Control de políticas de preferencias de privacidad para permitir tanto el acceso a la app como las extensiones del sistema y del kernel en el sistema operativo macOS de la carga de trabajo con el fin de llevar a cabo la instalación del agente de Cyber Protection. Puede hacerlo implementando una carga útil de PPPC personalizada o configurando las preferencias en la interfaz gráfica de usuario de la carga de trabajo. Las siguientes tablas enumeran los permisos necesarios.

Consulte también "Solución de problemas de permisos en macOS" (p. 109).

Requisitos para macOS 11 (Big Sur) y versiones posteriores

Pestaña	Sección	Campo	Valor

© Acronis International GmbH, 2003-2025

Control de directiva de preferencias de privacidad	Acceso a la app	Identificador	com.acronis.backup

© Acronis International GmbH, 2003-2025

		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir
	Acceso a la app	Identificador	com.acronis.backup.aakore
		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir
	Acceso a la app	Identificado	com.acronis.backup.activeprotection
		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir

© Acronis International GmbH, 2003-2025

	Acceso a la app	Identificador	cyber-protect-service
		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir
Extensiones del sistema		Permitir a los usuarios aprobar extensiones del sistema	Habilitado
	Extensiones del sistema e ID de equipo permitidos	Nombre que se muestra	Extensiones del sistema del agente de ciberprotección de Acronis
		Tipos de extensiones del sistema	Identificadores de equipo permitidos
		Identificador de equipo	ZU2TV78AA6

Requisitos para macOS hasta la versión 11

Pestaña	Sección	Campo	Valor

© Acronis International GmbH, 2003-2025

Control de directiva de preferencias de privacidad	Acceso a la app	Identificador	com.acronis.backup

© Acronis International GmbH, 2003-2025

		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir
	Acceso a la app	Identificador	com.acronis.backup.aakore
		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir
	Acceso a la app	Identificado	com.acronis.backup.activeprotection
		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir

© Acronis International GmbH, 2003-2025

	Acceso a la app	Identificador	cyber-protect-service
		Tipo de identificador	ID de paquete
		Requisito de código	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		SERVICIO O APP	SystemPolicyAllFiles
		ACCESS	Permitir
Extensiones de kernel aprobadas		Permitir a los usuarios aprobar extensiones de kernel	Habilitado
		Permitir a los usuarios aprobar extensiones de kernel heredadas (macOS 11 y versiones posteriores)	Habilitado
	Extensiones de kernel e ID de equipo aprobados	ID de equipo aprobado: nombre que se muestra	Extensiones de kernel del agente de ciberprotección de Acronis
		ID del equipo	ZU2TV78AA6
		ID de paquete de extensiones de kernel	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Extensiones del sistema		Permitir a los usuarios aprobar extensiones del sistema	Habilitado
	Extensiones del sistema e ID de equipo permitidos	Nombre que se muestra	Acronis Cyber Protection Agent System Extensions
		Tipos de extensiones del sistema	Identificadores de equipo permitidos

© Acronis International GmbH, 2003-2025

		Identificador de equipo	ZU2TV78AA6

Solución de problemas de permisos en macOS

Es posible que aparezca el mensaje "Extensión del sistema bloqueada" durante la instalación del Agente para macOS en la pantalla del equipo Mac protegido. Se realizan los siguientes procedimientos en el equipo protegido.

Pasos para aprobar la extensión del sistema del agente de ciberprotección de Acronis

1. Haga clic en **Abrir configuración del sistema**.
   Si cierra el cuadro de diálogo accidentalmente, puede acceder a **Configuración/Preferencias del sistema** desde el menú **Apple** .
2. Vaya a **Privacidad y seguridad**.
3. Desplácese hacia abajo para encontrar el mensaje que indica que la extensión del sistema fue bloqueada.
4. Haga clic en el botón **Permitir** junto a la extensión bloqueada.
5. Reinicie el equipo Mac para que los cambios surtan efecto.

Nota
Si el botón **Permitir** no aparece, es posible que necesite ajustar la configuración de seguridad en el modo de recuperación.

Pasos para ajustar la configuración de seguridad en el modo de recuperación

1. Apague el Mac.
2. Mantenga presionado el botón de encendido hasta que vea las opciones de inicio.
3. Haga clic en **Opciones** y luego continúe a la siguiente pantalla.
4. En el menú **Utilidades** , seleccione **Utilidad de seguridad de arranque**.
5. En la Utilidad de seguridad de arranque, haga clic en el botón **Política de seguridad**.
6. Seleccione **Reducir seguridad** y luego marque la casilla de verificación **Permitir la administración de usuarios de extensiones de kernel de desarrolladores identificados**.
7. Haga clic en **Aceptar**, introduzca su contraseña de administrador y espere a que se apliquen los cambios.
8. En la barra del menú, haga clic en **Disco de arranque** y luego en **Salir del disco de arranque**. Esto le llevará a la pantalla anterior.
9. Haga clic en el icono de Apple y seleccione **Reiniciar**.

Registro de cargas de trabajo

Un registro está conectando una carga de trabajo en la que se instala un agente de protección a una cuenta de usuario en un inquilino de cliente. Después de que se complete el registro, puede ver la

© Acronis International GmbH, 2003-2025

carga de trabajo en la consola de Cyber Protect, bajo **Dispositivos** > **Equipos con agentes**. Puede gestionar las cargas de trabajo registradas aplicándoles planes.

Cuando instala un agente de protección utilizando la interfaz gráfica de usuario, el registro es parte del procedimiento de instalación.

Cuando utiliza la interfaz de línea de comandos, puede realizar el registro como un procedimiento independiente.

Registro de cargas de trabajo utilizando la interfaz gráfica de usuario

Cuando instala un agente de protección utilizando la interfaz gráfica de usuario, el registro es parte del procedimiento de instalación.

Los siguientes métodos de registro están disponibles:

- Registro en la consola de Cyber Protect
- Registro con credenciales de cuenta de usuario
- Registro con un token de registro

El agente se da de baja automáticamente cuando lo desinstala.

Registro de cargas de trabajo utilizando la consola de Cyber Protect

Al utilizar la consola de Cyber Protect, el registro de cargas de trabajo es parte de la instalación de agentes de protección.

Requisitos previos

- Finalizó la instalación de un agente de protección con la configuración de instalación predeterminada (**Configuración de registro** > **Usar consola de Cyber Protect**) y el asistente de instalación sigue abierto.

  Nota
  No cierre el asistente de instalación antes de completar el registro. De lo contrario, tendrá que repetir la instalación y comenzar el registro de nuevo.

- Para poder seleccionar un plan durante el registro, la autenticación de doble factor (2FA) debe estar habilitada para el inquilino al que pertenece su cuenta. Para obtener más información, consulte "Planes preseleccionados" (p. 244).

Para registrar una carga de trabajo desde la consola de Cyber Protect

1. En el asistente de instalación, haga clic en **Registrar carga de trabajo**.
   La consola de Cyber Protect se abre.
2. Inicie sesión en la consola de Cyber Protect.
   Se abre el asistente **Registrar carga de trabajo**.

© Acronis International GmbH, 2003-2025

3. [Si inicia sesión como administrador] En la pestaña **Seleccionar cuenta**, seleccione la cuenta bajo la cual desea registrar la carga de trabajo.

   Esta cuenta debe estar en un cliente-inquilino o una unidad. Los administradores de partners pueden ver los clientes-inquilinos que gestionan y registrar cargas de trabajo en las cuentas de esos inquilinos.

   Nota
   Si solo hay una cuenta en el inquilino o unidad seleccionada, este campo se rellena automáticamente.

4. Haga clic en **Validar código**.
5. Haga clic en **Siguiente**.
6. [Si 2FA está habilitada para su cuenta] En la pestaña **Seleccionar planes**, revise los planes preseleccionados que se aplicarán a la carga de trabajo.
7. [Opcional] [Si 2FA está habilitada para su cuenta] Para cambiar un plan preseleccionado, haga clic en **Modificar**.
   - Seleccione un plan.
   - Haga clic en **Seleccionar**.
8. [Opcional] Si no desea aplicar un plan preseleccionado, haga clic en **Modificar** y luego en **No aplicar**.
9. En la pantalla **Revisar y registrar**, compruebe las cuotas requeridas y, a continuación, realice una de las siguientes acciones:
   a. Para registrar la carga de trabajo, haga clic en **Registrar**.

      Si ha iniciado sesión como administrador de partner, se habilitarán automáticamente los paquetes Advanced necesarios para el inquilino en el que registre la carga de trabajo.

      Si no ha iniciado sesión como administrador de partner, no se habilitarán automáticamente los paquetes Advanced requeridos. Aún puede aplicar los planes seleccionados, pero es posible que no funcionen correctamente. Para resolver este problema, pida a su administrador de partner que habilite los paquetes Advanced requeridos o que cambie los planes preseleccionados.
   b. Para seleccionar diferentes planes, vaya a la pestaña **Seleccionar planes** y continúe con este procedimiento.

Como resultado, la carga de trabajo se registra en la cuenta especificada y se aplican automáticamente los planes seleccionados.

Registro de cargas de trabajo utilizando credenciales de usuario

Puede modificar el procedimiento de instalación predeterminado y seleccionar el registro con un nombre de usuario y contraseña, en lugar del registro en la consola de Cyber Protect.

Para registrar una carga de trabajo con un nombre de usuario y una contraseña

© Acronis International GmbH, 2003-2025

1. En el asistente de instalación, haga clic en **Personalizar configuración de la instalación**.
2. En la sección de **Ajustes de registro**, haga clic en **Modificar**.
3. Seleccione **Usar credenciales**.
4. Especifique el nombre de usuario y la contraseña de la cuenta bajo la cual desea registrar la carga de trabajo.
   Esta cuenta debe ser una cuenta en un inquilino de cliente.

   Nota
   Solo puede usar cuentas para las cuales no está habilitada la autenticación de dos factores.
5. Haga clic en **Listo**, y luego complete la instalación.

Registro de cargas de trabajo utilizando un token de registro

Puede modificar el procedimiento de instalación predeterminado y seleccionar el registro con un token de registro, en lugar del registro en la consola de Cyber Protect.

Para registrar una carga de trabajo con un token de registro

1. En el asistente de instalación, haga clic en **Personalizar configuración de la instalación**.
2. En la sección de **Ajustes de registro**, haga clic en **Modificar**.
3. Seleccione **Usar token de registro**.
4. Introduzca el token de registro.
5. Haga clic en **Listo**, y luego complete la instalación.

Generar un token de registro

Un token de registro es una serie de 12 caracteres, separados por guiones en tres segmentos. El token de registro transmite la identidad de un usuario al programa de configuración del agente, sin almacenar las credenciales del usuario para la consola de Cyber Protect. Esto permite a los usuarios registrar cargas de trabajo bajo su cuenta o aplicar planes de protección a las cargas de trabajo sin iniciar sesión en la consola.

Nota
Los planes de protección no se aplican automáticamente durante el registro de la carga de trabajo. La aplicación de un plan de protección es una tarea independiente.

Por motivos de seguridad, los tokens tienen una vida útil limitada que puede ajustar. La vida útil predeterminada es de 3 días.

Los administradores pueden generar tokens de registro para todas las cuentas de usuario en el inquilino que administran. Los usuarios pueden generar tokens de registro solo para sus propias cuentas.

Para generar un token de registro

© Acronis International GmbH, 2003-2025

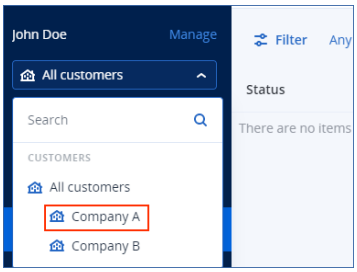
Como administrador

1. Inicie sesión como administrador en la consola de Cyber Protect.

   Si ya ha iniciado sesión en el portal de administración, puede ir a la consola de Cyber Protect. Para ello, vaya a **Supervisión** > **Uso** y, en la pestaña **Protección**, haga clic en **Gestionar servicio**.

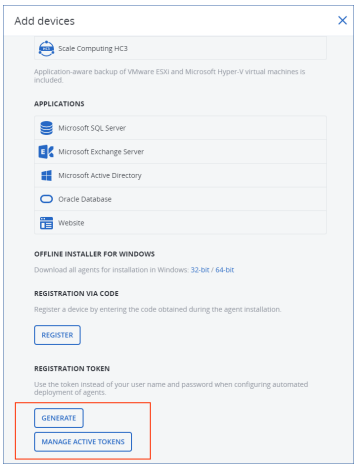
   [Para administradores de partner que gestionen inquilinos de cliente] En la consola de Cyber Protect, seleccione el inquilino con el usuario para el que desea generar un token. No puede generar un token en el nivel **Todos los clientes**.

2. En **Dispositivos**, haga clic en **Todos los dispositivos** > **Agregar**.

   Se abrirá el panel **Añadir dispositivos** en la parte derecha.

3. Desplácese hasta **Token de registro** y haga clic en **Generar**.

4. Especifique la vida útil del token.
5. Seleccione el usuario para el que desea generar un token.

   Nota
   Cuando utilice el token, las cargas de trabajo se registrarán en la cuenta de usuario que seleccione aquí.

6. [Opcional] Para permitir que el usuario del token pueda aplicar y revocar un plan de protección en las cargas de trabajo añadidas, seleccione el plan de la lista desplegable.

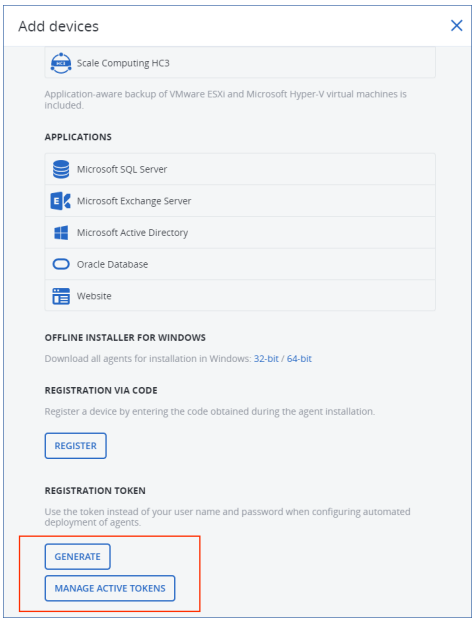
© Acronis International GmbH, 2003-2025

Para aplicar o revocar el plan de protección en las cargas de trabajo añadidas, debe ejecutar un script. Para obtener más información, consulte este artículo de la base de conocimiento.

7. Haga clic en **Generar token**.
8. Haga clic en **Copiar** para copiar el token al portapapeles de su dispositivo o escriba el token manualmente.

Como usuario

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar**.
   Se abrirá el panel **Añadir dispositivos** en la parte derecha.
3. Desplácese hasta **Token de registro** y haga clic en **Generar**.



4. Especifique la vida útil del token.
5. Haga clic en **Generar token**.
6. Haga clic en **Copiar** para copiar el token al portapapeles de su dispositivo o escriba el token manualmente.

Gestión de tokens de registro

Puede ver y eliminar los tokens de registro activos.

Para ver los tokens de registro

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar**.
3. Desplácese hasta **Token de registro** y haga clic en **Gestionar tokens activos**.
   A la derecha se abrirá una lista con los tokens activos generados para el inquilino.

© Acronis International GmbH, 2003-2025

Nota
Por motivos de seguridad, en la columna **Token**, solo se muestran los dos primeros caracteres del valor del token.

Para eliminar un token de registro

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar**.
3. Desplácese hasta **Token de registro** y haga clic en **Gestionar tokens activos**.
   A la derecha se abrirá una lista con los tokens activos generados para el inquilino.

   Nota
   Por motivos de seguridad, en la columna **Token**, solo se muestran los dos primeros caracteres del valor del token.

4. Seleccione el token y haga clic en **Eliminar**.

Registro y anulación de registro de cargas de trabajo utilizando la interfaz de línea de comandos

Cuando utiliza la interfaz de línea de comandos, puede realizar el registro como un procedimiento independiente.

Por lo tanto, por ejemplo, no tiene que desinstalar el agente de protección si desea registrarlo bajo otra cuenta.

Registro de cargas de trabajo utilizando credenciales de usuario

Utilice el nombre de usuario y la contraseña para la cuenta bajo la cual desea registrar la carga de trabajo. Esta cuenta debe ser una cuenta en un inquilino de cliente. Si la contraseña contiene caracteres especiales o espacios en blanco, consulte "Uso de contraseñas con caracteres especiales o espacios en blanco" (p. 116).

La dirección del servicio es la URL que utiliza para iniciar sesión en el servicio Cyber Protection.

Por ejemplo, `https://cloud.company.com`.



Para registrar una carga de trabajo con un nombre de usuario y una contraseña

En Windows

© Acronis International GmbH, 2003-2025

- En el Símbolo del sistema, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

- En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Por ejemplo:

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

En macOS

Importante
Si utiliza macOS 10.14 o posterior, conceda acceso total al disco al agente de protección. Para ello, vaya a **Aplicaciones** > **Utilidades** y, a continuación, ejecute el **Asistente para el Agente de Cyber Protect**. A continuación, siga las instrucciones de la ventana de la aplicación.

- En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Por ejemplo:

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

Uso de contraseñas con caracteres especiales o espacios en blanco

Si su contraseña contiene caracteres especiales o espacios en blanco, póngala entre comillas cuando la escriba en la línea de comando.

Por ejemplo, en Windows, ejecute este comando en el símbolo del sistema:

Plantilla de comando:

© Acronis International GmbH, 2003-2025

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

Ejemplo de comando:

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

Si falla este comando, cifre su contraseña en formato base64 en https://www.base64encode.org/. A continuación, en la línea de comando, especifique la contraseña cifrada mediante el parámetro -b o --base64.

Por ejemplo, en Windows, ejecute este comando en el símbolo del sistema:

Plantilla de comando:

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

Ejemplo de comando:

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

Registro de cargas de trabajo utilizando un token de registro

Un token de registro es una serie de 12 caracteres, separados por guiones en tres segmentos. El token de registro transmite la identidad de un usuario al programa de configuración del agente, sin almacenar las credenciales del usuario para la consola de Cyber Protect. Esto permite a los usuarios registrar cargas de trabajo bajo su cuenta o aplicar planes de protección a las cargas de trabajo sin iniciar sesión en la consola.

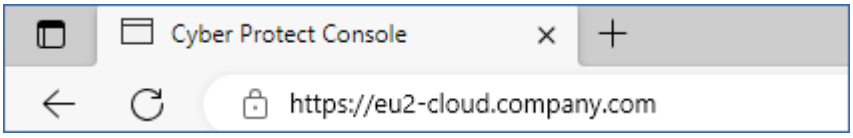
Para obtener más información, consulte "Generar un token de registro" (p. 112).

Nota
Los planes de protección no se aplican automáticamente durante el registro de la carga de trabajo. La aplicación de un plan de protección es una tarea independiente.

Para obtener más información, consulte este artículo de la base de conocimientos.

Cuando utiliza un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve después de iniciar sesión en el servicio Cyber Protection.

Por ejemplo, `https://eu2-cloud.company.com`.



© Acronis International GmbH, 2003-2025

Para registrar una carga de trabajo con un token de registro

En Windows

- En el Símbolo del sistema, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

- En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Por ejemplo:

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

En macOS

Importante
Si utiliza macOS 10.14 o posterior, conceda acceso total al disco al agente de protección. Para ello, vaya a **Aplicaciones** > **Utilidades** y, a continuación, ejecute el **Asistente para el Agente de Cyber Protect**. A continuación, siga las instrucciones de la ventana de la aplicación.

- En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Por ejemplo:

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

Virtual Appliance

1. En la consola del dispositivo virtual, presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
2. En la interfaz de línea de comandos, ejecute el siguiente comando:

© Acronis International GmbH, 2003-2025

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

Por ejemplo:

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

3. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

Dispositivo de arranque

1. En la interfaz gráfica de usuario del dispositivo de arranque, haga clic en **Acciones** > **Iniciar shell**.
2. En la interfaz de la línea de comandos, navegue a la carpeta `/bin`:

```
cd /bin
```

3. En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Por ejemplo:

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

4. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo de arranque.

Dar de baja cargas de trabajo

Desde la interfaz de línea de comandos, puede dar de baja un agente de protección sin desinstalarlo.

Para anular el registro de una carga de trabajo

En Windows

- En el Símbolo del sistema, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

- En la interfaz de línea de comandos, ejecute el siguiente comando:

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


© Acronis International GmbH, 2003-2025

En macOS

- En la interfaz de línea de comandos, ejecute el siguiente comando:

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

Virtual Appliance

1. En la consola del dispositivo virtual, presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
2. En la interfaz de línea de comandos, ejecute el siguiente comando:

```
register_agent -o unregister
```

3. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

Cambio de registro de una carga de trabajo

Puede cambiar el registro de una carga de trabajo registrándola en un nuevo inquilino o una nueva cuenta de usuario.

Importante
Cuando cambie el registro de una carga de trabajo, se revocarán todos los planes de protección que se le apliquen. Para seguir protegiendo la carga de trabajo, aplíquele un nuevo plan de protección.

Si registra la carga de trabajo en un nuevo inquilino, esta perderá el acceso a las copias de seguridad ubicadas en el almacenamiento en la nube del inquilino original. Podrá seguir accediendo a las copias de seguridad ubicadas en cualquier almacenamiento que no sea la nube.

Cómo cambiar el registro de una carga de trabajo

Utilizando la interfaz de línea de comandos

1. Anule el registro del agente de protección como se describe en "Dar de baja cargas de trabajo" (p. 119).
2. Registre el agente de protección en el nuevo inquilino o con la nueva cuenta de usuario como se describe en "Registro de cargas de trabajo utilizando credenciales de usuario" (p. 115) o "Registro de cargas de trabajo utilizando un token de registro" (p. 117).

Utilizando la interfaz gráfica de usuario

1. Desinstale el agente de protección.
2. Instale el agente de protección y regístrelo en el nuevo inquilino o con la nueva cuenta de usuario.

Para obtener más información sobre cómo instalar y registrar un agente, consulte "Instalación de agentes de protección utilizando la interfaz gráfica de usuario" (p. 65).

© Acronis International GmbH, 2003-2025

Traslado de cargas de trabajo a otro inquilino

Mover una carga de trabajo a otro inquilino no es compatible de forma nativa. Como solución alternativa, puede cancelar el registro de la carga de trabajo y luego registrarla en otro inquilino. Todos los planes de protección aplicados se revocarán desde esa carga de trabajo y esta perderá el acceso a las copias de seguridad ubicadas en el almacenamiento en la nube del inquilino original.

Para obtener más información sobre cómo registrar una carga de trabajo en un nuevo inquilino o una nueva cuenta de usuario, consulte "Cambio de registro de una carga de trabajo" (p. 120).

Actualización de agentes de protección

Puede actualizar todos los agentes de forma manual mediante la consola de Cyber Protect o mediante la descarga y ejecución del archivo de instalación.

Puede configurar actualizaciones automáticas para los siguientes agentes:

- Agente para Windows
- Agente para Linux
- Agente para Mac
- Agente de Cyber Files Cloud para File Sync & Share

Espacio libre en disco que se requiere para la actualización

Se requiere espacio libre para actualizar un agente de forma automática o manual, mediante la consola de Cyber Protect.

Sistema operativo	Ubicación de descarga	Espacio de disco requerido
Linux	/opt/acronis/Acroinst2/	3 GB
Mac	/Library/Application Support/Acronis/Acroinst2	2 GB
Windows	%ProgramData%\Acronis\Acroinst2\ %ProgramData%\Acronis\InstallationCache\	2 GB

© Acronis International GmbH, 2003-2025

Nota
[Para todos los agentes facilitados en forma de dispositivo virtual, incluido agente para VMware, agente para Scale Computing, agente para Virtuozzo Hybrid Infrastructure y agente para RHV (oVirt)]

Para llevar a cabo una actualización automática o manual de un dispositivo virtual ubicado detrás de un proxy, este se debe configurar en cada dispositivo del siguiente modo:

En el archivo `/opt/acronis/etc/va-updater/config.yaml`, añada la siguiente línea al final de este e introduzca los valores específicos para su entorno:

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

Configuración del método predeterminado para actualizar agentes

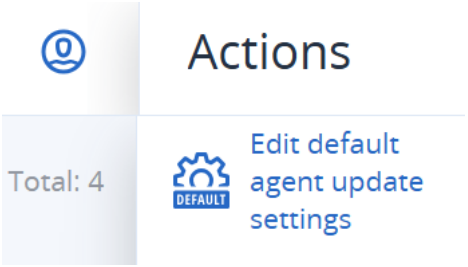
Puede configurar el método predeterminado para actualizar agentes (manual o automático) para todos los agentes en todos los equipos o en cada equipo por separado.

La configuración predeterminada para las actualizaciones de agentes es accesible desde la consola de Cyber Protection y el portal de administración, para todos los roles de usuario.

Actualizaciones automáticas

Para ajustar la configuración predeterminada de las actualizaciones automáticas para todos los agentes en la consola de Cyber Protect

1. Seleccione **Configuración** > **Agentes**.
2. En **Acciones** en la esquina superior derecha, haga clic en **Editar configuración predeterminada de actualización de agentes**.



3. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

4. Compruebe que la opción **Actualizar agentes automáticamente** esté activada.

© Acronis International GmbH, 2003-2025

Nota

Las actualizaciones automáticas solo están disponibles para los siguientes agentes:

- Agentes de Cyber Protect de la versiones 26986 (publicada en mayo de 2021) o posteriores.
- Agente de escritorio para File Sync & Share, versión 15.0.30370 o posterior.

Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente antes de que se produzcan las actualizaciones automáticas.

5. [Opcional] Establezca la ventana de mantenimiento.
   La ventana predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

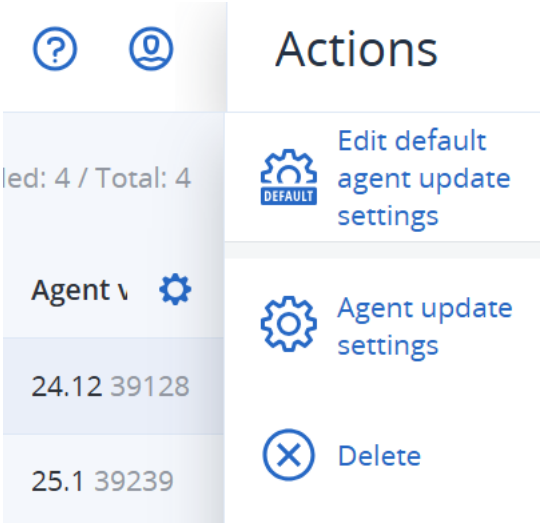
Nota

Aunque las actualizaciones de los agentes son rápidas y fluidas, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

6. Haga clic en **Guardar**.

Para ajustar la configuración predeterminada de las actualizaciones automáticas para agentes seleccionados en la consola de Cyber Protect.

1. Seleccione **Configuración** > **Agentes**.
2. En la lista de agentes, seleccione el agente para el que desee configurar los ajustes de actualización automática.
3. En la esquina superior derecha, en **Acciones**, haga clic en **Configuración de actualización del agente**.



4. Haga clic en **Editar configuración predeterminada de actualización del agente**.
5. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

6. Compruebe que la opción **Actualizar agentes automáticamente** esté activada.

Nota
Las actualizaciones automáticas solo están disponibles para los siguientes agentes:

- Agentes de Cyber Protect de la versiones 26986 (publicada en mayo de 2021) o posteriores.
- Agente de escritorio para File Sync & Share, versión 15.0.30370 o posterior.

Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente antes de que se produzcan las actualizaciones automáticas.

7. [Opcional] Establezca la ventana de mantenimiento.
La ventana predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

Nota
Aunque las actualizaciones de los agentes son rápidas y fluidas, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

8. Haga clic en **Guardar**.

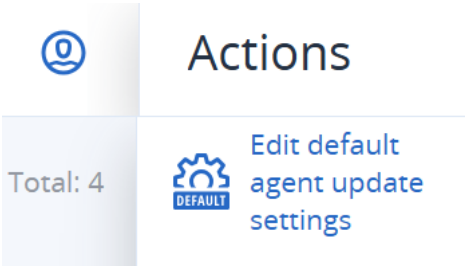
Actualizaciones manuales

Importante
Le recomendamos encarecidamente que habilite las actualizaciones automáticas para sus agentes. Las actualizaciones periódicas garantizan que sus agentes estén actualizados, tengan un mejor rendimiento, solucionen errores y mejoren las funciones de protección y seguridad.

Para ajustar la configuración predeterminada de las actualizaciones manuales para todos los agentes en la consola de Cyber Protection

1. Vaya a **Configuración** > **Agentes**.
2. En **Acciones** en la esquina superior derecha, haga clic en **Editar configuración predeterminada de actualización de agentes**.

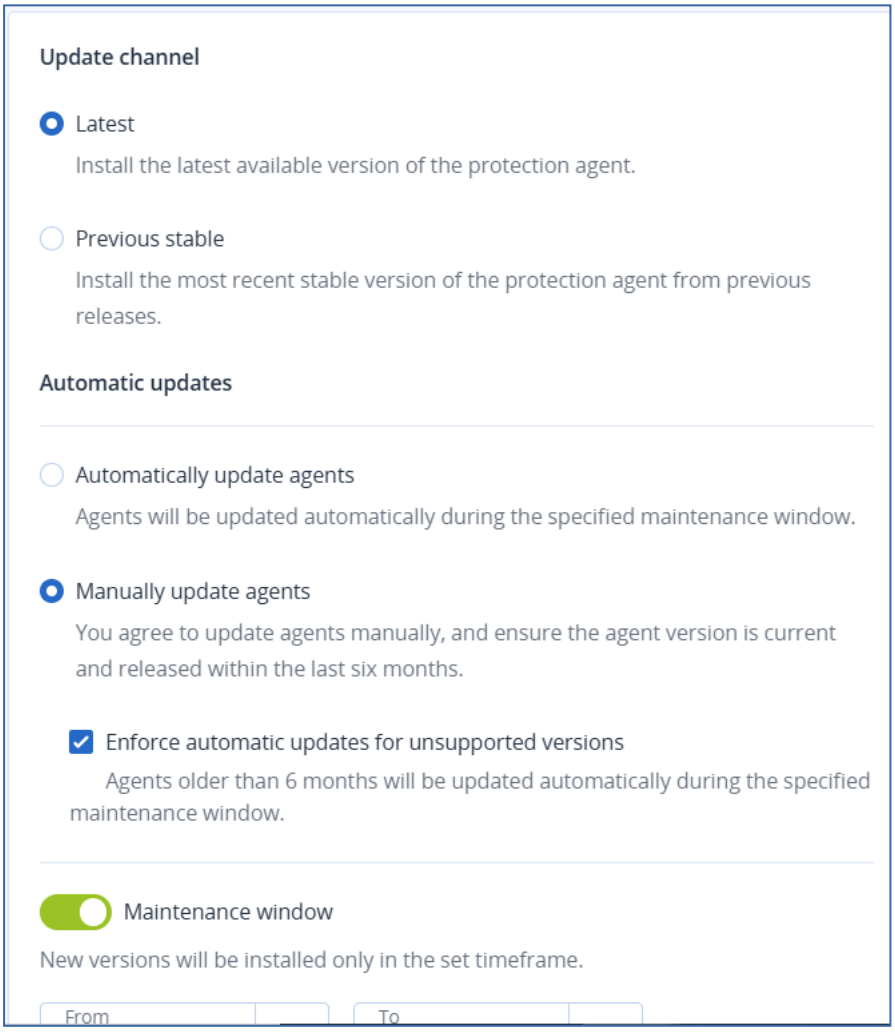
© Acronis International GmbH, 2003-2025



3. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

4. Seleccione **Actualizar agentes manualmente.**



5. [Opcional] Para prevenir riesgos de seguridad, garantizar el acceso a las últimas funciones y minimizar los problemas técnicos causados por agentes significativamente obsoletos, habilite las

© Acronis International GmbH, 2003-2025

actualizaciones automáticas de los agentes que tengan más de 6 meses.

a. Seleccione **Imponer actualizaciones automáticas para las versiones no compatibles**.

Importante
Si de cara a la versión C25.02 no ha habilitado las actualizaciones automáticas de los agentes, esta opción se actualizará automáticamente para todos los inquilinos de su entorno.

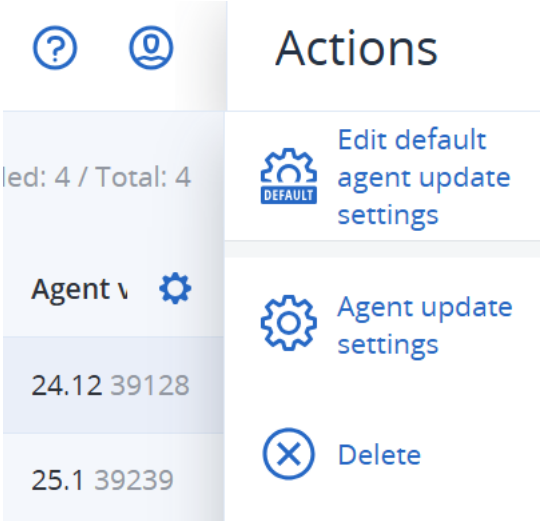
b. [Opcional] Establezca la ventana de mantenimiento.
La ventana de mantenimiento predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

Nota
Aunque los procesos de actualización de los agentes están diseñados para ser rápidos y fluidos, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

6. Haga clic en **Guardar.**

Para configurar actualizaciones manuales para agentes seleccionados en la consola de Cyber Protect.

1. Vaya a **Configuración** > **Agentes**.
2. En la lista de agentes, seleccione el agente para el que desee configurar los ajustes de actualización automática.
3. En la esquina superior derecha, en **Acciones**, haga clic en **Configuración de actualización del agente**.

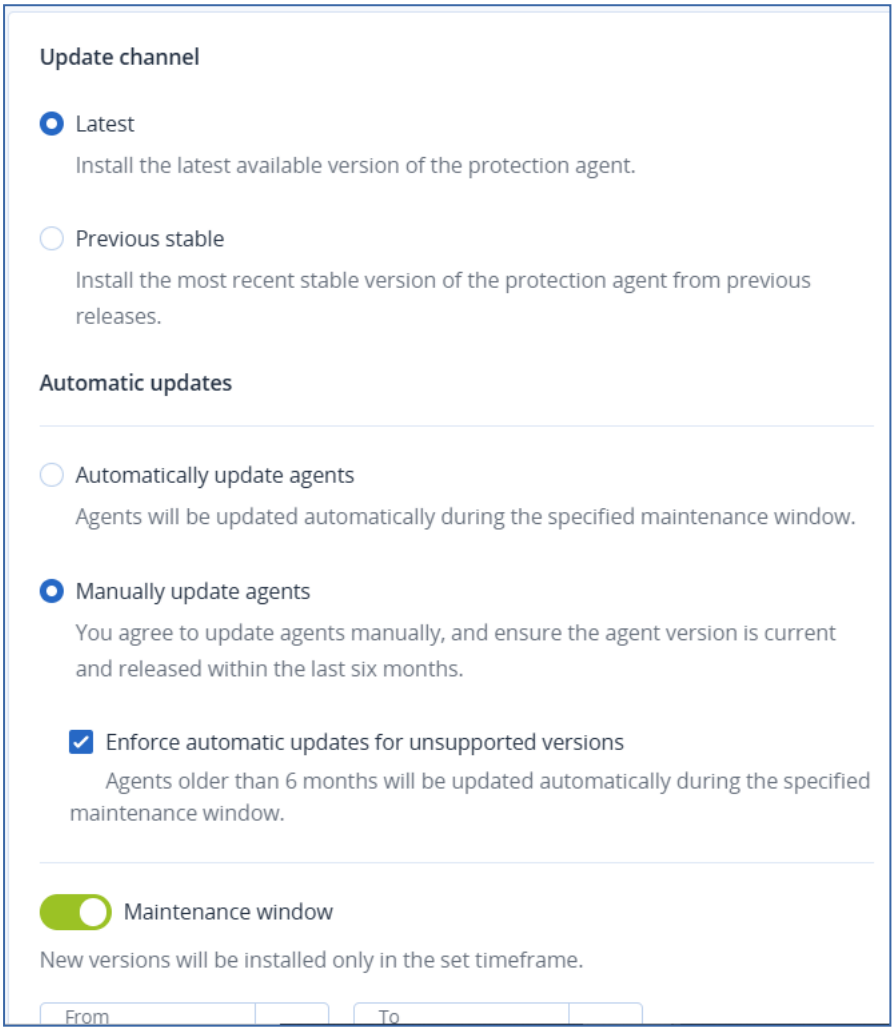


4. Haga clic en **Editar configuración predeterminada de actualización del agente**.
5. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

6. Seleccione **Actualizar agentes manualmente.**



7. [Opcional] Para prevenir riesgos de seguridad, garantizar el acceso a las últimas funciones y minimizar los problemas técnicos causados por agentes significativamente obsoletos, habilite las actualizaciones automáticas de los agentes que tengan más de 6 meses.
   a. Seleccione **Imponer actualizaciones automáticas para las versiones no compatibles**.

   Importante
   Si de cara a la versión C25.02 no ha habilitado las actualizaciones automáticas de los agentes, esta opción se actualizará automáticamente para todos los inquilinos de su entorno.

   b. [Opcional] Establezca la ventana de mantenimiento.
   La ventana de mantenimiento predeterminada es diaria, de 23:00 a 08:00 en el equipo donde

© Acronis International GmbH, 2003-2025

está instalado el agente.

Nota
Aunque las actualizaciones de los agentes son rápidas y fluidas, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

8. Haga clic en **Guardar.**

Supervisión de las actualizaciones del agente

Para supervisar las actualizaciones de los agentes, consulte las secciones "Panel de control de Alertas" (p. 290) y "Panel de control Actividades" (p. 289).

Actualización manual de agentes de protección

Puede actualizar los agentes mediante la consola de Cyber Protect o mediante la descarga y ejecución del archivo de instalación.

Los dispositivos virtuales con las siguientes versiones deben actualizarse únicamente mediante la consola de Cyber Protect:

- Agente para VMware (dispositivo virtual): versión 12.5.23094 y posteriores.
- Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual): versión 12.5.23094 y posteriores.

Los agentes con las siguientes versiones también se pueden actualizar mediante la consola de Cyber Protect:

- Agente para Windows, Agente para VMware (Windows), Agente para Hyper-V: versiones 12.5.21670 y posteriores.
- Agente para Linux: versiones 12.5.23094 y posteriores.
- Otros agentes: versiones 12.5.23094 y posteriores.

Para actualizar versiones anteriores de esos agentes, descargue e instale la versión más reciente de forma manual. Para buscar los enlaces de descarga, haga clic en **Todos los dispositivos** > **Agregar**.

Para localizar la versión del agente, en la consola de Cyber Protect, seleccione el equipo y haga clic en **Detalles**.

Requisitos previos

En equipos Windows, las funciones de Cyber Protect requieren Microsoft Visual C++ 2017 Redistributable. Asegúrese de que esté instalado en su equipo o hágalo antes de actualizar el agente. Es posible que tenga que reiniciar el equipo después de la instalación. Puede encontrar el paquete de Microsoft Visual C++ Redistributable en el sitio web de Microsoft: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Para actualizar un agente mediante la consola de Cyber Protect

© Acronis International GmbH, 2003-2025

Nota
[Para planes de protección creados después de noviembre de 2024] La desinstalación y modificación de los agentes de protección para Windows está prohibida de forma predeterminada. El Agente para Windows solo se puede modificar durante una ventana de mantenimiento o a través de la funcionalidad de actualización automática del agente. Para obtener instrucciones sobre cómo habilitar la desinstalación o modificación de un solo uso de un agente, consulte "Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada" (p. 213). Para deshabilitar la protección de desinstalación del agente, consulte "Pasos para deshabilitar la protección de desinstalación del agente" (p. 214).

1. Haga clic en **Configuración** > **Agentes**.
   Aparece la lista de equipos protegidos. Los equipos con versiones de agentes obsoletas tienen un signo de exclamación naranja.
2. Seleccione los equipos en los que desea actualizar los agentes.

   Nota
   Los equipos deben estar conectados.

3. Haga clic en **Actualizar agente**.

Nota
Durante la actualización, toda copia de seguridad en curso fallará.

Pasos para actualizar las definiciones de ciberprotección de un equipo

1. Haga clic en **Configuración** > **Agentes**.
2. Seleccione el equipo en el que desea actualizar las definiciones de ciberprotección y haga clic en **Actualizar definiciones**. El equipo debe estar conectado.

Pasos para asignar el rol de actualizador a un agente

1. Haga clic en **Configuración** > **Agentes**.
2. Seleccione el equipo al que desea asignar el rol de actualizador, haga clic en **Detalles** y, a continuación, en la sección **Definiciones de ciberprotección**, habilite la opción **Utilice este agente para descargar y distribuir parches y actualizaciones**.

   Nota
   Un agente con el rol de actualizador puede descargar y distribuir parches solo para productos Windows de terceros. En el caso de los productos de Microsoft, la distribución de parches no es compatible con el agente actualizador.

Pasos para borrar los datos de la caché en un agente

© Acronis International GmbH, 2003-2025

1. Haga clic en **Configuración** > **Agentes**.
2. Seleccione el equipo cuyos datos de la caché desea borrar (Datos obsoletos de los archivos de actualización y la gestión de parches) y haga clic en **Borrar caché**.

Actualización de agentes de protección automática

Para facilitar la gestión de varios recursos informáticos, puede configurar la actualización automática de Agente para Windows, Agente para Linux y Agente para Mac. Las actualizaciones automáticas están disponibles para los agentes de las versiones 26986 (publicada en mayo de 2021) o posteriores. Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente en primer lugar.

Nota
La configuración de actualizaciones automáticas para un agente de protección anula la configuración de **Protección de desinstalación del agente** en todos los planes de protección para el agente.

Las actualizaciones automáticas son compatibles en equipos con alguno de los siguientes sistemas operativos:

- Windows XP SP 3 y posterior
- Red Hat Enterprise Linux 6 y posterior, CentOS 6 y posterior
- OS X 10.9 Mavericks y posterior

Los ajustes de las actualizaciones automáticas están preconfigurados a nivel de centro de datos. Un partner o los administradores de empresas pueden personalizar estos ajustes en todos los equipos de una empresa o una unidad o en equipos individuales. Si no se aplican ajustes personalizados, se utilizarán los del nivel superior en este orden:

1. centro de datos de Cyber Protection
2. Empresa (inquilino de cliente)
3. Unidad
4. Equipo

Por ejemplo, el administrador de una unidad puede configurar los ajustes de actualizaciones automáticas personalizados para todos los equipos de la unidad, que pueden ser distintos a los aplicados en equipos a nivel de empresa. El administrador también puede configurar ajustes diferentes para uno o más equipos individuales de la unidad, a los que no se aplicarán ni los ajustes de la unidad ni los de la empresa.
Incluso con la ventana de mantenimiento habilitada, las actualizaciones no se instalarán mientras el agente lleve a cabo alguna de las siguientes operaciones:

- Copia de seguridad
- Recuperación

© Acronis International GmbH, 2003-2025

- Réplica de copia de seguridad
- Réplica de máquina virtual
- Realización de pruebas en una réplica
- Ejecución de una máquina virtual desde una copia de seguridad (con finalización)
- Conmutación por error de la recuperación ante desastres
- Conmutación por recuperación de la recuperación ante desastres
- Ejecución de una secuencia de comandos (para la funcionalidad de Secuencia de comandos cibernética)
- Instalación del parche
- Copia de seguridad de configuración de ESXi

Actualizaciones automáticas para todos los agentes

Pasos para configurar las actualizaciones automáticas de agentes desde la consola de Cyber Protection

1. Seleccione **Configuración > Agentes**.
2. En **Acciones** en la parte superior derecha, haga clic en **Edite la configuración predeterminada de la actualización del agente**.
3. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

4. Compruebe que la opción **Actualizar agentes automáticamente** esté activada.

   Nota
   Las actualizaciones automáticas solo están disponibles para los siguientes agentes:
   - Agentes de Cyber Protect de la versiones 26986 (publicada en mayo de 2021) o posteriores.
   - Agente de escritorio para File Sync & Share, versión 15.0.30370 o posterior.

   Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente antes de que se produzcan las actualizaciones automáticas.

5. [Opcional] Habilite la ventana de mantenimiento.
   La ventana predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

© Acronis International GmbH, 2003-2025

Nota
Aunque los procesos de actualización de los agentes están diseñados para ser rápidos y fluidos, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

6. Haga clic en **Guardar.**

Actualizaciones automáticas para un solo agente

Importante
Le recomendamos encarecidamente que habilite las actualizaciones automáticas para sus agentes. Las actualizaciones periódicas garantizan que sus agentes estén actualizados, tengan un mejor rendimiento, solucionen errores y mejoren las funciones de protección y seguridad.

Pasos para configurar las actualizaciones automáticas de un agente desde la consola de Cyber Protection

1. Seleccione **Configuración > Agentes**.
2. En la lista de agentes, seleccione el agente para el que desea configurar los ajustes de actualización automática.
3. En **Acciones** en la esquina superior derecha, haga clic en **Configuración de la actualización del agente**.
4. En **Canal de actualización**, seleccione qué versión utilizar para las actualizaciones automáticas.

Opción	Descripción
Más reciente (seleccionada de manera predeterminada)	Instale la versión más reciente disponible del agente de Cyber Protection.
Anterior estable	Instale la versión estable más reciente de las versiones anteriores del agente de Cyber Protection.

5. Compruebe que la opción **Actualizar agentes automáticamente** esté activada.

Nota
Las actualizaciones automáticas solo están disponibles para los siguientes agentes:

- Agentes de Cyber Protect de la versiones 26986 (publicada en mayo de 2021) o posteriores.
- Agente de escritorio para File Sync & Share, versión 15.0.30370 o posterior.

Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente antes de que se produzcan las actualizaciones automáticas.

6. [Opcional] Habilite la ventana de mantenimiento.
La ventana predeterminada es diaria, de 23:00 a 08:00 en el equipo donde está instalado el agente.

© Acronis International GmbH, 2003-2025

Nota
Aunque los procesos de actualización de los agentes están diseñados para ser rápidos y fluidos, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

7. Haga clic en **Guardar.**

Supervisión del estado de la actualización automática

Pasos para comprobar el estado de las actualizaciones automáticas

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Haga clic en el icono de engranaje en la esquina superior derecha de la tabla y asegúrese de que la casilla de verificación **Actualización automática** está seleccionada.
3. Compruebe el estado que se muestra en la columna **Actualización automática**.

Eliminar la configuración de actualización automática

Importante
Para garantizar el correcto funcionamiento y la protección robusta de sus recursos informáticos, no recomendamos deshabilitar las actualizaciones automáticas de los agentes de protección.

Pasos para eliminar los ajustes personalizados de actualizaciones automáticas

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione el ámbito de los ajustes:
   - Para eliminar los ajustes personalizados de todos los equipos, haga clic en **Edite la configuración predeterminada de la actualización del agente**.
   - Para eliminar los ajustes personalizados para equipos específicos, seleccione los equipos que desee y haga clic en **Configuración de la actualización del agente**.
3. Haga clic en **Restablecer a los valores predeterminados** y, a continuación, haga clic en **Guardar**.

Actualización de agentes de protección en cargas de trabajo cifradas con BitLocker

Las actualizaciones de agentes que introducen cambios en Startup Recovery Manager interfieren con BitLocker en cargas de trabajo en las que tanto BitLocker como Startup Recovery Manager están habilitados. En este caso, después de un reinicio, se requiere la clave de recuperación de BitLocker. Para mitigar este problema, suspenda o deshabilite BitLocker antes de actualizar el agente.

Versiones del agente afectadas:

© Acronis International GmbH, 2003-2025

- 23.12.36943, lanzado en diciembre de 2023
- 25.01.XXXXX lanzado en enero de 2025
- 25.03.XXXXX lanzado en marzo de 2025

También puede verificar si una actualización introduce cambios en Startup Recovery Manager en las notas de versión del agente de protección.

Cómo actualizar el agente en una carga de trabajo con BitLocker y Startup Recovery Manager activados

1. En la carga de trabajo en la que desee actualizar el agente, suspenda o desactive BitLocker.
2. Actualice el agente.
3. Reinicie la carga de trabajo.
4. Active BitLocker.

Despliegue de agentes de protección a través de la directiva de grupo

Puede instalar (o desplegar) de manera central el Agente para Windows en los equipos que pertenecen a un dominio de Active Directory usando la directiva de grupo de Windows.

En esta sección, encontrará cómo instalar un objeto de directiva de grupo para implementar agentes en un dominio completo o en la unidad organizacional de los equipos.

Siempre que un equipo inicie sesión en el dominio, el objeto de directiva de grupo resultante garantizará que el agente se encuentre instalado y registrado.

Requisitos previos

- Dominio de Active Directory con un controlador de dominio que utiliza Microsoft Windows Server 2003 o una versión posterior.
- Debe ser miembro del grupo **Administradores del dominio** de este dominio.
- Ha descargado el programa de instalación **Todos los agentes para Windows**.
  Para descargar el programa de instalación, en la consola de Cyber Protect, haga clic en el icono de la cuenta en la esquina superior derecha y, a continuación, haga clic en **Descargas**. El enlace de descarga también está disponible en el panel **Añadir dispositivos**.

Pasos para desplegar agentes mediante la directiva de grupo

1. Genere un token de registro como se describe en "Generar un token de registro" (p. 112).
2. Cree el archivo .mst, el archivo .msi y los archivos .cab como se describe en "Creación del archivo de transformación y extracción de los paquetes de instalación" (p. 135).
3. Configure el objeto de directiva de grupo como se describe en "Configurar el objeto de directiva de grupo" (p. 135).

© Acronis International GmbH, 2003-2025

Creación del archivo de transformación y extracción de los paquetes de instalación

Para desplegar los agentes de protección a través de la directiva de grupo de Windows, necesita un archivo de transformación (.mst) y los paquetes de instalación (archivos .msi y .cab).

Nota
El siguiente procedimiento utiliza la opción de registro predeterminado, que es el registro por token. Para obtener más información sobre cómo generar un token de registro, consulte "Generar un token de registro" (p. 112).

Pasos para crear el archivo .mst y los paquetes de instalación (archivos .msi y .cab)

1. Conéctese como administrador en cualquier equipo del dominio de Active Directory.
2. Cree una carpeta compartida que contendrá los paquetes de instalación. Asegúrese de que los usuarios del dominio puedan acceder a la carpeta compartida, por ejemplo, manteniendo la configuración de uso compartido predeterminada para **Todos**.
3. Ejecute el programa de instalación del agente.
4. Haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión**.
5. En **Qué instalar**, seleccione los componentes que desea incluir en la instalación y haga clic en **Listo**.
6. En **Ajustes de registro**, haga clic en **Especificar**, introduzca un token de registro y haga clic en **Listo**.
   Puede cambiar el método de registro de **Usar token de registro** (opción predeterminada) a **Usar credenciales** u **Omitir registro**. La opción **Omitir registro** implica que registrará las cargas de trabajo de forma manual más tarde.
7. Compruebe o modifique la configuración de instalación, que se añadirá al archivo .mst, y haga clic en **Continuar**.
8. En **Guardar los archivos en**, especifique la ruta a la carpeta compartida que haya creado.
9. Haga clic en **Generar**.

Como resultado, el archivo .mst, el archivo .msi y los archivos .cab se crearán y copiarán en la carpeta compartida que haya especificado.

A continuación, configure el objeto de directiva de grupo de Windows. Para obtener más información sobre cómo hacerlo, consulte "Configurar el objeto de directiva de grupo" (p. 135).

Configurar el objeto de directiva de grupo

En este procedimiento, utilizará los paquetes de instalación que ha creado en "Creación del archivo de transformación y extracción de los paquetes de instalación" (p. 135) para configurar un objeto de directiva de grupo (GPO). El GPO implementará los agentes en los equipos de su dominio.

Pasos para configurar el objeto de directiva de grupo

© Acronis International GmbH, 2003-2025

1. Inicie sesión en el controlador de dominio como un administrador de dominio.

   Si el dominio tiene más de un controlador de dominio, conéctese a cualquiera de ellos como un administrador de dominio.
2. [Si implementa agentes en una unidad organizativa] Asegúrese de que la unidad organizativa en la que quiera implementar los agentes existe en el dominio.
3. En el menú **Inicio** de Windows, seleccione **Herramientas administrativas** y haga clic en **Gestión de directivas de grupo** (o en **Equipos y usuarios de Active Directory** si usa Windows Server 2003).
4. [En Windows Server 2008 y versiones posteriores] Haga clic con el botón derecho del ratón en el nombre del dominio o de la unidad organizativa y haga clic en **Crear un GPO en este dominio y vincularlo aquí**.
5. [En Windows Server 2003] Haga clic con el botón derecho en el nombre del dominio o de la unidad organizativa y después haga clic en **Propiedades**. En el cuadro de diálogo, haga clic en la pestaña **Directiva de grupo** y después en **Nueva**.
6. Llame al nuevo objeto de directiva de grupo **Agente para Windows.**
7. Abra el objeto de directiva de grupo de **Agente para Windows** para editarlo:
   - [En Windows Server 2008 y versiones posteriores] En **Objetos de directiva de grupo**, haga clic con el botón derecho en el objeto de directiva de grupo y, a continuación, haga clic en **Editar**.
   - [En Windows Server 2003] Haga clic en el objeto de directiva de grupo y, a continuación, en **Editar**.
8. En el complemento del editor de objeto de directiva de grupo, expanda **Configuración del equipo**.
9. [En Windows Server 2012 y versiones posteriores] Amplíe **Directivas** > **Configuración de software**.
10. [En Windows Server 2003 y Windows Server 2008] Amplíe **Configuración de software**.
11. Haga clic con el botón derecho en **Instalación de software**, seleccione **Nueva** y haga clic en **Paquete**.
12. Seleccione el paquete de instalación .msi del agente en la carpeta compartida que ha creado y haga clic en **Abrir**.
13. En el cuadro de diálogo **Implementar software**, haga clic en **Avanzado** y después en **Aceptar**.
14. En la pestaña **Modificaciones**, haga clic en **Agregar** y seleccione el archivo .mst en la carpeta compartida que ha creado.
15. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Implementar software**.

© Acronis International GmbH, 2003-2025

Despliegue de dispositivos virtuales

Implementación de Agente para VMware (dispositivo virtual)

Antes de empezar

Requisitos del sistema para el agente

De forma predeterminada, se asignan al dispositivo virtual 4 GB de RAM y 2 vCPU, que son óptimos y suficientes para llevar a cabo la mayoría de las operaciones.

Para mejorar el rendimiento de copia de seguridad y evitar fallos relacionados con la memoria RAM insuficiente, le recomendamos que aumente estos recursos a 16 GB de RAM y 4 vCPU en los casos que sean más exigentes. Por ejemplo, aumente los recursos asignados cuando espere que la transferencia de datos de la copia de seguridad exceda los 100 MB por segundo (por ejemplo, en redes de 10 Gigabit) o si realiza una copia de seguridad de varias máquinas virtuales simultáneamente con discos duros grandes (500 GB o más).

Las unidades de disco virtual del propio dispositivo no ocupan más de 6 GB. No importa si el formato del disco es ligero o denso, ya que esto no afecta al rendimiento del dispositivo.

¿Cuántos agentes necesito?

Aunque un dispositivo virtual puede proteger todo un entorno vSphere, lo mejor es implementar un dispositivo virtual por clúster vSphere (o por host, si no hay clústeres). Esto provoca que las copias de seguridad sean más rápidas porque el dispositivo puede adjuntar los discos de los que se ha realizado la copia mediante el transporte HotAdd y, por tanto, la transferencia de datos de la copia de seguridad se dirige desde un disco local a otro.

Es normal usar tanto el dispositivo virtual como el agente para VMware (Windows) a la vez, siempre que estén conectados al mismo vCenter Server *o* a diferentes hosts ESXi. Evite los casos en los que un agente se conecte a un ESXi directamente y otro se conecte al vCenter Server que gestione este ESXi.

No le recomendamos usar un almacenamiento conectado localmente (es decir, almacenar copias de seguridad en discos virtuales añadidos al dispositivo virtual) si tiene más de un agente. Para obtener más detalles, consulte "Utilización de almacenamiento conectado localmente" (p. 964).

Deshabilitar el DRS automático para el agente

Si el dispositivo virtual se implementa en un clúster vSphere, asegúrese de deshabilitar el vMotion automático. En la configuración del clúster de DRS, habilite los niveles de automatización del equipo virtual individual y, a continuación, establezca la opción **Nivel de automatización** del dispositivo virtual en **Deshabilitado**.

© Acronis International GmbH, 2003-2025

Implementación de la plantilla OVF

1. Haga clic en **Todos los dispositivos** > **Agregar** > **Broadcom (VMware) ESXi** > **Virtual Appliance (OVF)**.
   El archivo .zip se descarga en su equipo.
2. Descomprima el archivo .zip. La carpeta contiene un archivo .ovf y tres archivos .vmdk.
3. Asegúrese de que se puede acceder a estos archivos desde el equipo que ejecuta vSphere Client.
4. Abra vSphere Client e inicie sesión en vCenter Server.
5. Implemente la plantilla de OVF.
   - Al configurar el almacenamiento, seleccione el almacén de datos compartido si existe. No importa si el formato del disco es ligero o denso, ya que esto no afecta al rendimiento del dispositivo.
   - Al configurar las conexiones de red, asegúrese de seleccionar una red que permita la conexión a Internet, para que el agente pueda registrarse adecuadamente en la nube.

Configuración del dispositivo virtual

Después de implementar el dispositivo virtual, debe configurarlo de modo que pueda acceder al host de vCenter Server o ESXi y al servicio de Cyber Protection.

Para configurar la aplicación virtual

1. En vSphere Client, abra la consola del dispositivo virtual.
2. Asegúrese de que se ha configurado la conexión de red.
   La conexión se configura automáticamente con el Protocolo de configuración dinámica de host (DHCP).
   Para cambiar la configuración predeterminada, en **Opciones del agente**, en el campo **eth0**, haga clic en **Modificar** y especifique las configuraciones de red.
3. Conecte el dispositivo virtual al host de vCenter Server o ESXi.
   a. En **Opciones del agente**, en el campo **vCenter/ESX(i)**, haga clic en **Modificar** y especifique lo siguiente:
      - [Si utiliza vCenter Server] El nombre o la dirección IP de vCenter Server.
      - [Si no utiliza un vCenter Server] El nombre o la dirección IP del host ESXi cuyas máquinas virtuales desea incluir en la copia de seguridad y recuperar. Para copias de seguridad más rápidas, implemente el dispositivo virtual en el mismo host.
      - Las credenciales necesarias para que el dispositivo se conecte al host de vCenter Server o ESXi.
        Recomendamos que utilice una cuenta dedicada para acceder al servidor vCenter o al host ESXi, en lugar de usar una cuenta existente con el rol de Administrador. Para obtener más información, consulte "Privilegios necesarios para el agente para VMware" (p. 971).

© Acronis International GmbH, 2003-2025

b. Haga clic en **Verificar la conexión** para asegurarse de que la configuración es correcta.

c. Haga clic en **Aceptar**.

4. Registre el dispositivo en el servicio de Cyber Protection mediante uno de los siguientes métodos.

   - Registre el dispositivo en su interfaz gráfica.

     a. En **Opciones del agente**, en el campo **Servidor de gestión**, haga clic en **Modificar**.

     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.

     Aparecerá la dirección del servicio Cyber Protect. No cambie esta dirección a menos que se le indique lo contrario.

     c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta de Cyber Protect. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.

     d. [Solo si la autenticación de dos factores está habilitada] Introduzca la contraseña de un solo uso de su app de autenticación y haga clic en **Aceptar**.

     e. Haga clic en **Aceptar**.

   - Registre el dispositivo en la interfaz de la línea de comandos.

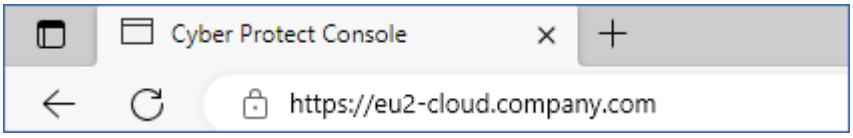
     Nota
     Con este método, necesita un token de registro. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112).

     a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.

     b. Ejecute el siguiente comando:

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

     Nota
     Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión** en la consola de Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.

     No utilice `https://cloud.company.com` aquí.

     c. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

5. [Opcional] Añada almacenamiento de copia de seguridad local al dispositivo virtual.

   a. En su entorno de máquina virtual, seleccione el dispositivo virtual y, a continuación, abra su configuración para ajustarla.

   b. Agregue un nuevo disco duro al dispositivo virtual.

© Acronis International GmbH, 2003-2025

La capacidad del disco debe ser de al menos 10 GB.

Advertencia.
Si utiliza un disco que contiene datos, se eliminarán los datos.

c. En su entorno de máquina virtual, abra la consola del dispositivo virtual.

d. En **Almacenamientos locales**, haga clic en **Actualizar**.
Se activará el botón **Crear almacenamiento**.

e. Haga clic en **Crear almacenamiento** y, a continuación, seleccione el disco que agregó al dispositivo virtual.
- Seleccione una letra de unidad.
- [Opcional] Especifique una etiqueta de disco.
La longitud de la etiqueta está limitada a 16 caracteres debido a las restricciones del sistema de archivos.

f. Haga clic en **Aceptar**.

g. Haga clic en **Sí**.

6. [Si hay un servidor proxy habilitado en la red] Configure el servidor proxy.

a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.

b. Abra el archivo **/etc/Acronis/Global.config** en un editor de texto.

c. Realice uno de los siguientes procedimientos:
- Si especificó la configuración del servidor proxy durante la instalación del agente, busque la sección siguiente:

```
<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>
```

- En caso contrario, copie les líneas anteriores y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.

d. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.

e. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` Y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.

f. Guarde el archivo.

g. Abra el archivo **/opt/acronis/etc/aakore.yaml** en un editor de texto.

h. Busque la sección **env** o créela y añada las siguientes líneas:

© Acronis International GmbH, 2003-2025

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

i. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.

j. Ejecute el comando de `reboot`.

Nota

Para poder actualizar un dispositivo virtual desplegado detrás de un proxy, edite el archivo del dispositivo `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`). Para ello, añada la siguiente línea al final del archivo e introduzca los valores específicos para su entorno:

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

Por ejemplo:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Implementación de Agent para Scale Computing HC3 (dispositivo virtual)

Antes de empezar

Este dispositivo es un equipo virtual preconfigurado que se implementa en el clúster de Scale Computing HC3. Contiene un agente de protección que le permite administrar la ciberprotección de todos los equipos virtuales del clúster.

Requisitos del sistema para el agente

De forma predeterminada, la máquina virtual que contiene el agente utiliza 2 vCPU y 4 GB de RAM. Esta configuración es suficiente para la mayoría de operaciones, pero puede cambiarla al editar la máquina virtual en la interfaz web de Scale Computing HC3.

Para mejorar el rendimiento de copia de seguridad y evitar fallos relacionados con la memoria RAM insuficiente, le recomendamos que aumente estos recursos a 4 vCPU y 8 GiB de RAM en los casos que sean más exigentes. Por ejemplo, aumente los recursos asignados cuando espere que la transferencia de datos de la copia de seguridad exceda los 100 MB por segundo (por ejemplo, en redes de 10 Gigabit) o si realiza una copia de seguridad de varias máquinas virtuales simultáneamente con discos duros grandes (500 GB o más).

El tamaño del disco virtual del dispositivo es de alrededor de 9 GB.

© Acronis International GmbH, 2003-2025

¿Cuántos agentes necesito?

Un agente puede proteger todo el clúster. Sin embargo, puede tener más de un agente en el clúster si necesita distribuir la carga del ancho de banda del tráfico de copias de seguridad.

Si tiene más de un agente en un clúster, las máquinas virtuales se distribuyen automáticamente entre ellos de forma equitativa, de modo que cada agente gestione un número similar de máquinas.

La redistribución automática se realiza cada vez que un desequilibrio de cargas entre los agentes llega al 20 por ciento. Esto puede suceder al añadir o eliminar una máquina o un agente. Por ejemplo, se da cuenta que necesita más agentes para ayudar al rendimiento e implementa un dispositivo virtual adicional en el clúster. El servidor de gestión asignará los equipos más adecuados al nuevo agente. La carga de los agentes anteriores se reducirá. Cuando retira un agente del servidor de gestión, las máquinas asignadas al agente se redistribuyen entre los agentes restantes. Sin embargo, esto no sucederá si un agente se daña o elimina manualmente del clúster de Scale Computing HC3. La redistribución comenzará solo después de eliminar dicho agente de la consola de Cyber Protect.

Pasos para comprobar qué agente gestiona una máquina específica

1. En la consola de Cyber Protect, haga clic en **Dispositivos** y, a continuación, seleccione **Scale Computing**.
2. Haga clic en el icono de engranaje en la esquina superior derecha de la tabla y, en la sección **Sistema**, seleccione la casilla de verificación **Agente**.
3. Compruebe el nombre del agente en la columna que aparezca.

Implementación de la plantilla de QCOW2

1. Inicie sesión en su cuenta de Cyber Protection.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar** > **Scale Computing HyperCore**. El archivo .zip se descarga en su equipo.
3. Descomprima el archivo .zip y guarde los archivos .qcow2 y .xml en una carpeta llamada **ScaleAppliance**.
4. Cargue la carpeta **ScaleAppliance** en un recurso compartido de red y asegúrese de que el clúster de Scale Computing HC3 tenga acceso a ella.
5. Inicie sesión en el clúster de Scale Computing HC3 como un administrador con el rol **Crear/editar máquina virtual** asignado. Para obtener más información sobre los roles necesarios para las operaciones con las máquinas virtuales de Scale Computing HC3, consulte "Agent para Scale Computing HC3: roles obligatorios" (p. 146).
6. En la interfaz web de Scale Computing HC3, importe la plantilla de la máquina virtual desde la carpeta **ScaleAppliance**.
   a. Haga clic en el icono **Importar máquina virtual de HC3**.
   b. En la ventana **Importar máquina virtual de HC3**, especifique lo siguiente:

© Acronis International GmbH, 2003-2025

- Un nombre para el nuevo equipo virtual.
- El recurso compartido de red en el que se encuentra la carpeta **ScaleAppliance**.
- El nombre de usuario y la contraseña necesarios para acceder al recurso compartido de red.
- [Opcional] Una etiqueta de dominio para la nueva máquina virtual.
- La ruta a la carpeta **ScaleAppliance** en el recurso compartido de red.

c. Haga clic en **Importar**.

Cuando se complete la implementación, configure el dispositivo virtual. Para obtener más información sobre cómo hacerlo, consulte "Configuración del dispositivo virtual" (p. 143).

Nota
Si necesita más de un dispositivo virtual en su clúster, repita los pasos anteriores e implemente dispositivos virtuales adicionales. No clone un dispositivo virtual existente mediante la opción **Clonar máquina virtual** de la interfaz web de Scale Computing HC3.

Configuración del dispositivo virtual

Después de implementar el dispositivo virtual, debe configurarlo de modo que pueda alcanzar tanto el clúster de Scale Computing HC3 que protegerá como el servicio Cyber Protection.

Para configurar la aplicación virtual

1. Inicie sesión en su cuenta de Scale Computing HC3.
2. Seleccione el dispositivo virtual que necesite configurar y haga clic en el icono **Consola**.
3. En el campo **eth0**, configure las interfaces de red del dispositivo.
   Asegúrese de que las direcciones DHCP asignadas automáticamente (de haberlas) sean válidas dentro de las redes que utiliza su máquina virtual, o bien asígnelas de forma manual. Puede haber una o más interfaces para configurar, en función del número de redes que utilice el dispositivo.
4. En el campo **Scale Computing**, haga clic en **Modificar** para especificar la dirección del clúster de Scale Computing HC3 y las credenciales para acceder a él.
   a. En el campo **Nombre del servidor o IP**, escriba el nombre DNS o la dirección IP del clúster.
   b. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de la cuenta de administrador de Scale Computing HC3.
      Asegúrese de que esta cuenta tiene los roles necesarios para realizar operaciones con máquinas virtuales Scale Computing HC3. Para obtener más información sobre estos roles, consulte "Agent para Scale Computing HC3: roles obligatorios" (p. 146).
   c. Haga clic en **Verificar la conexión** para asegurarse de que la configuración es correcta.
   d. Haga clic en **Aceptar**.
5. Registre el dispositivo en el servicio de Cyber Protection mediante uno de los siguientes métodos.

© Acronis International GmbH, 2003-2025

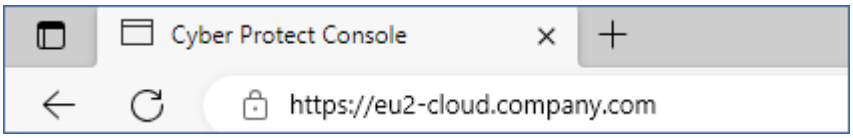
- Registre el dispositivo en su interfaz gráfica.
  a. En **Opciones del agente**, en el campo **Servidor de gestión**, haga clic en **Modificar**.
  b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.
     Aparecerá la dirección del servicio Cyber Protect. No cambie esta dirección a menos que se le indique lo contrario.
  c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta de Cyber Protect. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
  d. [Solo si la autenticación de dos factores está habilitada] Introduzca la contraseña de un solo uso de su app de autenticación y haga clic en **Aceptar**.
  e. Haga clic en **Aceptar**.
- Registre el dispositivo en la interfaz de la línea de comandos.

  Nota
  Con este método, necesita un token de registro. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112).

  a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
  b. Ejecute el siguiente comando:

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

  Nota
  Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión** en la consola de Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.

  No utilice `https://cloud.company.com` aquí.

  c. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

6. [Opcional] En el campo **Nombre**, haga clic en **Modificar** para editar el nombre predeterminado del dispositivo virtual, que es **localhost**. Este nombre se mostrará en la consola de Cyber Protect.
7. [Opcional] En el campo **Hora**, haga clic en **Modificar** y seleccione la zona horaria de su ubicación para asegurar que las operaciones planificadas se ejecutan en el momento apropiado.
8. [Opcional] Añada almacenamiento de copia de seguridad local al dispositivo virtual.
   a. En su entorno de máquina virtual, seleccione el dispositivo virtual y, a continuación, abra su configuración para ajustarla.
   b. Agregue un nuevo disco duro al dispositivo virtual.

© Acronis International GmbH, 2003-2025

La capacidad del disco debe ser de al menos 10 GB.

Advertencia.
Si utiliza un disco que contiene datos, se eliminarán los datos.

c. En su entorno de máquina virtual, abra la consola del dispositivo virtual.

d. En **Almacenamientos locales**, haga clic en **Actualizar**.
Se activará el botón **Crear almacenamiento**.

e. Haga clic en **Crear almacenamiento** y, a continuación, seleccione el disco que agregó al dispositivo virtual.
- Seleccione una letra de unidad.
- [Opcional] Especifique una etiqueta de disco.
  La longitud de la etiqueta está limitada a 16 caracteres debido a las restricciones del sistema de archivos.

f. Haga clic en **Aceptar**.

g. Haga clic en **Sí**.

9. [Si hay un servidor proxy habilitado en la red] Configure el servidor proxy.

a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.

b. Abra el archivo **/etc/Acronis/Global.config** en un editor de texto.

c. Realice uno de los siguientes procedimientos:
- Si especificó la configuración del servidor proxy durante la instalación del agente, busque la sección siguiente:

```
<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>
```

- En caso contrario, copie les líneas anteriores y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.

d. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.

e. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` Y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.

f. Guarde el archivo.

g. Abra el archivo **/opt/acronis/etc/aakore.yaml** en un editor de texto.

h. Busque la sección **env** o créela y añada las siguientes líneas:

© Acronis International GmbH, 2003-2025

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

i. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.

j. Ejecute el comando de `reboot`.

Nota

Para poder actualizar un dispositivo virtual desplegado detrás de un proxy, edite el archivo del dispositivo `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`). Para ello, añada la siguiente línea al final del archivo e introduzca los valores específicos para su entorno:

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

Por ejemplo:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pasos para proteger máquinas virtuales en el clúster de Scale Computing HC3

1. Inicie sesión en su cuenta de Cyber Protection.
2. Vaya a **Dispositivos** > **Scale Computing HyperCore**> <your cluster>, o busque sus equipos en **Dispositivos** > **Todos los dispositivos**.
3. Seleccione los equipos y aplíqueles un plan de protección.

Agent para Scale Computing HC3: roles obligatorios

Esta sección describe los roles necesarios para realizar operaciones con máquinas virtuales Scale Computing HC3.

Operación	Rol
Copias de seguridad de un equipo virtual	Copia de seguridad Crear/editar equipo virtual Borrar equipo virtual
Recuperación en un equipo virtual existente	Copia de seguridad Crear/editar equipo virtual Control de energía del equipo virtual Borrar equipo virtual Configuración del clúster
Recuperación en un nuevo equipo virtual	Copia de seguridad

© Acronis International GmbH, 2003-2025

	Crear/editar equipo virtual Control de energía del equipo virtual Borrar equipo virtual Configuración del clúster

Implementación del Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual)

Antes de empezar

Este dispositivo es un equipo virtual preconfigurado que se implementa en la Virtuozzo Hybrid Infrastructure. Contiene un agente de protección que le permite administrar ciberprotección a todos los equipos virtuales en un clúster de la Virtuozzo Hybrid Infrastructure.

Nota
Para garantizar que las copias de seguridad con la opción **Servicio de instantáneas de volumen (VSS) para máquinas virtuales** activada funcionen correctamente y capturen los datos en un estado coherente con la aplicación, compruebe que las herramientas de invitado de Virtuozzo están instaladas y actualizadas en las máquinas virtuales protegidas.

Requisitos del sistema para el agente

Al implementar el dispositivo virtual, puede elegir entre distintas combinaciones predefinidas de vCPU y RAM (variantes). También puede crear sus propias variantes.

La combinación de 2 vCPU y 4 GB de RAM (variante intermedia) es óptima y suficiente para llevar a cabo la mayoría de las operaciones. Para mejorar el rendimiento de copia de seguridad y evitar fallos relacionados con la memoria RAM insuficiente, le recomendamos que aumente estos recursos a 4 vCPU y 8 GB de RAM en los casos que sean más exigentes. Por ejemplo, aumente los recursos asignados cuando espere que la transferencia de datos de la copia de seguridad exceda los 100 MB por segundo (por ejemplo, en redes de 10 Gigabit) o si realiza una copia de seguridad de varias máquinas virtuales simultáneamente con discos duros grandes (500 GB o más).

¿Cuántos agentes necesito?

Un agente puede proteger todo el clúster. Sin embargo, puede tener más de un agente en el clúster si necesita distribuir la carga del ancho de banda del tráfico de copias de seguridad.

Si tiene más de un agente en un clúster, las máquinas virtuales se distribuyen automáticamente entre ellos de forma equitativa, de modo que cada agente gestione un número similar de máquinas.

La redistribución automática se realiza cada vez que un desequilibrio de cargas entre los agentes llega al 20 por ciento. Esto puede suceder al añadir o eliminar una máquina o un agente. Por ejemplo, se da cuenta que necesita más agentes para ayudar al rendimiento e implementa un

© Acronis International GmbH, 2003-2025

dispositivo virtual adicional en el clúster. El servidor de gestión asignará los equipos más adecuados al nuevo agente. La carga de los agentes anteriores se reducirá. Cuando retira un agente del servidor de gestión, las máquinas asignadas al agente se redistribuyen entre los agentes restantes. Sin embargo, esto no sucederá si un agente se daña o elimina manualmente del nodo de la Virtuozzo Hybrid Infrastructure. La redistribución comenzará solo después de eliminar dicho agente de la interfaz web de Cyber Protection.

Pasos para comprobar qué agente gestiona una máquina específica

1. En la consola de Cyber Protect, haga clic en **Dispositivos** y, a continuación, seleccione **Virtuozzo Hybrid Infrastructure**.
2. Haga clic en el icono de engranaje en la esquina superior derecha de la tabla y, en la sección **Sistema**, seleccione la casilla de verificación **Agente**.
3. Compruebe el nombre del agente en la columna que aparezca.

Limitaciones

- El dispositivo de la Virtuozzo Hybrid Infrastructure no se puede implementar de forma remota.
- No se admite la copia de seguridad compatible con la aplicación de equipos virtuales.

Configurar redes en la Virtuozzo Hybrid Infrastructure

Antes de implementar y configurar el dispositivo virtual, debe configurar sus redes en la Virtuozzo Hybrid Infrastructure.

Requisitos de red para el agente para la Virtuozzo Hybrid Infrastructure (dispositivo virtual)

- El dispositivo virtual requiere dos adaptadores de red.
- El dispositivo virtual debe estar conectado a redes Virtuozzo con los siguientes tipos de tráfico:
  - API de procesamiento
  - Realizar la copia de seguridad de VM
  - ABGW público
  - Equipo virtual público

Para obtener más información sobre la configuración de redes, consulte Requisitos de clúster de procesamiento en la documentación de Virtuozzo.

Configurar cuentas de usuario en la Virtuozzo Hybrid Infrastructure

Para configurar el dispositivo virtual, necesita una cuenta de usuario de Virtuozzo Hybrid Infrastructure.

Puede utilizar una de las siguientes cuentas:

© Acronis International GmbH, 2003-2025

- Administrador del sistema (en el dominio **Predeterminado** o en otro dominio)

  Asegúrese de que concede a esta cuenta acceso a todos los proyectos del dominio seleccionado. De esta forma, el dispositivo virtual podrá realizar copias de seguridad y recuperar todas las máquinas virtuales en todos los proyectos secundarios del dominio seleccionado.
- Administrador del proyecto

  Con esta cuenta, el dispositivo virtual podrá realizar copias de seguridad y recuperar solo las máquinas virtuales del proyecto en el que se ha creado la cuenta. El dispositivo virtual no dispondrá de información sobre otros proyectos del dominio.

Nota

Si desea proteger varios proyectos, debe desplegar un dispositivo virtual independiente para cada proyecto.

Cada dispositivo virtual debe usar una cuenta de administrador de proyecto independiente que se crea en el proyecto correspondiente. El dispositivo puede desplegarse en cualquier lugar del clúster de Virtuozzo Hybrid Infrastructure, incluso fuera del proyecto protegido.

Solo puede utilizar la cuenta de administrador de proyecto con Virtuozzo Hybrid Infrastructure 6.2 y versiones posteriores.

Consulte Capacidad multiinquilino en la documentación de Virtuozzo Hybrid Infrastructure para obtener más información sobre dominios y proyectos.

Uso de una cuenta de administrador del sistema

Con la cuenta de administrador del sistema, el dispositivo virtual puede realizar copias de seguridad y recuperar todas las máquinas virtuales en el dominio de Virtuozzo Hybrid Infrastructure.

Consulte Capacidad multiinquilino en la documentación de Virtuozzo Hybrid Infrastructure para obtener más información sobre dominios y proyectos.

Prerrequisito

- Debe poder conectarse al clúster de Virtuozzo Hybrid Infrastructure mediante la interfaz de línea de comandos de OpenStack. Para obtener más información, consulte Conexión a la interfaz de línea de comandos de OpenStack en la documentación de Virtuozzo Hybrid Infrastructure.

Pasos para utilizar la cuenta de administrador del sistema

1. Conéctese al clúster de Virtuozzo Hybrid Infrastructure mediante la interfaz de línea de comandos de OpenStack y, a continuación, ejecute el siguiente script para crear un archivo de entorno para el administrador del sistema.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Utilice el archivo de entorno para autorizar más comandos de OpenStack.

© Acronis International GmbH, 2003-2025

```
. /etc/kolla/admin-openrc.sh
```

3. Cree una cuenta de administrador en el dominio **Predeterminado**.

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <user name>
   ```

   De aquí en adelante, `<user name>` es la cuenta de Virtuozzo Hybrid Infrastructure. El dispositivo virtual usará esta cuenta para realizar copias de seguridad y recuperar las máquinas virtuales en cualquier proyecto secundario en el dominio **Predeterminado**.
4. Asigne el rol `admin` a la cuenta.

   ```
   openstack --insecure role add --domain Default --user <user name> --user-domain
   Default admin --inherited
   ```

5. [Opcional] Permitir que la cuenta acceda a dominios adicionales en Virtuozzo Hybrid Infrastructure.

   ```
   openstack --insecure role add --domain <domain name> --inherited --user <user name> -
   -user-domain Default admin
   ```

   En este caso, `<domain name>` es el dominio al que esta cuenta tendrá acceso. Si el nombre de dominio contiene espacios, encierre el nombre entre comillas.

   Repita este paso para cada dominio adicional que desee hacer accesible.
6. Compruebe los roles que se asignan a la cuenta.

   ```
   openstack --insecure role assignment list --user <user name> --names
   ```

7. [Opcional] Compruebe los roles efectivos de la cuenta.

   Los roles efectivos incluyen roles asignados, roles heredados y roles implícitos.

   ```
   openstack --insecure role assignment list --user <user name> --names --effective
   ```

Ejemplos

Concesión de acceso al dominio predeterminado

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Concesión de acceso al dominio predeterminado y a un dominio adicional

© Acronis International GmbH, 2003-2025

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
openstack --insecure role add --domain "New Domain"  --user johndoe --user-domain
Default admin --inherited
```

Comprobación de los roles asignados

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
```

```
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | New Domain  |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

En este ejemplo, las opciones `-c Role`, `-c User`, `-c Project` y `-c Domain` se utilizan para acortar la salida del comando para ajustarla a la página.

Comprobación de los roles efectivos

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
```

```
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
```


© Acronis International GmbH, 2003-2025

```
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

En este ejemplo, las opciones `-c Role`, `-c User`, `-c Project` y `-c Domain` se utilizan para acortar la salida del comando para ajustarla a la página.

Uso de una cuenta de administrador de proyecto

Con esta cuenta, el dispositivo virtual podrá realizar copias de seguridad y recuperar solo las máquinas virtuales del proyecto en el que se ha creado la cuenta. El dispositivo virtual no dispondrá de información sobre otros proyectos del dominio.

Nota
Si desea proteger varios proyectos, debe desplegar un dispositivo virtual independiente para cada proyecto.

Cada dispositivo virtual debe usar una cuenta de administrador de proyecto independiente que se crea en el proyecto correspondiente. El dispositivo puede desplegarse en cualquier lugar del clúster de Virtuozzo Hybrid Infrastructure, incluso fuera del proyecto protegido.

Solo puede utilizar la cuenta de administrador de proyecto con Virtuozzo Hybrid Infrastructure 6.2 y versiones posteriores.

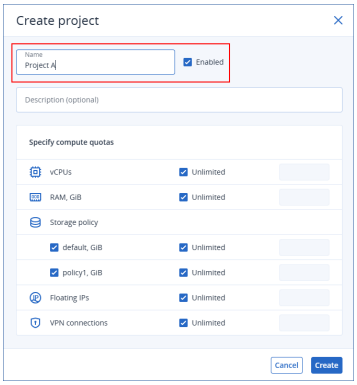
Consulte Capacidad multiinquilino en la documentación de Virtuozzo Hybrid Infrastructure para obtener más información sobre dominios y proyectos.

Prerrequisito

- Debe poder conectarse al clúster de Virtuozzo Hybrid Infrastructure mediante la interfaz de línea de comandos de OpenStack. Para obtener más información, consulte Conexión a la interfaz de línea de comandos de OpenStack en la documentación de Virtuozzo Hybrid Infrastructure.

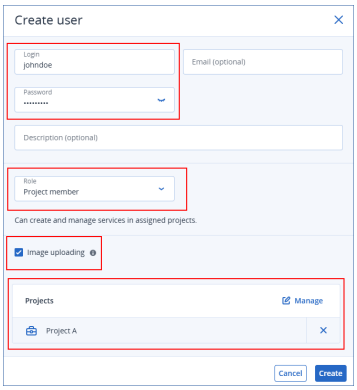
Pasos para utilizar la cuenta de administrador de proyecto

1. En el panel de administración de Virtuozzo Hybrid Infrastructure, vaya a **Configuración** > **Proyectos y usuarios**.
2. Elija un dominio y cree un proyecto en él.



© Acronis International GmbH, 2003-2025

3. En el mismo dominio, cree una cuenta de usuario. Asigne el rol de **Miembro del proyecto** a esta cuenta, seleccione la casilla de verificación **Carga de imágenes** y, a continuación, asigne el usuario al proyecto que creó.



Nota

En la interfaz de línea de comandos, el rol **Miembro del proyecto** se denomina **project_admin**.

```
+---------------+-----------------+-------+--------------------+--------+--------+-----------+
| Role          | User            | Group | Project            | Domain | System | Inherited |
+---------------+-----------------+-------+--------------------+--------+--------+-----------+
| project_admin | johndoe@Domain A |       | Project A@Domain A |        |        | False     |
| image_upload  | johndoe@Domain A |       | Project A@Domain A |        |        | False     |
+---------------+-----------------+-------+--------------------+--------+--------+-----------+
```

4. Conéctese al clúster de Virtuozzo Hybrid Infrastructure mediante la interfaz de línea de comandos de OpenStack.
   a. Ejecute el siguiente script para crear un archivo de entorno.

```
su - vstoradmin
kolla-ansible post-deploy
exit
```

   b. Utilice el archivo de entorno para autorizar más comandos de OpenStack.

```
. /etc/kolla/admin-openrc.sh
```

   c. Asigne el rol `compute` a la cuenta de usuario que creó en el panel de administración.

```
openstack --insecure role add --project <project name> --user <user name> --
project-domain <project domain name> --user-domain <user domain name> compute
```

   De aquí en adelante, `<project name>` es el nombre del proyecto, `<user name>` es la cuenta de Virtuozzo Hybrid Infrastructure, `<project domain name>` es el dominio principal del proyecto y `<user domain name>` es el dominio principal de la cuenta de usuario.

   Si un nombre contiene espacios, enciérrelo entre comillas.

   d. Asigne el rol `quota_manager` a la cuenta.

```
openstack --insecure role add --project <project name> --user <user name> --
project-domain <project domain name> --user-domain <user domain name> quota_
manager
```


© Acronis International GmbH, 2003-2025

e. Compruebe los roles que se asignan a la cuenta.

```
openstack --insecure role assignment list --names --user <user name> --user-domain
<user domain name>
```

f. [Opcional] Compruebe los roles efectivos de la cuenta.

Los roles efectivos incluyen roles asignados, roles heredados y roles implícitos.

```
openstack --insecure role assignment list --names --effective  --user <user
name> --user-domain <user domain name>
```

Ejemplos

En los ejemplos, la cuenta de usuario es `johndoe` y el proyecto es `Project A`. Tanto la cuenta de usuario como el proyecto se crean en `Domain A`.

Asignación de roles

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure role add --project "Project A" --user johndoe --project-domain
"Domain A" --user-domain "Domain A" compute
openstack --insecure role add --project "Project A" --user johndoe --project-domain
"Domain A" --user-domain "Domain A" quota_manager
```

Comprobación de los roles asignados

```
openstack --insecure role assignment list --names --user johndoe --user-domain "Domain
A" -c Role -c User -c Project -c Domain
```

```
+--------------+------------------+-------------------+-------------+
| Role         | User             | Project           | Domain      |
+--------------+------------------+-------------------+-------------+
| compute      | johndoe@Domain A | Project A@Domain A|             |
| project_admin| johndoe@Domain A | Project A@Domain A|             |
| image-upload | johndoe@Domain A | Project A@Domain A|             |
| quota_manager| johndoe@Domain A | Project A@Domain A|             |
+--------------+------------------+-------------------+-------------+
```

En este ejemplo, las opciones `-c Role`, `-c User`, `-c Project` y `-c Domain` se utilizan para acortar la salida del comando para ajustarla a la página.

Comprobación de los roles efectivos

```
openstack --insecure role assignment list --names --effective  --user johndoe --user-
domain "Domain A"  -c Role -c User -c Project -c Domain
```


© Acronis International GmbH, 2003-2025

```
+--------------+-----------------+---------------------+---------+
| Role         | User            | Project             | Domain  |
+--------------+-----------------+---------------------+---------+
| compute      | johndoe@Domain A | Project A@Domain A |         |
| project_admin| johndoe@Domain A | Project A@Domain A |         |
| image_upload | johndoe@Domain A | Project A@Domain A |         |
| quota_manager| johndoe@Domain A | Project A@Domain A |         |
| project_user | johndoe@Domain A | Project A@Domain A |         |
| member       | johndoe@Domain A | Project A@Domain A |         |
| reader       | johndoe@Domain A | Project A@Domain A |         |
+--------------+-----------------+---------------------+---------+
```

En este ejemplo, las opciones `-c Role`, `-c User`, `-c Project` y `-c Domain` se utilizan para acortar la salida del comando para ajustarla a la página.

Implementación de la plantilla de QCOW2

1. Inicie sesión en su cuenta de Cyber Protection.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar** > **Virtuozzo Hybrid Infrastructure**.
   El archivo .zip se descarga en su equipo.
3. Descomprímalo. Contiene un archivo de imagen .qcow2.
4. Inicie sesión en su cuenta de la Virtuozzo Hybrid Infrastructure.
5. Añada el archivo de imagen .qcow2 al clúster de procesamiento de la Virtuozzo Hybrid Infrastructure de la siguiente manera:
   - En la pestaña **Procesamiento** > **Equipos virtuales** > **Imágenes**, haga clic en **Añadir imagen**.
   - En la ventana **Añadir imagen**, haga clic en **Examinar** y seleccione el archivo qcow2.
   - Especifique el nombre de la imagen, seleccione el tipo **SO Linux genérico** y, a continuación, haga clic en **Agregar**.
6. En la pestaña **Procesamiento** > **Equipos virtuales** > **Equipos virtuales**, haga clic en **Crear equipo virtual**. Se abrirá una ventana en la que debe especificar los parámetros siguientes:
   - Un nombre para el nuevo equipo virtual.
   - En **Implementar desde**, escoja **Imagen**.
   - En la ventana **Imágenes**, seleccione el archivo de imagen .qcow2 del dispositivo y haga clic en **Listo**.
   - No es necesario añadir volúmenes en la ventana **Volúmenes**. El volumen que se añade de forma automática al disco del sistema es suficiente.
   - En la ventana **Variante**, elija la combinación de vCPU y RAM que desee y haga clic en **Listo**. Normalmente, basta con 2 vCPU y 4 GiB de RAM.
   - En la ventana **Interfaces de red**, haga clic en **Agregar**, seleccione la red virtual de tipo *público* y, a continuación, haga clic en **Agregar**. Aparecerá en la lista de **Interfaces de red**.

© Acronis International GmbH, 2003-2025

Si utiliza una configuración con más de una red física (y, por tanto, con más de una red virtual de tipo público), repita este paso y seleccione las redes virtuales que necesite.

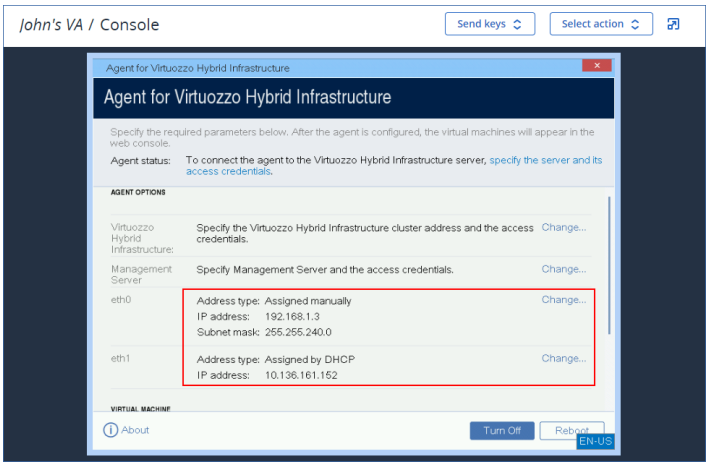
7. Haga clic en **Listo**.
8. De nuevo en la ventana **Crear equipo virtual**, haga clic en **Implementar** para crear y arrancar el equipo virtual.

Configuración del dispositivo virtual

Después de desplegar el Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual), debe configurar el dispositivo virtual para que pueda acceder tanto al clúster de Virtuozzo Hybrid Infrastructure como al servicio en la nube de Cyber Protection.

Para configurar la aplicación virtual

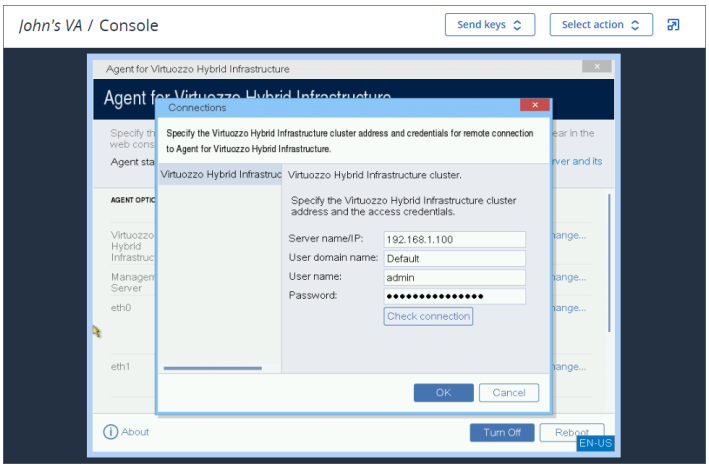
1. Inicie sesión en el panel de autoservicio de Virtuozzo Hybrid Infrastructure.
2. Vaya a **Procesamiento** > **Equipos virtuales** y seleccione la pestaña **Equipos virtuales** en el menú horizontal.
3. Haga clic en el icono de puntos suspensivos (...) junto a la máquina virtual que ha creado y, a continuación, haga clic en **Consola**.
4. Configure las interfaces de red del dispositivo. Puede que tenga que configurar una o más interfaces, en función del número de redes virtuales que utilice el dispositivo. Asegúrese de que las direcciones DHCP asignadas automáticamente (de haberlas) sean válidas dentro de las redes que utiliza su máquina virtual, o bien asígnelas de forma manual.



5. Especifique la dirección y las credenciales del clúster de Virtuozzo.
   - Nombre DNS o dirección IP del clúster de Virtuozzo Hybrid Infrastructure: esta es la dirección del nodo de administración del clúster. El puerto predeterminado (5000) se establece automáticamente. Si utiliza un puerto diferente, debe especificarlo de forma manual.
   - En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de la cuenta de usuario de Virtuozzo Hybrid Infrastructure. Puede ser una cuenta de administrador del sistema o una cuenta de administrador de proyecto. Para obtener más información sobre usuarios, roles y dominios, consulte Configuración de cuentas de usuario en Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2025

- En el campo **Nombre de dominio de usuario**, especifique el dominio principal en la cuenta de usuario. Por ejemplo, **Predeterminado**. El nombre del dominio distingue entre mayúsculas y minúsculas.



6. Registre el dispositivo en el servicio de Cyber Protection mediante uno de los siguientes métodos.
   - Registre el dispositivo en su interfaz gráfica.
     a. En **Opciones del agente**, en el campo **Servidor de gestión**, haga clic en **Modificar**.
     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.
        Aparecerá la dirección del servicio Cyber Protect. No cambie esta dirección a menos que se le indique lo contrario.
     c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta de Cyber Protect. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
     d. [Solo si la autenticación de dos factores está habilitada] Introduzca la contraseña de un solo uso de su app de autenticación y haga clic en **Aceptar**.
     e. Haga clic en **Aceptar**.
   - Registre el dispositivo en la interfaz de la línea de comandos.

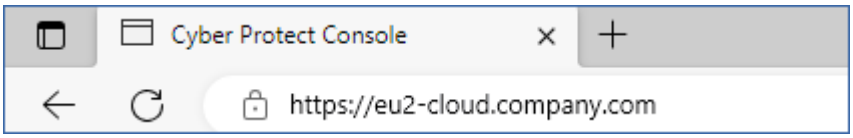
     Nota
     Con este método, necesita un token de registro. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112).

     a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
     b. Ejecute el siguiente comando:

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


© Acronis International GmbH, 2003-2025

Nota
Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión** en la consola de Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.



No utilice `https://cloud.company.com` aquí.

c. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

7. [Si hay un servidor proxy habilitado en la red] Configure el servidor proxy.
   a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
   b. Abra el archivo **/etc/Acronis/Global.config** en un editor de texto.
   c. Realice uno de los siguientes procedimientos:
      - Si especificó la configuración del servidor proxy durante la instalación del agente, busque la sección siguiente:

```
<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>
```

      - En caso contrario, copie les líneas anteriores y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.
   d. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.
   e. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` Y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.
   f. Guarde el archivo.
   g. Abra el archivo **/opt/acronis/etc/aakore.yaml** en un editor de texto.
   h. Busque la sección **env** o créela y añada las siguientes líneas:

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

   i. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.
   j. Ejecute el comando de `reboot`.

© Acronis International GmbH, 2003-2025

Nota

Para poder actualizar un dispositivo virtual desplegado detrás de un proxy, edite el archivo del dispositivo `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`). Para ello, añada la siguiente línea al final del archivo e introduzca los valores específicos para su entorno:

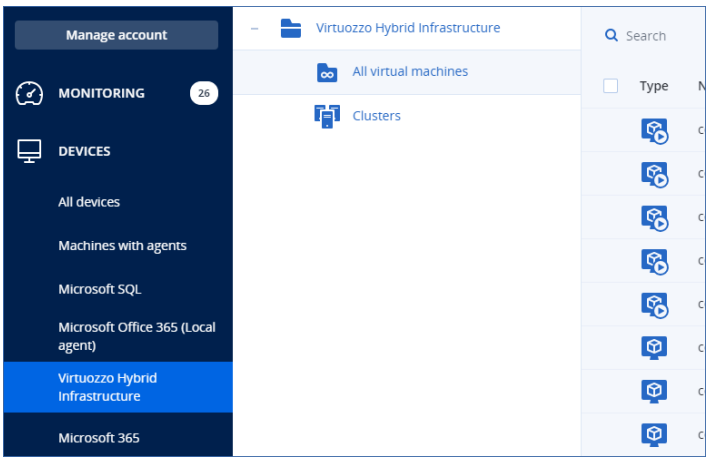
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Por ejemplo:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Cómo proteger los equipos virtuales en el clúster de la Virtuozzo Hybrid Infrastructure

1. Inicie sesión en la consola de Cyber Protection.
2. Vaya a **Dispositivos** > **Virtuozzo Hybrid Infrastructure**> <your cluster> > **Proyecto predeterminado** > **admin**, o busque su equipo en **Dispositivos** > **Todos los dispositivos**.
3. Seleccione los equipos y aplíqueles un plan de protección.



Implementando Agent para oVirt (dispositivo virtual)

Antes de empezar

Este dispositivo es una máquina virtual preconfigurada que despliega en un entorno Red Hat Virtualization/oVirt. El dispositivo contiene un agente de protección que puede realizar copias de seguridad y recuperar las máquinas virtuales del entorno.

Requisitos del sistema para el agente

De forma predeterminada, el dispositivo virtual utiliza 2 vCPU y 4 GiB de RAM. Estas configuraciones son suficientes para la mayoría de las operaciones.

Para mejorar el rendimiento de copia de seguridad y evitar fallos relacionados con una RAM insuficiente, puede aumentar el número de vCPU a cuatro y la RAM a 8 GiB en los casos que sean más exigentes. Por ejemplo, espere que la transferencia de datos de la copia de seguridad exceda

© Acronis International GmbH, 2003-2025

los 100 MB por segundo (como en las redes de 10 Gigabit) o si realiza de manera simultánea una copia de seguridad de varias máquinas virtuales con discos duros grandes (500 GiB o más).

El tamaño del disco virtual del dispositivo es de 8 GiB.

¿Cuántos agentes necesito?

Un dispositivo virtual puede realizar copias de seguridad y recuperar todas las máquinas virtuales del entorno. Puede utilizar varios dispositivos virtuales si desea distribuir la carga de ancho de banda de la transferencia de datos de la copia de seguridad.

Si se despliega más de un dispositivo virtual en el entorno, la redistribución automática de las máquinas virtuales de copia de seguridad se produce cuando el desequilibrio de carga entre los dispositivos alcanza el 20 %.

Cuando despliega un dispositivo virtual adicional, el servidor de administración asigna las máquinas virtuales más apropiadas al nuevo dispositivo, y la carga del dispositivo existente disminuye. Cuando elimina un dispositivo virtual, las máquinas virtuales de copia de seguridad se redistribuyen entre los dispositivos restantes. La redistribución solo ocurre si elimina el dispositivo virtual de la consola de Cyber Protect. La redistribución no se iniciará si elimina el dispositivo virtual del portal de administración de Red Hat Virtualization/oVirt o si el dispositivo se corrompe.

Pasos para comprobar qué agente gestiona una máquina específica

1. En la consola de Cyber Protect, haga clic en **Dispositivos** y, a continuación, seleccione **oVirt**.
2. Haga clic en el icono de engranaje en la esquina superior derecha de la tabla y, en la sección **Sistema**, seleccione la casilla de verificación **Agente**.
3. Compruebe el nombre del agente en la columna que aparezca.

Limitaciones

No se admiten las siguientes operaciones en máquinas virtuales de Red Hat Virtualization/oVirt:

- Copia de seguridad compatible con la aplicación
- Ejecución de un equipo virtual desde una copia de seguridad
- Replicación de equipos virtuales
- Seguimiento de bloqueo cambiado

Implementación de la plantilla de OVA

Puede desplegar el dispositivo virtual de oVirt creando una máquina virtual en el entorno de Red Hat Virtualization/oVirt y desplegando la plantilla QCOW que ha descargado de la consola de Cyber Protect.

Si necesita más de un dispositivo virtual en su entorno, despliegue dispositivos virtuales adicionales. No clone un dispositivo virtual existente mediante la opción **Clonar máquina virtual** del portal de administración de Red Hat Virtualization/oVirt.

© Acronis International GmbH, 2003-2025

Pasos para desplegar la plantilla de OVA

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar** > **Red Hat Virtualization (oVirt)**.
   Un archivo ZIP se descarga en su equipo.
3. Descomprima el archivo ZIP y extraiga el archivo de imagen OVA.
4. Cargue el archivo OVA a un host del entorno de Red Hat Virtualization/oVirt que desee proteger.
5. Inicie sesión como administrador en el portal de administración de Red Hat Virtualization/oVirt.
   Para obtener más información sobre los roles necesarios para las operaciones con las máquinas virtuales, consulte "Agente para oVirt: roles y puertos necesarios" (p. 165).
6. En el menú navegación, seleccione **Procesamiento** > **Equipos virtuales**.
7. Haga clic en el icono  de elipsis vertical encima de la tabla principal y, a continuación, haga clic en **Importar**.
8. En la ventana **Importar Máquinas(s) virtual(es)**, haga lo siguiente:
   a. En **Centro de datos**, seleccione el centro de datos que desea proteger.
   b. En **Origen**, seleccione **Dispositivo Virtual (OVA)**.
   c. En **Host**, seleccione el host en el que cargó el archivo OVA.
   d. En **Ruta del archivo**, especifique la ruta del directorio que contiene el archivo OVA.
   e. Haga clic en **Cargar**.
      La plantilla del dispositivo virtual oVirt del archivo OVA aparecerá en el panel **Máquinas virtuales en la fuente**.
      Si la plantilla no aparece en este panel, asegúrese de que ha especificado la ruta del archivo correcta, que el archivo no esté dañado o que no se pueda acceder al servidor.
   f. En **Máquinas virtuales en la fuente**, seleccione la plantilla del dispositivo virtual oVirt y, a continuación, haga clic en la flecha derecha.
      La plantilla aparecerá en el panel **Máquinas virtuales para importar**.
   g. Haga clic en **Siguiente**.
9. En la nueva ventana, haga clic en el nombre del dispositivo y establezca la siguiente configuración:
   - En la pestaña **Interfaces de red**, configure las interfaces de red.
   - En la pestaña **General**, cambie el nombre predeterminado de la máquina virtual con el agente.
10. [Opcional] Para ocultar el dispositivo virtual en la consola de Cyber Protect, asigne la etiqueta `acronis_virtual_appliance` al dispositivo virtual.
    Esto le impedirá aplicar accidentalmente planes de protección al propio dispositivo e incluirlo en grupos dinámicos.

El despliegue se ha completado. A continuación, debe configurar el dispositivo. Consulte "Configuración del dispositivo virtual" (p. 162).

© Acronis International GmbH, 2003-2025

Nota
Si utiliza un dispositivo virtual oVirt con Oracle Linux Virtualization Manager, puede recibir el siguiente error: "Máquina virtual <name of the virtual appliance> está inactiva con error. Mensaje de salida: configuración no compatible: la configuración de dominio no es compatible con el modelo de vídeo 'qxl'." Para resolver este error, cambie el adaptador gráfico del dispositivo virtual a **CIRRUS**. Consulte "Cambio del adaptador gráfico de un dispositivo virtual" (p. 165).

Configuración del dispositivo virtual

Después de implementar el dispositivo virtual, debe configurarlo de modo que pueda alcanzar tanto el oVirt Engine como el servicio Cyber Protection.

Para configurar la aplicación virtual

1. Inicie sesión en el Portal de administración de Red Hat Virtualization/oVirt.
2. Seleccione el dispositivo virtual que necesite configurar y haga clic en el icono **Consola**.
3. En el campo **eth0**, configure las interfaces de red del dispositivo.
   Asegúrese de que las direcciones DHCP asignadas automáticamente (de haberlas) sean válidas dentro de las redes que utiliza su máquina virtual, o bien asígnelas de forma manual. Puede haber una o más interfaces para configurar, en función del número de redes que utilice el dispositivo.
4. En el campo **oVirt**, haga clic en **Modificar** para especificar la dirección del oVirt Engine y las credenciales para acceder a él:
   a. En el campo **Nombre del servidor o IP**, escriba el nombre DNS o la dirección IP del motor.
   b. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador de este motor.
      Asegúrese de que esta cuenta de administrador cuenta con los roles necesarios para las operaciones con las máquinas virtuales de Red Hat Virtualization/oVirt. Para obtener más información sobre estos roles, consulte "Agente para oVirt: roles y puertos necesarios" (p. 165).
      Si Keycloak es el proveedor de inicio de sesión único (SSO) para el oVirt Engine (valor predeterminado en oVirt 4.5.1), use el formato de Keycloak al especificar el nombre de usuario. Por ejemplo, especifique la cuenta del administrador predeterminada como `admin@ovirt@internalsso`, en lugar de `admin@internal`.
   c. [Opcional] Haga clic en **Verificar la conexión** para asegurarse de que las credenciales proporcionadas son las correctas.
   d. Haga clic en **Aceptar**.
5. Registre el dispositivo en el servicio de Cyber Protection mediante uno de los siguientes métodos.

© Acronis International GmbH, 2003-2025

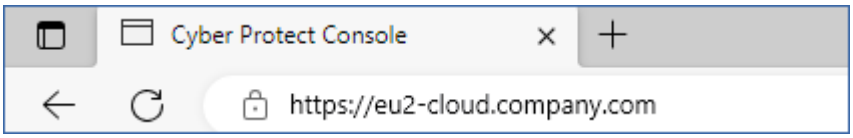
- Registre el dispositivo en su interfaz gráfica.
  a. En **Opciones del agente**, en el campo **Servidor de gestión**, haga clic en **Modificar**.
  b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.
     Aparecerá la dirección del servicio Cyber Protect. No cambie esta dirección a menos que se le indique lo contrario.
  c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta de Cyber Protect. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
  d. [Solo si la autenticación de dos factores está habilitada] Introduzca la contraseña de un solo uso de su app de autenticación y haga clic en **Aceptar**.
  e. Haga clic en **Aceptar**.
- Registre el dispositivo en la interfaz de la línea de comandos.

  Nota
  Con este método, necesita un token de registro. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112).

  a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
  b. Ejecute el siguiente comando:

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

  Nota
  Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión** en la consola de Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.

  No utilice `https://cloud.company.com` aquí.

  c. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

6. [Opcional] En el campo **Nombre**, haga clic en **Modificar** para editar el nombre predeterminado del dispositivo virtual, que es **localhost**. Este nombre se mostrará en la consola de Cyber Protect.
7. [Opcional] En el campo **Hora**, haga clic en **Modificar** y seleccione la zona horaria de su ubicación para asegurar que las operaciones planificadas se ejecutan en el momento apropiado.
8. [Opcional] [Si hay un servidor proxy habilitado en la red] Configure el servidor proxy.
   a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
   b. Abra el archivo **/etc/Acronis/Global.config** en un editor de texto.

© Acronis International GmbH, 2003-2025

c. Realice uno de los siguientes procedimientos:
   - Si especificó la configuración del servidor proxy durante la instalación del agente, busque la sección siguiente:

```
<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>
```

   - En caso contrario, copie les líneas anteriores y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.

d. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.

e. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` Y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.

f. Guarde el archivo.

g. Abra el archivo **/opt/acronis/etc/aakore.yaml** en un editor de texto.

h. Busque la sección **env** o créela y añada las siguientes líneas:

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

i. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.

j. Ejecute el comando de `reboot`.

Nota

Para poder actualizar un dispositivo virtual desplegado detrás de un proxy, edite el archivo del dispositivo `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`). Para ello, añada la siguiente línea al final del archivo e introduzca los valores específicos para su entorno:

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

Por ejemplo:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Pasos para proteger las máquinas virtuales del centro de datos de Red Hat Virtualization/oVirt

1. Inicie sesión en su cuenta de Cyber Protection.
2. Vaya a **Dispositivos** > **oVirt**> <your cluster>, o busque sus máquinas en **Dispositivos** > **Todos**

© Acronis International GmbH, 2003-2025

los dispositivos.

3. Seleccione los equipos y aplíqueles un plan de protección.

Cambio del adaptador gráfico de un dispositivo virtual

Si utiliza un dispositivo virtual oVirt con Oracle Linux Virtualization Manager, puede recibir el siguiente error: "La máquina virtual <name of the virtual appliance> está inactiva con error. Mensaje de salida: configuración no compatible: la configuración de dominio no es compatible con el modelo de vídeo 'qxl'."

Para resolver este error, cambie el adaptador gráfico del dispositivo virtual a **CIRRUS**.

Pasos para cambiar el adaptador gráfico de un dispositivo virtual

1. Inicie sesión en el portal de administración de Oracle Linux como administrador.
2. Vaya a **Cálculo** > **Equipos virtuales**.
3. [Si el dispositivo virtual está encendido] Haga clic con el botón derecho en el dispositivo virtual y, a continuación, seleccione **Apagar**.
4. Haga clic con el botón derecho en el dispositivo virtual y, a continuación, seleccione **Editar**.
5. [Si solo ve la pestaña **General**] Haga clic en **Mostrar opciones avanzadas**.
6. Haga clic en **Consola**.
7. En **Consola gráfica**, para **Tipo de Vídeo**, seleccione **CIRRUS**.
8. Haga clic en **Aceptar**.
9. En el portal de administración de Oracle Linux, encienda el dispositivo virtual.

Agente para oVirt: roles y puertos necesarios

Roles necesarios

Para implementar y operar el Agente para oVirt, es necesaria una cuenta de administrador con los siguientes roles asignados.

oVirt/Red Hat Virtualization 4.2 y 4.3/Oracle Virtualization Manager 4.3

- Creador de disco
- Administrador del usuario de la máquina virtual
- Administrador de etiquetas
- Administrador del tiempo de ejecución del usuario de la máquina virtual
- Creador de la máquina virtual

oVirt/Red Hat Virtualization 4.4 y 4.5

- Superusuario

© Acronis International GmbH, 2003-2025

Puertos necesarios

El Agente para oVirt se conecta al oVirt Engine mediante la URL que especifique al configurar el dispositivo virtual. Por lo general, la URL del motor tiene el siguiente formato: `https://ovirt.company.com`. En este caso, se utilizan el protocolo HTTPS y el puerto 443.

La configuración no predeterminada de oVirt puede necesitar otro puerto. Puede encontrar el puerto exacto mediante el análisis del formato de la URL. Por ejemplo:

URL de oVirt Engine	Puerto	Protocolo
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

No se necesitan puertos adicionales para las operaciones de lectura o escritura del disco porque la copia de seguridad se ha llevado a cabo en el modo HotAdd.

Despliegue del agente para Azure

Puede realizar una copia de seguridad sin agente de máquinas virtuales de Microsoft Azure al configurar el agente para Azure, un único agente que puede acceder a los datos de máquinas virtuales de Microsoft Azure de forma transparente.

El agente para Azure asegura lo siguiente:

- Funciones de copia de seguridad y restauración para máquinas virtuales de Microsoft Azure que funcionan con Windows o Linux.
- Reducción de los costes generales de la máquina virtual de Microsoft Azure, con un único agente para gestionar.
- Migración transparente de cualquier copia de seguridad de equipos locales o de la nube a máquinas virtuales de Microsoft Azure, configurable a través de la consola de Cyber Protect.
- Costes de recursos de Microsoft Azure reducidos, con sobrecargas de CPU y RAM para un único agente dentro de la máquina virtual.

Antes de empezar

Requisitos del sistema para el agente

De forma predeterminada, se asigna el tamaño **Standard_B2s** (4 GiB de RAM y 2 CPU) al dispositivo virtual, que es óptimo y suficiente para operaciones con hasta diez máquinas virtuales respaldadas en paralelo. Para mejorar el rendimiento de la copia de seguridad y evitar fallos relacionados con insuficiente memoria RAM, le recomendamos que cambie el tamaño del dispositivo virtual (tamaño en Azure) para obtener 4 vCPU y 8 GB de RAM en casos más exigentes. Por ejemplo, aumente los recursos asignados cuando realice copias de seguridad de más de diez máquinas virtuales en

© Acronis International GmbH, 2003-2025

paralelo o si realiza copias de seguridad simultáneamente de varias máquinas virtuales con discos duros grandes (500 GB o más).

Para obtener más información sobre esta y otras propiedades de máquinas virtuales de Azure, consulte la documentación de Microsoft Azure.

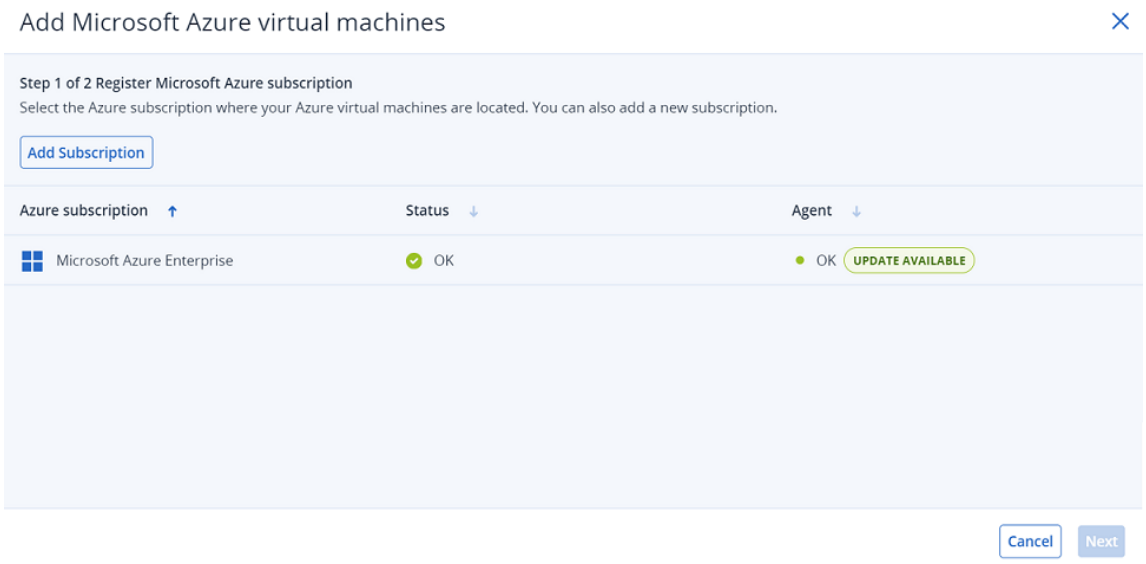
Despliegue del agente para el dispositivo virtual de Azure

Despliegue el dispositivo virtual del agente para Azure conectándose primero a la suscripción de Microsoft Azure correspondiente y, a continuación, definiendo la configuración de despliegue de Azure.

Nota
Se puede configurar la conexión a una suscripción de Microsoft Azure al crear una ubicación de copia de seguridad a través del menú **Dispositivos** o **Almacenamiento de la copia de seguridad**, tal y como se describe en "Definir una ubicación de copia de seguridad en Microsoft Azure" (p. 734).

Pasos para desplegar el dispositivo virtual del agente para Azure

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los equipos**.
2. Haga clic en **Agregar**.
3. En la sección **Cargas de trabajo en la nube**, seleccione **Máquinas virtuales de Microsoft Azure**.
   - Si tiene suscripciones de Microsoft Azure en uso, se mostrará el Asistente para añadir máquinas virtuales de Microsoft Azure, con sus suscripciones enumeradas. Puede seleccionar la suscripción correspondiente y hacer clic en **Siguiente**. Luego, continúe con el paso 8.



   - Si ya tiene suscripciones de Microsoft Azure en uso pero desea añadir una nueva, haga clic en **Añadir suscripción**.
   - Si no tiene suscripciones, haga clic en **Agregar** para añadir una suscripción.

© Acronis International GmbH, 2003-2025

4. En el diálogo mostrado, haga clic en **Iniciar sesión**. Se le redirigirá a la página de inicio de sesión de Microsoft.

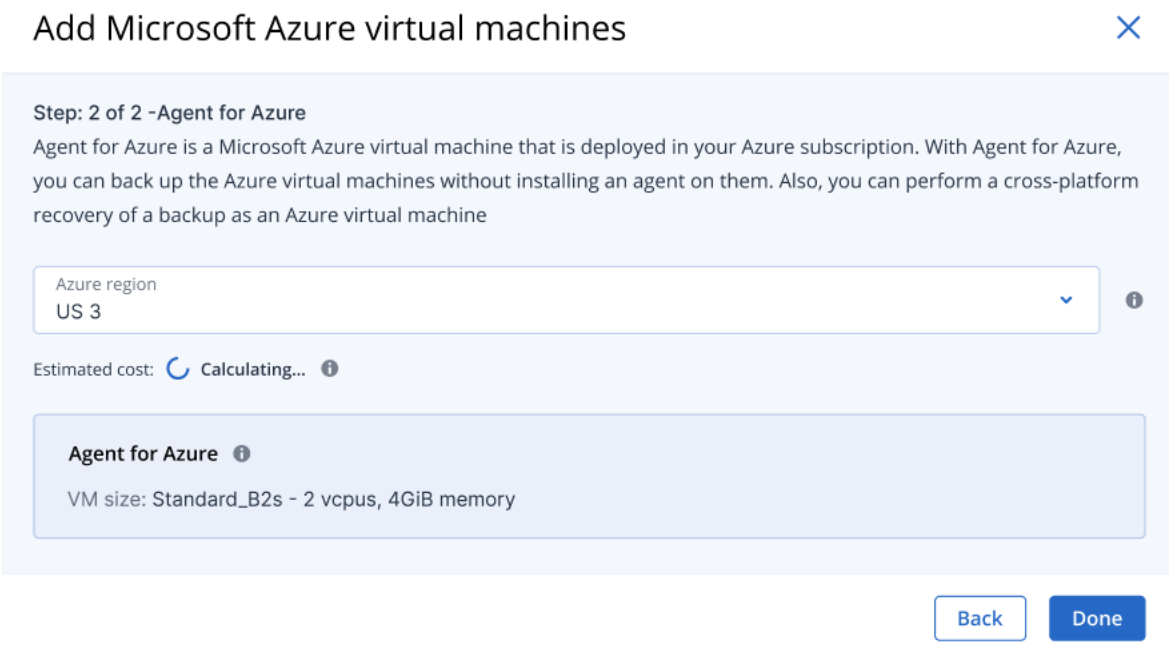
   Nota
   Debe tener asignado uno de los siguientes roles en Microsoft Entra ID para poder completar la conexión con la suscripción: Administrador de aplicaciones en la nube, administrador de aplicaciones o administrador general. También debe tener asignado el rol Propietario para cada suscripción seleccionada.

5. Introduzca las credenciales de inicio de sesión de Microsoft y acepte los permisos solicitados. Se iniciará el proceso de conexión y puede tardar varios minutos.

   Para obtener más información sobre el acceso seguro a su suscripción de Microsoft Azure, consulte el artículo Auditoría y seguridad de conexión de Microsoft Azure (72684).

6. Una vez completada la recuperación:
   - Si tiene varias suscripciones, seleccione la suscripción correspondiente en la lista desplegable del diálogo mostrada y haga clic en **Añadir suscripción**. A continuación, se redirigirá a la pantalla principal del asistente.
   - Si va a añadir su primera suscripción, se le redirigirá a la pantalla principal del asistente.
7. Seleccione la suscripción correspondiente y haga clic en **Siguiente**.
8. En la lista desplegable **Región de Azure**, seleccione la región correspondiente a la suscripción. Debe seleccionar una región de Azure en la que se despliega la mayoría de las máquinas virtuales que se desea proteger para optimizar el rendimiento de la copia de seguridad.

   Se calculará y mostrará el coste estimado de la región. Estos costes se cargarán en su suscripción de Microsoft Azure y se facturarán a través de Microsoft.



© Acronis International GmbH, 2003-2025

Nota
El agente para Azure desplegado utiliza el tamaño Standard_B2s.

9. Haga clic en **Listo**.
   Se le redirige a la pantalla **Dispositivos** > **Microsoft Azure**, donde se muestra el progreso del despliegue. Cuando se complete, puede comenzar a definir planes de protección con la suscripción recién añadida.
   Para obtener más información acerca de las opciones de copia de seguridad y recuperación de Microsoft Azure, consulte "Puntos de restauración de Azure" (p. 593) y "Recuperación del equipos virtuales" (p. 678).

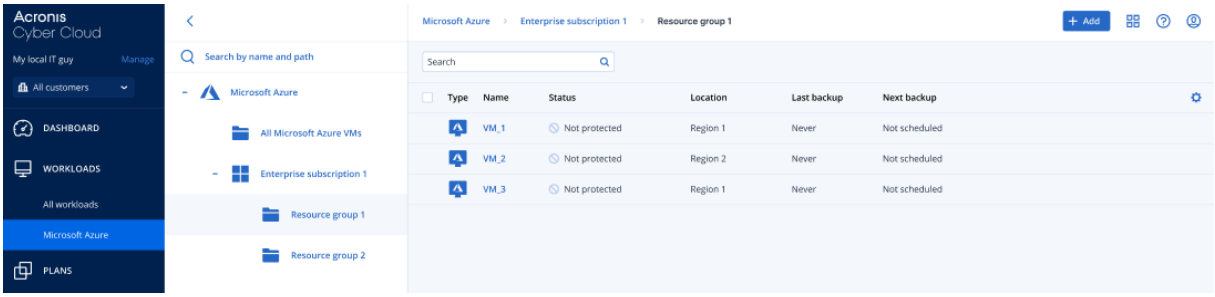
Visualización y actualización de un agente para Azure desplegado

Puede ver y actualizar su despliegue de agente para Azure de las siguientes maneras:

- Vea los despliegues actuales a través del menú **Dispositivos > Microsoft Azure**.
- Vea, actualice, acceda y vuelva a desplegar los despliegues actuales a través del menú **Infraestructura > Nubes públicas**.

Pasos para ver los despliegues actuales a través del menú de Microsoft Azure

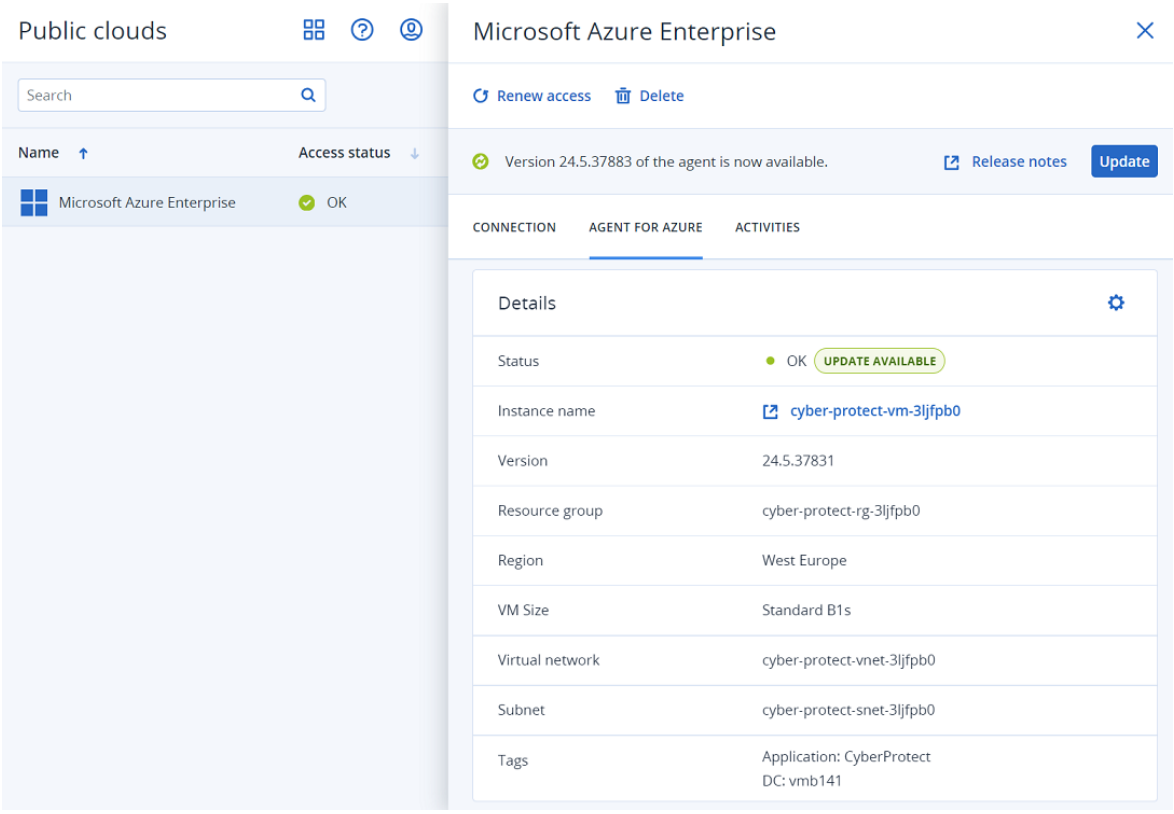
En la consola de Cyber Protect, vaya a **Dispositivos > Microsoft Azure**. Se mostrará la lista actual de los despliegues de agente para Azure. Tenga en cuenta que cada suscripción de la lista muestra los grupos de recursos pertinentes debajo de ella en el árbol jerárquico.



Pasos para ver y actualizar los despliegues actuales a través del menú Infraestructura > Nubes públicas

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
   Se muestra la lista actual de las conexiones de nube pública.
2. Seleccione la suscripción de Microsoft Azure en la que se despliega el agente para Azure.
3. En el panel de la derecha, haga clic en la pestaña **Agente para Azure**.

© Acronis International GmbH, 2003-2025



4. Puede:
   - Vea el estado actual del despliegue.
   - Haga clic en el vínculo del campo **Nombre de la instancia** para acceder a la instancia donde se desplegó el agente para Azure. Tenga en cuenta que deberá haber iniciado sesión en su cuenta de Microsoft Azure para acceder a la instancia.
   - Haga clic en ⚙ para volver a desplegar el agente para Azure.
   - Haga clic en **Actualizar** si hay una actualización disponible.

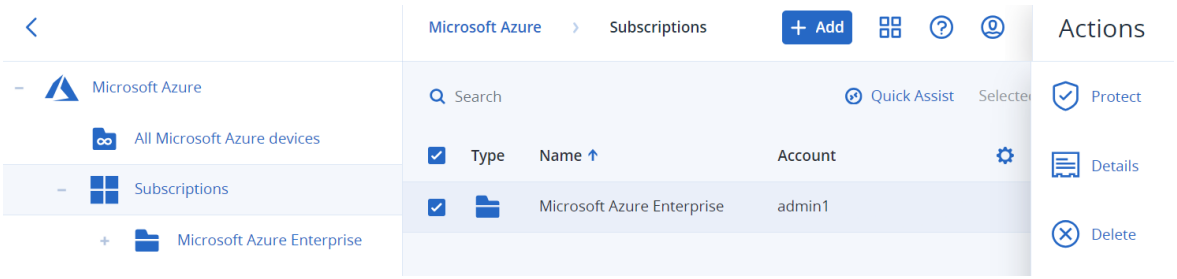
Cómo quitar el agente para dispositivo virtual de Azure

El dispositivo virtual del agente para Azure se elimina automáticamente cuando elimina la suscripción correspondiente de Microsoft Azure.

Pasos para eliminar el dispositivo virtual de agente para Azure

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Microsoft Azure**.
2. Haga clic en el nodo **Suscripciones** del árbol jerárquico y después seleccione la suscripción correspondiente de la lista que se muestra a la derecha.

© Acronis International GmbH, 2003-2025



3. En el panel derecho, haga clic en **Eliminar**.
4. Haga clic en **Eliminar** en el diálogo de confirmación que se muestra.
   Cuando se elimina la suscripción, el dispositivo virtual del agente para Azure se desaprovisiona y no utiliza los recursos de Microsoft Azure.

Nota
No puede eliminar una suscripción si se está utilizando en máquinas virtuales de Microsoft Azure.

Despliegue de Agente para Nutanix AHV

Antes de empezar

Este dispositivo es una máquina virtual preconfigurada que puede desplegar en un clúster de Nutanix. El dispositivo contiene un agente de protección que puede realizar copias de seguridad y recuperar las máquinas virtuales del clúster.

Requisitos del sistema para el dispositivo virtual

Le recomendamos que configure el dispositivo virtual con 4 vCPU (4 vCPU de un solo núcleo o 2 vCPU con 2 núcleos cada una) y 8 GiB de RAM. Estas configuraciones son suficientes para la mayoría de las operaciones.

Para mejorar el rendimiento de copia de seguridad y evitar fallos relacionados con la memoria RAM insuficiente, puede aumentarla a 16 GiB en los casos que sean más exigentes. Por ejemplo, espere que la transferencia de datos de la copia de seguridad exceda los 100 MB por segundo (como en las redes de 10 Gigabit) o si realiza una copia de seguridad de varias máquinas virtuales simultáneamente con discos duros grandes (500 GiB o más).

El tamaño del disco virtual del dispositivo es de 8 GiB.

¿Cuántos dispositivos virtuales necesito?

Un dispositivo virtual puede realizar copias de seguridad y recuperar todas las máquinas virtuales del clúster. Puede utilizar varios dispositivos virtuales por clúster si desea distribuir la carga de ancho de banda de la transferencia de datos de la copia de seguridad.

© Acronis International GmbH, 2003-2025

Si se despliega más de un dispositivo virtual en el clúster, la redistribución automática de las máquinas virtuales de copia de seguridad se produce cuando el desequilibrio de carga entre los dispositivos alcanza el 20 %.

Cuando despliega un dispositivo virtual adicional, el servidor de administración asigna las máquinas virtuales más apropiadas al nuevo dispositivo, y la carga del dispositivo existente disminuye. Cuando elimina un dispositivo virtual, las máquinas virtuales de copia de seguridad se redistribuyen entre los dispositivos restantes. La redistribución solo ocurre si elimina el dispositivo virtual de la consola de Cyber Protect. La redistribución no se iniciará si elimina el dispositivo virtual de la consola Nutanix Prism Element o si el dispositivo se corrompe.

Limitaciones

Las siguientes operaciones no son compatibles:

- Copia de seguridad compatible con la aplicación
- Ejecución de un equipo virtual desde una copia de seguridad
- Replicación de equipos virtuales
- Copias de seguridad de grupos de volúmenes de Nutanix

Implementación de la plantilla de QCOW2

Puede desplegar el dispositivo virtual de Nutanix creando una máquina virtual en el clúster de Nutanix y desplegando la plantilla QCOW que ha descargado de la consola de Cyber Protect.

Debe desplegar al menos un dispositivo virtual por clúster.

Pasos para desplegar la plantilla de QCOW2

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Agregar** > **Nutanix AHV**.
   Un archivo ZIP se descarga en su equipo.
3. Descomprima el archivo ZIP y extraiga el archivo de imagen QCOW2.
4. Inicie sesión como administrador en la consola de Nutanix Prism Element.
5. Cargue el archivo de imagen QCOW2 en la consola de Nutanix Prism Element.
   a. Vaya a **Configuración** y, a continuación, en **General**, seleccione **Configuración de imagen**.
   b. Haga clic en **Cargar imagen**.
   c. Especifique un nombre para la imagen.
   d. En **Tipo de imagen**, seleccione **Disco**.
   e. Haga clic en **Cargar un archivo** y, a continuación, en **Elegir archivo**.
   f. Seleccione la imagen de QCOW2 que ha descargado de la consola de Cyber Protect.
   g. Haga clic en **Guardar**.

© Acronis International GmbH, 2003-2025

6. En la consola de Nutanix Prism Element, cree una nueva máquina virtual utilizando la imagen QCOW2.
   a. Vaya a **Máquina virtual** y haga clic en **Crear máquina virtual**.
   b. Especifique un nombre para el máquina virtual.
   c. En **Detalles de cálculo**, especifique 4 vCPU (un núcleo) o 2 vCPU con 2 núcleos cada uno, y 8 GiB de memoria.
   d. En **Discos**, haga clic en **Agregar disco nuevo**.
   e. En **Operación**, seleccione **Clonar desde el servicio de imagen**.
   f. En **Imagen**, seleccione la imagen que ha cargado en la consola de Nutanix Prism Element.
   g. Haga clic en **Agregar**.
   h. En **Adaptadores de red (NIC)**, haga clic en **Agregar nuevo NIC**.
   i. Ajuste la configuración de red y haga clic en **Agregar**.
   j. [Opcional] Para ocultar el dispositivo virtual en la consola de Cyber Protect, en **Descripción**, especifique lo siguiente:

      ```
      {AB53A0F1-AD54-480f-80BB-FC72DC41DF53}
      ```

      Esto le impedirá aplicar accidentalmente planes de protección al propio dispositivo e incluirlo en grupos dinámicos.
   k. Haga clic en **Guardar**.
7. En la pestaña **Máquina virtual** > **Tabla**, haga clic con el botón derecho en la máquina virtual que ha creado y después seleccione **Encender**.
   Como resultado, el dispositivo virtual se desplegará y se encenderá.
   A continuación, configure dispositivo virtual. Consulte "Configuración del dispositivo virtual de Nutanix" (p. 173).

Configuración del dispositivo virtual de Nutanix

Después de desplegar el dispositivo virtual, debe configurar su acceso al clúster de Nutanix y a la consola de Cyber Protect.

Requisitos previos

- Ha desplegado y encendido el dispositivo virtual de Nutanix. Consulte "Implementación de la plantilla de QCOW2" (p. 172).

Pasos para configurar el dispositivo virtual de Nutanix

1. Inicie sesión como administrador en la consola de Nutanix Prism Element.
2. Vaya a **Máquina virtual** > **Tabla**.
3. Haga clic con el botón derecho en la máquina virtual que ha desplegado y seleccione **Lanzar consola**.
4. En el campo **eth0**, configure las interfaces de red del dispositivo.

© Acronis International GmbH, 2003-2025

Si hay direcciones DHCP asignadas automáticamente, asegúrese de que sean válidas dentro de las redes que utiliza su máquina virtual, o bien asígnelas de forma manual. Podría haber una o más interfaces para configurar, en función del número de redes que utilice el dispositivo.

5. Especifique la dirección IP del clúster de Nutanix (Nutanix Prism Element) y las credenciales para acceder a él.

   Nota
   No puede configurar el Agente para Nutanix AHV con la dirección IP de Nutanix Prism Central. Aunque gestione el clúster a través de Nutanix Prism Central, el Agente para Nutanix AHV solo puede acceder a través de Nutanix Prism Element.

   a. En **Opciones del agente**, en el campo **Nutanix**, haga clic en **Modificar**.
   b. En el campo **Nombre del servidor o IP**, escriba la dirección IP del clúster.
   c. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de una cuenta de administrador de Nutanix.
      Esta cuenta debe tener los roles de **administrador de usuario** y **administrador de clúster** en el clúster de Nutanix.
   d. Para verificar que la configuración es correcta, haga clic en **Comprobar conexión**.
   e. Haga clic en **Aceptar**.

6. Registre el dispositivo en el servicio de Cyber Protection mediante uno de los siguientes métodos.

   - Registre el dispositivo en su interfaz gráfica.
     a. En **Opciones del agente**, en el campo **Servidor de gestión**, haga clic en **Modificar**.
     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.
        Aparecerá la dirección del servicio Cyber Protect. No cambie esta dirección a menos que se le indique lo contrario.
     c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta de Cyber Protect. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
     d. [Solo si la autenticación de dos factores está habilitada] Introduzca la contraseña de un solo uso de su app de autenticación y haga clic en **Aceptar**.
     e. Haga clic en **Aceptar**.
   - Registre el dispositivo en la interfaz de la línea de comandos.

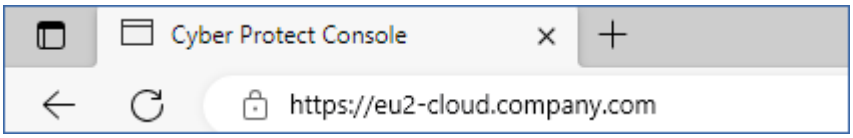
     Nota
     Con este método, necesita un token de registro. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 112).

     a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
     b. Ejecute el siguiente comando:

© Acronis International GmbH, 2003-2025

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

Nota
Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión** en la consola de Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.



No utilice `https://cloud.company.com` aquí.

c. Pulse ALT+F1 para volver a la interfaz gráfica del dispositivo.

7. [Opcional] Edite el nombre predeterminado del dispositivo virtual, que es **localhost**.
   Este nombre se mostrará en la consola de Cyber Protect.
   a. En **Máquina virtual**, en el campo **Nombre**, haga clic en **Modificar**.
   b. Edite el nombre y, a continuación, haga clic en **Aceptar**.
8. [Opcional] Establezca la zona horaria del dispositivo virtual.
   a. En **Máquina virtual**, en el campo **Zona horaria**, haga clic en **Modificar**.
   b. Para garantizar que las operaciones programadas se ejecuten en el momento correcto, seleccione la zona horaria de su ubicación.
9. [Si hay un servidor proxy habilitado en la red] Configure el servidor proxy.
   a. Presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
   b. Abra el archivo **/etc/Acronis/Global.config** en un editor de texto.
   c. Realice uno de los siguientes procedimientos:
      - Si especificó la configuración del servidor proxy durante la instalación del agente, busque la sección siguiente:

```
<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>
```

      - En caso contrario, copie les líneas anteriores y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.
   d. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.
   e. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.

© Acronis International GmbH, 2003-2025

f. Guarde el archivo.

g. Abra el archivo **/opt/acronis/etc/aakore.yaml** en un editor de texto.

h. Busque la sección **env** o créela y añada las siguientes líneas:

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

i. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.

j. Ejecute el comando de `reboot`.

Nota

Para poder actualizar un dispositivo virtual desplegado detrás de un proxy, edite el archivo del dispositivo `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`). Para ello, añada la siguiente línea al final del archivo e introduzca los valores específicos para su entorno:

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

Por ejemplo:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Cómo realizar copias de seguridad de máquinas virtuales de Nutanix

Requisitos previos

- Ha desplegado y configurado el dispositivo virtual de Nutanix.

Pasos para proteger máquinas virtuales de Nutanix

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Dispositivos** > **Nutanix** > <your cluster>.
3. Seleccione las máquinas virtuales y aplíqueles un plan de protección.

Implementar Agente para Synology

Antes de empezar

Con Agente para Synology, podrá realizar la copia de seguridad de archivos y carpetas desde dispositivos NAS de Synology y hacia estos. Se conservan las propiedades específicas de NAS y los permisos de acceso para recursos compartidos, carpetas y archivos.

El agente para Synology se ejecuta en el dispositivo NAS. De este modo, puede utilizar los recurso del dispositivo para operaciones de procesamiento de datos fuera del host como replicación de

© Acronis International GmbH, 2003-2025

copia de seguridad, validación y limpieza. Para obtener más información acerca de estas operaciones, consulte "Planes de protección de datos fuera del host" (p. 260).

Nota
El agente para Synology solo admite dispositivos NAS con procesadores x86_64. Los procesadores ARM no son compatibles. Consulte el centro de conocimientos de Synology.

Puede recuperar una copia de seguridad a la ubicación original o a una nueva en el dispositivo NAS y a una carpeta de red que sea accesible a través de ese dispositivo. Las copias de seguridad del almacenamiento de la nube también se pueden recuperar a un dispositivo NAS que no sea original en el que esté instalado el Agente para Synology.

La siguiente tabla resume los orígenes y destinos de copias de seguridad disponibles.

Qué incorporar en la copia de seguridad	**Elementos que se incluirán en la copia de seguridad (Origen de copias de seguridad)**	**En dónde realizar la copia de seguridad (Destino de copias de seguridad)**
Archivos/carpetas	Carpeta local*	Almacenamiento en la nube
		Carpeta local*
	Carpeta de red (SMB)**	Carpeta de red (SMB)**
		Carpeta NFS
		Nubes públicas***

* Se incluyen las unidades USB que están conectadas al dispositivo NAS.

Nota
Las carpetas cifradas no son compatibles. Estas carpetas no se muestran en la interfaz de usuario gráfica de Cyber Protection.

** El uso de recursos compartidos de red externos como origen o destino de copias de seguridad mediante el protocolo SMB solo está disponible para los agentes que ejecutan Synology DiskStation Manager 6.2.3 o una versión posterior. Se puede hacer una copia de seguridad de los datos alojados en el propio NAS de Synology, incluidos los recursos compartidos de red alojados, sin limitaciones.

*** La copia de seguridad en nubes públicas, como Microsoft Azure, Amazon, Wasabi o almacenamientos compatibles con S3, solo es compatible con el Agente para Synology 7.x. El agente para Synology 6.x no admite este destino de copia de seguridad debido a las limitaciones del kernel de Linux de Synology DSM 6.x.

© Acronis International GmbH, 2003-2025

Limitaciones

- El agente para Synology solo admite dispositivos NAS con procesadores x86_64. Los procesadores ARM no son compatibles. Consulte el centro de conocimientos de Synology.
- Los recursos compartidos cifrados de los que se haya hecho una copia de seguridad se recuperan como no cifrados.
- Los recursos compartidos de los que se haya hecho una copia de seguridad y para los cuales esté habilitada la opción **Compresión de archivos** se recuperan con esa opción deshabilitada.
- En un dispositivo NAS de Synology, solo puede recuperar copias de seguridad creadas por Agente para Synology.

Descarga del programa de instalación

El programa de instalación de Agente para Synology está disponible en un archivo SPK.

Agente para Synology 7.x

Pasos para descargar el programa de instalación

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. En la esquina superior derecha, haga clic en **Agregar**.
3. En **Network attached storage (NAS)**, haga clic en **Synology**.
   El programa de instalación se descargará en su equipo.

Agente para Synology 6.x

Pasos para descargar el programa de instalación

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. En la esquina superior derecha, haga clic en **Agregar**.
3. En **Network attached storage (NAS)**, haga clic en **Synology**.
   El programa de instalación de Agente para Synology 7.x se descargará en su equipo.
   Puede detener el proceso de descarga de forma segura o ignorar el archivo descargado.
4. Haga clic en **Descargar Agente para Synology 6.x**.
   El programa de instalación de Agente para Synology 6.x se descargará en su equipo.

Instalación de Agente para Synology

Para instalar Agente para Synology, ejecute el archivo SPK en Synology DiskStation Manager.

Nota
El agente para Synology solo admite dispositivos NAS con procesadores x86_64. Los procesadores ARM no son compatibles. Consulte el centro de conocimientos de Synology.

Agente para Synology 7.x

Requisitos previos

© Acronis International GmbH, 2003-2025

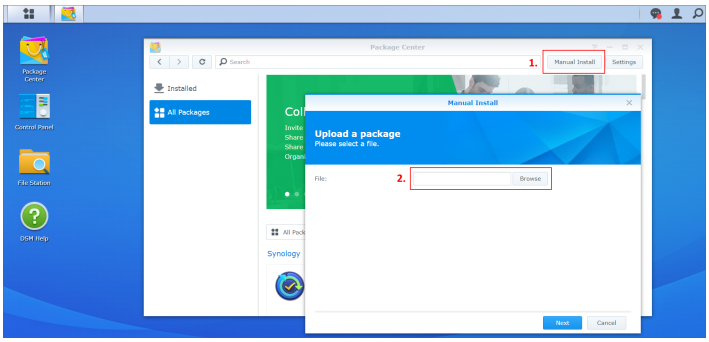
- El dispositivo NAS ejecuta la versión 7.x. de DiskStation Manager.
- Es un miembro del grupo de **administradores** del dispositivo NAS.
- Hay al menos 200 MB de espacio libre en el volumen NAS en el que desee instalar el agente.
- Hay un cliente SSH disponible en su equipo. En este documento se utiliza Putty como ejemplo.

Limitaciones

- No puede registrar el agente para Synology a través de QuickConnect. Para registrar el agente, acceda directamente al dispositivo NAS.

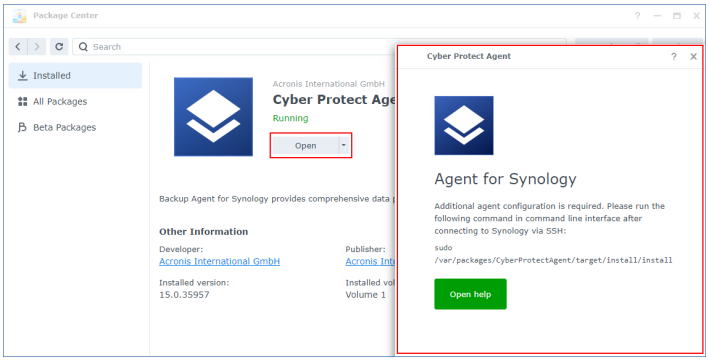
Pasos para instalar Agente para Synology

1. Inicie sesión en Synology DiskStation Manager.
2. Abra el **Centro de paquetes**.
3. Haga clic en **Instalación manual** y, a continuación, haga clic en **Examinar**.



4. Seleccione el archivo SPK que descargó de la consola de Cyber Protect y, a continuación, haga clic en **Siguiente**.

   Se muestra una advertencia de que va a instalar un paquete de software de terceros. Este mensaje forma parte del procedimiento de instalación estándar.
5. Para confirmar que desea instalar el paquete, haga clic en **Aceptar**.
6. Seleccione el volumen en el que desee instalar el agente y, a continuación, haga clic en **Siguiente**.
7. Compruebe la configuración y haga clic en **Listo**.
8. En el **Centro de paquetes** de Synology DiskStation Manager, abra el Agente para Synology Cyber Protect y compruebe que ve la pantalla siguiente.

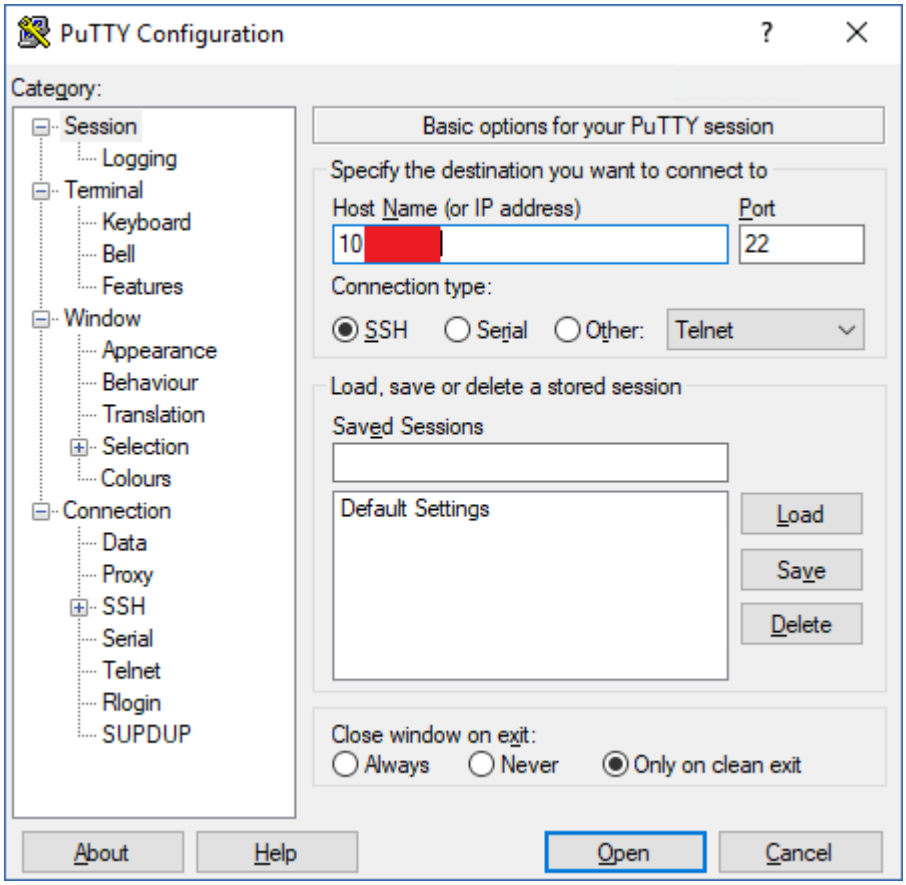


© Acronis International GmbH, 2003-2025

9. En el **Panel de control** de Synology DiskStation Manager, vaya a **Terminal y SNMP** y habilite el acceso de SSH al dispositivo NAS.
10. Ejecute la secuencia de comandos de `instalación` en el dispositivo NAS a través de un cliente SSH (en este ejemplo, Putty).

    La secuencia de comandos habilita el acceso root a DSM 7.0 o posterior, que es necesario para configurar el agente.

    a. Inicie Putty y especifique la dirección IP o el nombre del servidor del dispositivo NAS de Synology.



    b. Haga clic en **Abrir** e inicie sesión como administrador de Synology DSM.

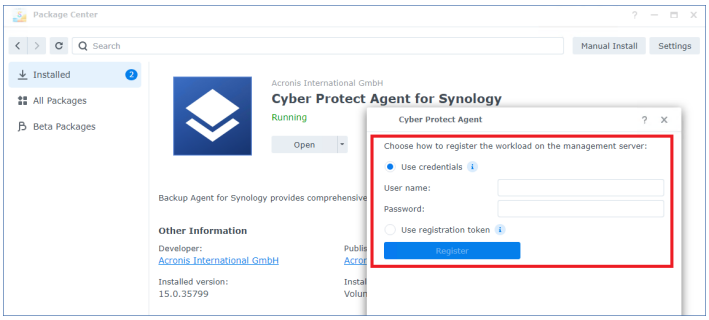
    c. Ejecute el siguiente comando.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

    Cuando comience la secuencia de comandos, espere 15 segundos durante los cuales se inicializan los servicios de Cyber Protection.

11. En el **Panel de control** de Synology DiskStation Manager, vaya a **Terminal y SNMP** y deshabilite el acceso de SSH al dispositivo NAS. El acceso SSH ya no es necesario.
12. En el **Centro de paquetes** de Synology DiskStation Manager, abra el Agente para Synology Cyber Protect.
13. Seleccione el método de registro.

© Acronis International GmbH, 2003-2025



- [Para registrar al agente utilizando credenciales]
  - En los campos **Nombre del usuario** y **Contraseña**, especifique las credenciales para la cuenta con la cual se registrará el agente. Esta cuenta no puede ser una cuenta de administrador de partners.
- [Para registrar el agente utilizando un token de registro]
  - En **Dirección de registro**, especifique la dirección exacta del centro de datos. La dirección exacta del centro de datos es la URL que se ve después de iniciar sesión en la consola de Cyber Protect. Por ejemplo, `https://us5-cloud.acronis.com`.

    Nota
    No utilice un formato de URL sin la dirección del centro de datos. Por ejemplo, no utilice `https://cloud.acronis.com`.

  - En el campo **Token**, especifique el token de registro.

    Para obtener más información sobre cómo generar un token de registro, consulte "Generar un token de registro" (p. 112).

14. Haga clic en **Registrar**.

Agente para Synology 6.x

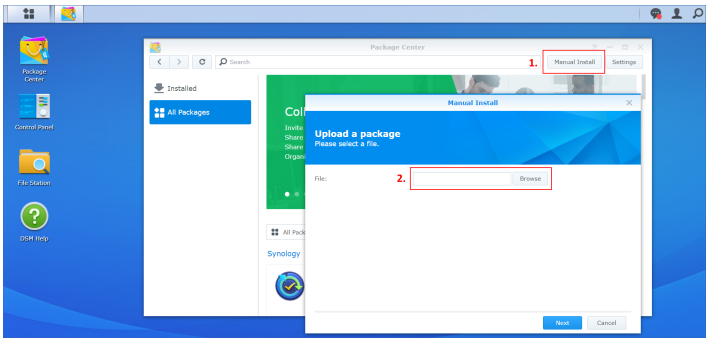
Requisitos previos

- El dispositivo NAS ejecuta la versión 6.2.x. de DiskStation Manager.
- Es un miembro del grupo de **administradores** del dispositivo NAS.
- Hay al menos 200 MB de espacio libre en el volumen NAS en el que desee instalar el agente.

Pasos para instalar Agente para Synology

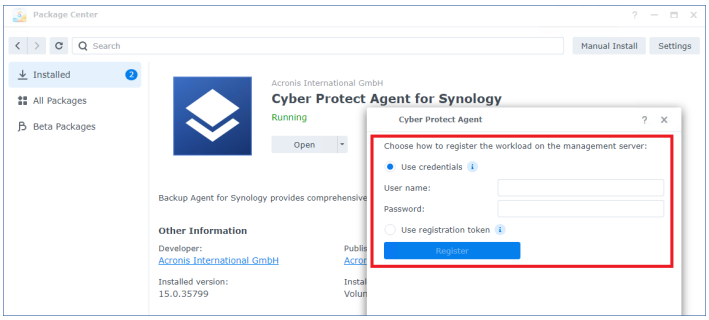
1. Inicie sesión en Synology DiskStation Manager.
2. Abra el **Centro de paquetes**.
3. Haga clic en **Instalación manual** y, a continuación, haga clic en **Examinar**.

© Acronis International GmbH, 2003-2025



4. Seleccione el archivo SPK que descargó de la consola de Cyber Protect y, a continuación, haga clic en **Siguiente**.

   Se muestra una advertencia de que va a instalar sin una firma digital. Este mensaje forma parte del procedimiento de instalación estándar.
5. Para confirmar que desea instalar el paquete, haga clic en **Sí**.
6. Seleccione el volumen en el que desee instalar el agente y, a continuación, haga clic en **Siguiente**.
7. Compruebe la configuración y haga clic en **Aplicar**.
8. En el **Centro de paquetes** de Synology DiskStation Manager, abra el Agente para Synology Cyber Protect.
9. Seleccione el método de registro.



- [Para registrar al agente utilizando credenciales]
  - En los campos **Nombre del usuario** y **Contraseña**, especifique las credenciales para la cuenta con la cual se registrará el agente. Esta cuenta no puede ser una cuenta de administrador de partners.
- [Para registrar el agente utilizando un token de registro]
  - En **Dirección de registro**, especifique la dirección exacta del centro de datos. La dirección exacta del centro de datos es la URL que se ve después de iniciar sesión en la consola de Cyber Protect. Por ejemplo, `https://us5-cloud.acronis.com`.

    Nota
    No utilice un formato de URL sin la dirección del centro de datos. Por ejemplo, no utilice `https://cloud.acronis.com`.

  - En el campo **Token**, especifique el token de registro.

© Acronis International GmbH, 2003-2025

Para obtener más información sobre cómo generar un token de registro, consulte "Generar un token de registro" (p. 112).

10. Haga clic en **Registrar**.

Una vez completado el registro, se mostrará el dispositivo NAS de Synology en la consola de Cyber Protect, en la pestaña **Dispositivos** > **Network Attached Storage**.

Para realizar la copia de seguridad de los datos del dispositivo NAS, aplique un plan de protección.

Actualizar Agente para Synology

Puede actualizar Agente para Synology 6.x a una versión más reciente de Agente para Synology 6.x. Del mismo modo, puede actualizar Agente para Synology 7.x a una versión más reciente de Agente para Synology 7.x.

Para actualizar el agente, ejecute la versión más reciente del programa de instalación en Synology DiskStation Manager. El registro original del agente, su configuración y los planes que se aplican a las cargas de trabajo protegidas se conservarán.

Nota
No puede actualizar el agente desde la consola de Cyber Protect.

Para pasar de Agente para Synology 6.x a Agente para Synology 7.x, es necesario desinstalar el agente más antiguo e instalar el más reciente. En este caso, se revocarán todos los planes de protección y deberá volver a aplicarlos manualmente.

Agente para Synology 7.x

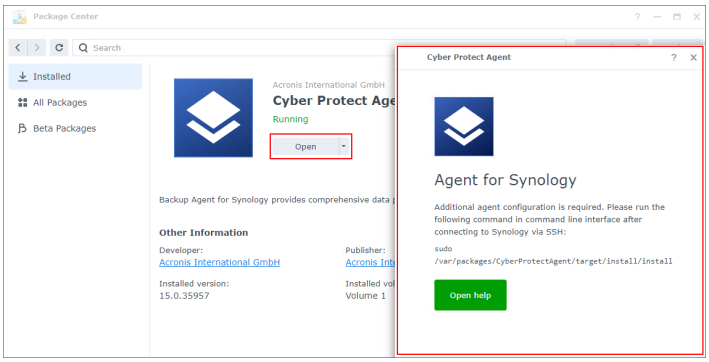
Requisitos previos

- Es un miembro del grupo de **administradores** del dispositivo NAS.
- Hay al menos 200 MB de espacio libre en el volumen NAS en el que desee instalar el agente.
- Hay un cliente SSH disponible en su equipo. En este documento se utiliza Putty como ejemplo.

Pasos para actualizar Agente para Synology

1. En DiskStation Manager, abra el **Centro de paquetes**.
2. Haga clic en **Instalación manual** y, a continuación, haga clic en **Examinar**.
3. Seleccione el archivo SPK más reciente de Agente para Synology 7.x que descargó de la consola de Cyber Protect y, a continuación, haga clic en **Siguiente**.
   Se muestra una advertencia de que va a instalar un paquete de software de terceros. Este mensaje forma parte del procedimiento de instalación estándar.
4. Para confirmar que desea instalar el paquete, haga clic en **Aceptar**.
5. Compruebe la configuración y haga clic en **Listo**.
6. En el **Centro de paquetes** de Synology DiskStation Manager, abra el Agente para Synology Cyber Protect y compruebe que ve la pantalla siguiente.

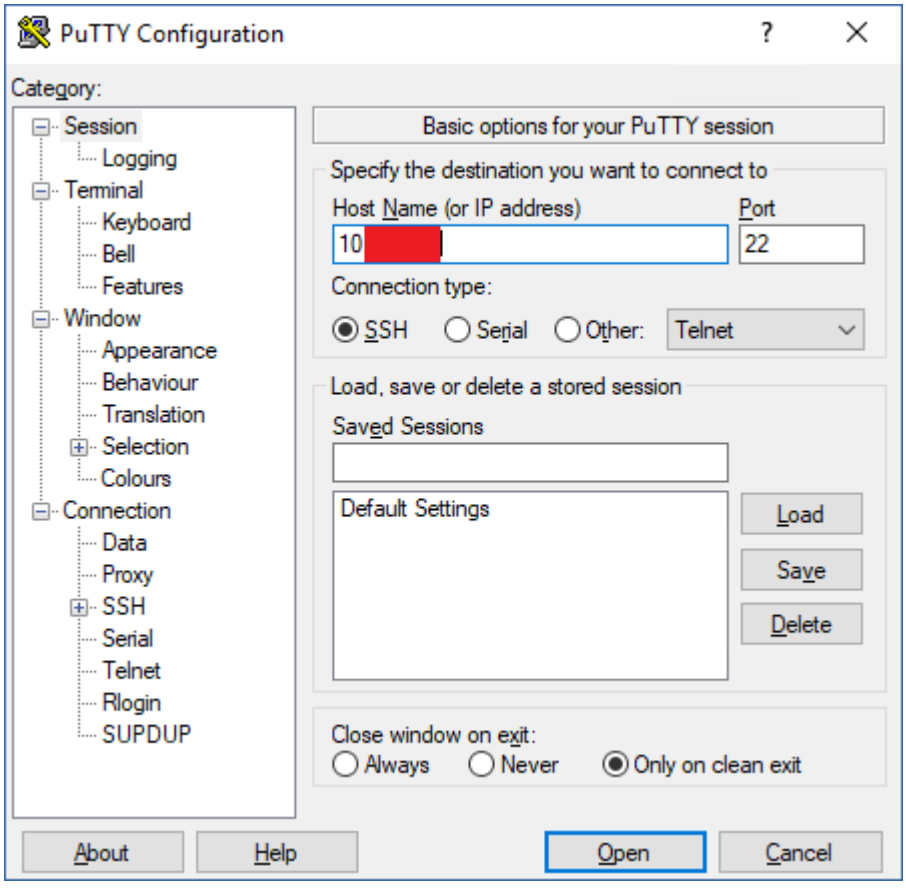
© Acronis International GmbH, 2003-2025



7. En el **Panel de control** de Synology DiskStation Manager, vaya a **Terminal y SNMP** y habilite el acceso de SSH al dispositivo NAS.
8. Ejecute la secuencia de comandos de `instalación` en el dispositivo NAS a través de un cliente SSH (en este ejemplo, Putty).

   La secuencia de comandos habilita el acceso root a DSM 7.0 o posterior, que es necesario para configurar el agente.

   a. Inicie Putty y especifique la dirección IP o el nombre del servidor del dispositivo NAS de Synology.



   b. Haga clic en **Abrir** e inicie sesión como administrador de Synology DSM.

   c. Ejecute el siguiente comando.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```


© Acronis International GmbH, 2003-2025

9. En el **Panel de control** de Synology DiskStation Manager, vaya a **Terminal y SNMP** y deshabilite el acceso de SSH al dispositivo NAS. El acceso SSH ya no es necesario.

Agente para Synology 6.x

Requisitos previos

- Es un miembro del grupo de **administradores** del dispositivo NAS.
- Hay al menos 200 MB de espacio libre en el volumen NAS en el que desee instalar el agente.

Pasos para actualizar Agente para Synology

1. En DiskStation Manager, abra el **Centro de paquetes**.
2. Haga clic en **Instalación manual** y, a continuación, haga clic en **Examinar**.
3. Seleccione el archivo SPK más reciente de Agente para Synology 6.x que descargó de la consola de Cyber Protect y, a continuación, haga clic en **Siguiente**.
   Se muestra una advertencia de que va a instalar sin una firma digital. Este mensaje forma parte del procedimiento de instalación estándar.
4. Para confirmar que desea instalar el paquete, haga clic en **Sí**.
5. Compruebe la configuración y haga clic en **Aplicar**.

Conexiones SSH a un dispositivo virtual

Utilice una conexión Secure Socket Shell (SSH) cuando acceda remotamente a un dispositivo virtual, para fines de mantenimiento.

Iniciar Secure Shell

Para permitir conexiones SSH a un dispositivo virtual, inicie Secure Shell (sshd) en el dispositivo.

Para iniciar Secure Shell

1. En el software del hipervisor, abra la consola del dispositivo virtual.
2. En la interfaz gráfica de usuario del dispositivo, presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
3. Ejecute el siguiente comando:

   ```
   /bin/sshd
   ```

4. [Solo durante la primera conexión al dispositivo] Establezca la contraseña para el usuario `root`.
   Para saber cómo establecer la contraseña, consulte "Establecer la contraseña root en un dispositivo virtual" (p. 186).

Nota
Recomendamos que detenga Secure Shell cuando no utilice la conexión SSH.

© Acronis International GmbH, 2003-2025

Establecer la contraseña root en un dispositivo virtual

Antes de establecer una conexión SSH a un dispositivo virtual por primera vez, debe establecer la contraseña root en el dispositivo.

Para establecer la contraseña de root

1. En el software del hipervisor, abra la consola del dispositivo virtual.
2. En la interfaz gráfica de usuario del dispositivo, presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
3. Ejecute el siguiente comando:

   ```
   passwd
   ```

4. Especifique una contraseña y luego presione Enter.

   La contraseña debe contener al menos nueve caracteres y debe tener una puntuación de complejidad de tres o más. La puntuación de complejidad se calcula automáticamente. Para alcanzar una puntuación más alta, use una combinación de símbolos especiales, símbolos en mayúsculas y minúsculas, y dígitos.
5. Confirme la contraseña y presione Enter.

Acceder a un dispositivo virtual a través de un cliente SSH

Requisitos previos

- En el equipo remoto tiene que haber un cliente SSH. El procedimiento a continuación utiliza el cliente WinSCP como ejemplo. Puede usar cualquier cliente SSH, adaptando los pasos en consecuencia.
- El daemon de Secure Shell (SSHD) debe iniciarse en el dispositivo virtual. Para obtener más información, consulte "Iniciar Secure Shell" (p. 185).

Para acceder a un dispositivo virtual a través de WinSCP

1. En el equipo remoto, abra WinSCP.
2. Haz clic en **Sesión** > **Nueva sesión**.
3. En **Protocolo de archivos**, seleccione **SCP**.
4. En el **Nombre del servidor**, especifique la dirección IP de su dispositivo virtual.
5. En **Nombre del usuario** y **Contraseña**, especifique `root` y la contraseña del usuario `root`.
6. Haga clic en **Iniciar sesión**.

Se muestra una lista de todos los directorios en el dispositivo virtual.

Detección de dispositivos

Al utilizar la funcionalidad de detección de dispositivos, puede:

© Acronis International GmbH, 2003-2025

- Obtener visibilidad completa de los dispositivos de red que están disponibles en las redes de la organización.
- Usar la sincronización con Active Directory para reducir los esfuerzos a la hora de aprovisionar recursos y gestionar equipos en un dominio de Active Directory grande.
- Automatizar la instalación de agentes de protección y el registro de equipos mediante la detección de equipos en su dominio de Active Directory o su red local.
- Instalar agentes de protección en varios recursos informáticos.

Puede utilizar uno de los siguientes métodos para detectar dispositivos:

- Detección de Active Directory.

  Durante un análisis de Active Directory, el agente de detección recopila información sobre la unidad organizativa (UO) de los equipos e información más detallada sobre sus nombres y sistemas operativos, pero no recopila las direcciones IP y MAC.
- Detección de redes locales mediante Device Sense ™. Para obtener más información, consulte "Detección de dispositivos mediante Device Sense ™" (p. 194).
- Detección manual: si se utiliza la dirección IP de un equipo o el nombre del host, o si se importa una lista de equipos desde un archivo.

  Durante una detección manual, los agentes de protección existentes se actualizan y se vuelven a registrar. Si para la detección de dispositivos utiliza la misma cuenta en la que está registrado el agente, este solo se actualizará a la versión más reciente. Si utiliza otra cuenta para la detección´de dispositivos, el agente se actualizará a la versión más reciente y volverá a registrarse bajo el inquilino propietario de la cuenta.

También puede configurar la detección de dispositivos pasivos mediante Device Sense ™ y ver información detallada acerca de los dispositivos que están disponibles en las redes locales corporativas de su organización. Para obtener más información, consulte "Detección pasiva de dispositivos mediante Device Sense ™" (p. 196).

Detección de varios dispositivos

El flujo de detección de varios dispositivos se puede resumir en los siguientes pasos:

1. Selección del método de detección:
   - Detección de Active Directory: al utilizar un controlador de dominio para el flujo automatizado completo o un agente de detección para el flujo con preconfiguración manual.
   - Detección de la red local mediante Device Sense ™.
   - Detección manual: si se utiliza la dirección IP de un equipo o el nombre del host, o si se importa una lista de equipos desde un archivo.
2. [Para la detección basada en Active Directory (flujo con preconfiguración manual) y la detección manual] Seleccione los equipos que desea agregar a su inquilino.
3. [Para la detección basada en Active Directory y la detección manual] Seleccione cómo agregar estos equipos:

© Acronis International GmbH, 2003-2025

- Instale un agente de protección y los componentes adicionales en los equipos, y regístrelos en la consola de Cyber Protect.
- Registre los equipos en la consola de Cyber Protect (si ya hay un agente de protección instalado).
- Añada los equipos a la consola de Cyber Protect como dispositivos sin gestionar sin instalar ningún agente de protección.

También puede aplicar un plan de protección, plan de supervisión y plan de gestión remota a los equipos en los que instale un agente de protección o que haya registrado en la consola de Cyber Protect.

4. [Para la detección basada en Active Directory (flujo con preconfiguración manual) y la detección manual] Proporcione las credenciales del administrador para los equipos seleccionados.
5. [Para la detección basada en Active Directory (flujo con preconfiguración manual) y la detección manual] Verifique que puede conectarse a los equipos al utilizar las credenciales proporcionadas.

Los equipos que se muestran en la consola de Cyber Protect se dividen en las siguientes categorías:

- **Dispositivos detectados**: Equipos que se han detectado, pero en los que no está instalado un agente de protección.
- **Equipos con agentes**: equipos en los que se ha instalado un agente de protección.
- **Dispositivos detectados/ Dispositivos sin agente**: equipos en los que se puede instalar un agente de protección.
- **Dispositivos detectados/Red local**: equipos y dispositivos de red detectados al escanear redes locales mediante el uso de Device Sense ™.
- **Dispositivos detectados/ Active Directory**: equipos detectados al buscar en Active Directory.
- **Dispositivos detectados/ Manual/Desde archivo de texto**: Equipos añadidos manualmente o desde un archivo de texto.

Requisitos para la detección de dispositivos

Antes de utilizar la funcionalidad de detección de dispositivos, asegúrese de que se cumplen los siguientes requisitos:

- Para el flujo de **Incorporación automática completa a través de Active Directory**, al menos un controlador de dominio con un agente de protección instalado debe estar disponible en su red local o dominio de Active Directory.
- Para el flujo **Preconfiguración manual e incorporación automática**, en su red local o dominio de Active Directory debe estar disponible, al menos, un equipo con un agente de protección instalado. Este agente se utilizará como un agente de detección.
- Debe estar asignado a uno de los siguientes roles para el servicio Cyber Protection: administrador de cibernética o administrador.

© Acronis International GmbH, 2003-2025

Importante
Solo los agentes instalados en equipos Windows pueden ser agentes de detección. Si no hay ningún agente de detección en su entorno, no podrá utilizar la opción **Múltiples dispositivos** en el panel **Añadir dispositivos**.

La instalación remota de agentes solo se admite en los equipos que ejecutan Windows (no es compatible con Windows XP). Para realizar la instalación remota en un equipo donde se ejecute Windows Server 2012 R2, debe tener la actualización KB2999226 de Windows instalada en ese equipo.

Incorporación de varios dispositivos

Antes de añadir varios dispositivos, asegúrese de que se cumplen los requisitos. Para obtener más información, consulte "Requisitos para la detección de dispositivos" (p. 188).

Nota
La función no permite añadir controladores de dominio, ya que se requieren permisos adicionales para que el servicio de agente se ejecute.

Buscar en Active Directory

Pasos para añadir varios dispositivos desde Active Directory

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Múltiples dispositivos**, haga clic en **Detectar dispositivos**.
   Se abre el asistente de detección.
4. Seleccione el agente de detección que llevará a cabo el análisis para detectar equipos.

   Nota
   Un agente de detección es un recurso informático en el que se instala un agente de protección.
   El agente de detección debe ser un miembro del dominio de Active Directory.
   Puede seleccionar un agente que esté asociado con la unidad seleccionada o sus unidades secundarias.

5. Seleccione **Buscar en Active Directory** y haga clic en **Siguiente**.
6. En la ventana **Buscar en Active Directory**, seleccione cómo buscar los equipos y haga clic en **Aceptar**.

Opción	Descripción
En lista de unidades organizativas	Seleccione el grupo de equipos que se va a añadir.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Por consulta en dialecto LDAP.	Use la consulta en dialecto LDAP para seleccionar los equipos. La **base de búsqueda** define dónde buscar, mientras que la opción **Filtro** le permite especificar el criterio de selección de los equipos.

7. En la lista de máquinas detectadas, seleccione los equipos que desee añadir y, a continuación, haga clic en **Siguiente**.

   Se abrirá la pestaña **Seleccionar opción de incorporación**. Las siguientes opciones de incorporación están disponibles.

Opción	Descripción
Incorporación automática completa a través de Active Directory	Esta opción utiliza un controlador de dominio en el que se ha instalado un agente de detección para incorporar dispositivos detectados desde Active Directory. No es necesario realizar una preconfiguración manual de los dispositivos.
Preconfiguración manual e incorporación automática	Esta opción requiere la preconfiguración manual de los dispositivos y utiliza un agente de detección para la incorporación de los dispositivos detectados.
Agregar como máquinas no administradas	Esta opción agrega los dispositivos detectados a la consola como dispositivos sin gestionar, sin instalar un agente de protección en ellos.

8. Dependiendo de la opción de incorporación que seleccione, haga lo siguiente:
   - Si ha seleccionado **Incorporación automática completa a través de Active Directory**, complete los pasos 4-13 del procedimiento correspondiente.
   - Si ha seleccionado **Preconfiguración manual e incorporación automática**, complete los pasos 4-11 del procedimiento correspondiente.
   - Si ha seleccionado **Agregar como equipos sin gestionar**, seleccione la cuenta de usuario en la que se registrarán los dispositivos y haga clic en **Agregar**.

Analizar red local

Para detectar varios dispositivos al analizar la red local

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Múltiples dispositivos**, haga clic en **Detectar dispositivos**.

   Se abre el asistente de detección.
4. Haga clic en **Análisis**.

   Comienza el análisis detección activa de dispositivos. Se le redirige a la pantalla **Dispositivos detectados** > **Red de área local**. Una vez finalizado el análisis, se muestra una notificación en la

© Acronis International GmbH, 2003-2025

que se indica la cantidad de dispositivos detectados e incluye un enlace a la lista de dispositivos donde puede ver detalles adicionales sobre ellos.

Qué hacer a continuación:

- Puede hacer clic en el enlace **Ver dispositivos recién detectados** en la notificación y ver los dispositivos y los detalles sobre ellos en la pestaña **Red de área local**.
- Puede instalar un agente de protección en los dispositivos detectados y registrarlos de forma remota. Para obtener más información, consulte "Instalación remota de agentes" (p. 205).
- Puede excluir dispositivos de la detección. Para obtener más información, consulte "Exclusión de dispositivos de la detección" (p. 209).

De forma manual o importando un archivo

Pasos para añadir varios dispositivos manualmente o importando un archivo

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Múltiples dispositivos**, haga clic en **Detectar dispositivos**.
   Se abre el asistente de detección.
4. Haga clic en **Especificar manualmente o importar desde un archivo**.
5. Añada equipos mediante una de las siguientes opciones.
   - Para añadir equipos manualmente:
     a. En el campo **Añadir equipo**, escriba la dirección IPv4 o el nombre de host del equipo.
     b. Repita el paso previo para cada equipo que quiera añadir.
   - Pasos para añadir equipos importando un archivo:
     a. Haga clic en **Importar lista de equipos desde archivo**.
     b. En la ventana **Importar lista de equipos desde archivo**, suelte el archivo de texto que contiene la lista de equipos o haga clic en **Examinar**, navegue hasta el archivo, selecciónelo y haga clic en **Abrir**.
     El archivo debe contener direcciones IP o nombres de host, uno por línea. A continuación se muestra un ejemplo del contenido del archivo:

     ```
     156.85.34.10
     156.85.53.32
     156.85.53.12
     EN-L00000100
     EN-L00000101
     ```

   Cuando ya se hayan añadido las direcciones de los equipos manualmente o se hayan importado de un archivo, el agente intentará anclar los equipos añadidos y comprobar su disponibilidad.
6. Haga clic en **Siguiente**.
   Se abrirá la pestaña **Seleccionar opción de incorporación**. Las siguientes opciones de incorporación están disponibles.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Incorporación automática completa a través de Active Directory	Esta opción utiliza un controlador de dominio en el que se ha instalado un agente de detección para incorporar dispositivos detectados desde Active Directory. No es necesario realizar una preconfiguración manual de los dispositivos.
Preconfiguración manual e incorporación automática	Esta opción requiere la preconfiguración manual de los dispositivos y utiliza un agente de detección para la incorporación de los dispositivos detectados.
Agregar como máquinas no administradas	Esta opción agrega los dispositivos detectados a la consola como dispositivos sin gestionar, sin instalar un agente de protección en ellos.

7. Dependiendo de la opción de incorporación que seleccione, haga lo siguiente:
   - Si ha seleccionado **Incorporación automática completa a través de Active Directory**, complete los pasos 4-13 del procedimiento correspondiente.
   - Si ha seleccionado **Preconfiguración manual e incorporación automática**, complete los pasos 4-11 del procedimiento correspondiente.
   - Si ha seleccionado **Agregar como equipos sin gestionar**, seleccione la cuenta de usuario en la que se registrarán los dispositivos y haga clic en **Agregar**.

Requisitos del control de cuentas de usuario (UAC)

En un equipo que ejecute Windows 7 o posterior y no sea miembro de un dominio de Active Directory, las operaciones de gestión centralizada (incluyendo la instalación remota) necesitan que UAC y las restricciones remotas de UAC estén deshabilitados.

Para deshabilitar UAC

Realice una de las siguientes acciones según el sistema operativo:

- **En un sistema operativo de Windows anterior a Windows 8:**
  Vaya al **Panel de control** > **Vista por: Iconos pequeños** > **Cuentas de usuario** > **Cambiar la configuración de control de la cuenta de usuario** y después mueva el control deslizante a **No notificar**. Después, reinicie el equipo.
- **En cualquier sistema operativo de Windows**:
  1. Abra el Editor del registro.
  2. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Para el valor **EnableLUA**, cambie el ajuste a **0**.
  4. Reinicie el equipo.

Para deshabilitar las restricciones remotas de UAC

© Acronis International GmbH, 2003-2025

1. Abra el Editor del registro.
2. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Para el valor **LocalAccountTokenFilterPolicy**, cambie el ajuste a **1**.

   Si el valor **LocalAccountTokenFilterPolicy** no existe, créelo como DWORD (32 bits). Para obtener más información sobre este valor, consulte la documentación de Microsoft: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Nota
Por motivos de seguridad, le recomendamos que, cuando acabe la operación de gestión (por ejemplo, la instalación remota) revierta ambos ajustes a su estado original: **EnableLUA**=**1** y **LocalAccountTokenFilterPolicy** = **0**

Componentes del agente

Cuando añade varios dispositivos que se detectaron al buscar en Active Directory, puede elegir instalar componentes adicionales.

La siguiente tabla proporciona más información acerca de los componentes de agente que puede instalar.

Componente	Descripción
Componentes obligatorios	
Agente para Windows	Este agente realiza copias de seguridad de discos, volúmenes y archivos, y se instalará en equipos Windows. Siempre estará instalado, no se seleccionará.
Componentes adicionales	
Agente para la prevención de la pérdida de datos	Este agente le permite limitar el acceso de usuario a dispositivos locales y periféricos redirigidos, puertos y cortapapeles de equipos con planes de protección. Se instalará si se selecciona.
Antimalware y filtrado de URL Antimalware	Este componente habilita la protección antivirus y antimalware y el módulo de filtrado de URL en los planes de protección. Incluso si selecciona no instalarlo, se instalará automáticamente más tarde si alguno de estos módulos está habilitado en un plan de protección para el equipo. Este componente habilita la protección antivirus y antimalware en los planes de protección. Incluso si selecciona no instalarlo, se instalará automáticamente más tarde si este módulo está habilitado en un plan de protección para el equipo.
Agente para Hyper-V	Este agente realiza copias de seguridad de máquinas virtuales Hyper-V y se instalará en hosts Hyper-V. Se instalará si se selecciona y detecta el rol Hyper-V en un equipo.
Agente para SQL	Este agente realiza copias de seguridad de bases de datos SQL Server y se

© Acronis International GmbH, 2003-2025

	instalará en equipos que ejecuten Microsoft SQL Server. Se instalará si se selecciona y detecta su aplicación en un equipo.
Agente para Exchange	Este agente realiza copias de seguridad de bases de datos y buzones de correo electrónico de Exchange. Se instalará en equipos con la función Buzón de Microsoft Exchange Server. Se instalará si se selecciona y detecta su aplicación en un equipo.
Agente para Active Directory	Este agente realiza copias de seguridad de los datos de los servicios de dominio de Active Directory. Se instalará en controladores de dominio. Se instalará si se selecciona y detecta su aplicación en un equipo.
Agente para VMware (Windows)	Este agente realiza copias de seguridad de máquinas virtuales VMware. Se instalará en equipos Windows que tengan acceso de red a vCenter Server. Se instalará si se selecciona.
Agente para Microsoft 365	Este agente realiza copias de seguridad de los buzones de correo de Microsoft 365 en un destino local. Se instalará en máquinas Windows. Se instalará si se selecciona.
Agente para Oracle	Este agente realiza copias de seguridad de bases de datos de Oracle y se instalará en equipos que ejecuten la base de datos de Oracle. Se instalará si se selecciona.
Cyber Protection Monitor	Este componente permite a un usuario supervisar tareas en ejecución en el área de notificación y se instalará en equipos Windows. Se instalará si se selecciona. Compatible con Windows 7 Service Pack 1 y versiones posteriores y Windows 2008 R2 Service Pack 1 y versiones posteriores.
Herramienta de línea de comandos	Admite la interfaz de la línea de comandos con la utilidad **acrocmd**. **acrocmd** no contiene ninguna herramienta que ejecute los comandos de forma física. Solo proporciona la interfaz de la línea de comandos para los componentes de Cyber Protect: agentes y el servidor de gestión.
Bootable Media Builder	Crea dispositivo de arranque. Soportado en Windows y Linux.

Detección de dispositivos mediante Device Sense ™

Device Sense ™ utiliza una combinación sofisticada de técnicas para analizar las redes locales de las organizaciones y detectar e identificar dispositivos. Además de detectar equipos físicos, máquinas virtuales y tablets, Device Sense ™ también detecta otros dispositivos de red, como routers, conmutadores, impresoras, smartphones y cámaras IP.

Al utilizar Device Sense ™, puede lograr:

- Visibilidad de red integral: Identificación de todos los dispositivos que están conectados a la red de un cliente.

© Acronis International GmbH, 2003-2025

Esto le ayuda a mantener un inventario de activos preciso y a gestionar y dar soporte a su infraestructura de TI de forma eficaz, lo que es esencial para el seguimiento y la gestión del ciclo de vida de los activos, y también garantiza el cumplimiento de los acuerdos de licencia.

- Seguridad y cumplimiento: Detección de dispositivos no autorizados o malintencionados que puedan suponer riesgos para la seguridad. Device Sense ™ le ayuda a asegurar que cada dispositivo de la red cumple con las directivas de seguridad y los requisitos normativos.
- Asignación eficiente de recursos: Comprensión del ámbito y la escala de una red de cliente, lo que permite asignar recursos de forma más eficiente y lograr una mejor planificación de servicios.

La detección de dispositivos mediante Device Sense ™ incluye las siguientes funciones:

- Selección inteligente automática de agentes y redes de detección para analizar
- Prevención de la detección de dispositivos en redes domésticas o no corporativas

Nota
La detección pasiva mediante Device Sense ™ no analizará las redes que tengan un número de agentes menor que el número que se especifica en la configuración **Evitar la detección de dispositivos en redes no corporativas**. En el nivel del centro de datos, el valor preconfigurado para esta configuración es 3, pero el valor se hereda del inquilino de mayor valor y puede ser diferente. Para asegurarse de que la detección pasiva analiza todas las redes corporativas, puede actualizar la configuración según lo que sea adecuado para su organización. Para obtener más información, consulte "Configuración de detección pasiva de dispositivos" (p. 196).

- Detección activa de dispositivos bajo demanda
- Categorización de dispositivos por tipos
- Opciones de búsqueda y filtrado avanzadas para explorar dispositivos detectados
- Detalles completos de los dispositivos detectados
- Instalación remota de agente de protección en dispositivos detectados, con aplicación de diferentes tipos de planes
- Informe ampliado sobre los dispositivos detectados

Puede utilizar Device Sense ™ para realizar un análisis de detección de dispositivos pasiva o un análisis de detección de dispositivos activa. Para obtener más información, consulte "Detección pasiva de dispositivos mediante Device Sense ™" (p. 196) y "Detección activa de dispositivos mediante Device Sense ™" (p. 197).

Nota
El período de retención de la información sobre los dispositivos detectados en la base de datos es de 3 meses.

© Acronis International GmbH, 2003-2025

Detección pasiva de dispositivos mediante Device Sense ™

La detección pasiva de dispositivos es un método no intrusivo que permite identificar y catalogar dispositivos en un entorno de red, sin necesidad de probar activamente ni de enviar solicitudes a esos dispositivos en la red de la organización.

La detección de dispositivos pasiva recopila los siguientes datos de los dispositivos:

- Nombre de dispositivo
- Tipo de dispositivo
- Familia del SO
- Fabricante
- Modelo
- Dirección MAC
- Dirección IP

Los ajustes de las detecciones pasivas están preconfigurados a nivel de centro de datos. Los administradores de empresas pueden personalizar estos ajustes en todos los dispositivos de una empresa o una unidad. Si no se aplican ajustes personalizados, se utilizarán los del nivel superior en el siguiente orden:

1. centro de datos de Cyber Protection
2. Empresa (inquilino de cliente)
3. Unidad

Por ejemplo, el administrador de una unidad puede configurar los ajustes de detecciones de dispositivos personalizados para la unidad, que pueden ser distintos a los aplicados en equipos a nivel de empresa.

Configuración de detección pasiva de dispositivos

La detección pasiva de dispositivos analiza continuamente las redes corporativas en busca de dispositivos. Al utilizar la detección de dispositivos pasivo:

- Los partners pueden obtener visibilidad de las redes de los clientes y del número y tipo de dispositivos que están disponibles en estas redes.
- Los clientes pueden obtener visibilidad de las redes de su organización y del número y tipo de dispositivos que están disponibles en estas redes.

Pasos para diseñar la configuración de búsqueda de dispositivos pasiva

1. En la consola de Cyber Protect, vaya a **Configuración** > **Gestión**.
2. Haga clic en la pestaña **Detección pasiva de dispositivos**.
3. Asegúrese de que el interruptor **Habilitar la detección pasiva de dispositivos** esté habilitado.

© Acronis International GmbH, 2003-2025

El sistema asigna automáticamente los agentes de Windows como agentes de detección.

4. [Opcional] Modifique los ajustes predeterminados.

Configuración	Descripción
Selección automática inteligente de agentes de detección	Número de agentes que se seleccionarán automáticamente para realizar la detección pasiva de dispositivos en la red local. El valor predeterminado es 1.* El valor máximo es 3.
Evitar la detección de dispositivos en redes no corporativas	Número mínimo de agentes que deben estar presentes en una red para clasificarla como un entorno corporativo y habilitar su exploración. El valor predeterminado es 3.* El valor máximo es 1000.
Identificación mejorada de dispositivos en una red	Habilite o deshabilite el uso de señales de multidifusión para obtener una identificación más precisa de los tipos de dispositivos que se incorporan a la red local. Por defecto, el interruptor está deshabilitado.*

* El valor predeterminado puede ser diferente, dependiendo de la configuración de un inquilino de nivel superior. Los valores predeterminados se heredan y son los mismos que los que se establecen para el inquilino de nivel superior. Sin embargo, puede cambiar los valores predeterminados según las necesidades de su organización.

5. Haga clic en **Guardar**.

Detección activa de dispositivos mediante Device Sense ™

La detección activa de dispositivos es un método utilizado en la gestión de redes en el que un sistema investiga o se comunica activamente con los dispositivos de una red para identificarlos y recopilar información sobre ellos.

Puede recuperar datos completos y precisos sobre los dispositivos en las redes, lo que garantiza que toda la información del dispositivo sea clara y visible.

La detección activa de dispositivos recopila los siguientes datos de dispositivos:

- Nombre de dispositivo
- Tipo de dispositivo
- Familia del SO
- Fabricante
- Modelo
- Dirección IP
- Dirección MAC

© Acronis International GmbH, 2003-2025

Ejecución de un análisis de detección activa de dispositivos mediante Device Sense ™

Puede ejecutar un análisis activo para la recopilación de datos exhaustiva y la identificación de los dispositivos que están conectados a la red local.

Para ejecutar un análisis activo

1. En la consola de Protección, vaya a **Dispositivos** > **Dispositivos detectados**.
2. Haga clic en la pestaña **Red local**.
3. Haga clic en **Ejecutar análisis activo**.
4. Seleccione la red en la que se ejecutará el análisis activo y haga clic en **Ejecutar**.
5. En el campo **Inquilino**, seleccione el inquilino.
6. En el campo **Agente de detección**, seleccione un recurso informático que esté registrado en el inquilino. El agente de protección instalado en este recurso se usará como agente de detección.
7. Haga clic en **Ejecutar**.

   Comienza el análisis activo de detección de dispositivos. Cuando el análisis se completa, se muestra una notificación. Esta notificación muestra la cantidad de dispositivos encontrados e incluye un enlace a la lista de dispositivos donde puede ver detalles adicionales acerca de ellos.

Nota
No puede ejecutar varios análisis activos simultáneamente. Si hay un análisis activo en curso, debe cancelarlo o esperar a que se complete antes de poder iniciar uno nuevo.

Puertos utilizados por Device Sense ™

Este tema enumera los puertos que utiliza Device Sense ™.

La detección de dispositivos pasivos utiliza los siguientes puertos.

Nombre	Puerto	Comentario
DHCP	udp/67	Escucha REQUEST mensajes
NBNS	udp/137	Escucha NAME REGISTRATION REQUEST y NAME REFRESH REQUEST paquetes
NBDS (Browser)	udp/138	Escucha los mensajes de anuncio
SSDP	udp/1900	Escucha M-SEARCH y NOTIFY mensajes
WSD	udp/3702	Escucha wsd:Probe mensajes
MDNS	udp/5353	Escucha varios anuncios de información del servicio
LLMNR	udp/5355	Escucha las consultas
TUYA	udp/6668	Escucha paquetes de detección

© Acronis International GmbH, 2003-2025

Cuando la **Identificación mejorada de dispositivos en una red** está habilitada, Device Sense ™ utiliza los siguientes puertos.

Nombre	Puertos	Comentario
SSDP	udp/1900	Envía M-SEARCH solicitudes
WSD	udp/3702	Envía wsd:Probe solicitudes

La detección de dispositivos activos (flujo de análisis a demanda) utiliza los siguientes puertos.

Nombre	Puertos	Comentario
FTP	tcp/21	Lee los banners del servicio
SSH	tcp/22	Lee los banners del servicio
TELNET	tcp/23	Lee los banners
SMTP	tcp/25 , tcp/587	Lee EHLO mensajes
RDNS	udp/53	Realiza una solicitud DNS inversa `*.in-addr.arpa`
HTTP	tcp/80 , tcp/8080 y otros puertos HTTP habituales	Envía GET solicitudes
NBNS	udp/135	Envía NBSTAT solicitudes
SNMP	udp/161	Lee MIBs : Versiones: v1, v2c; Comunidades: pública
HTTPS	tcp/443 , tcp/8443	Envía GET solicitudes
SMB	tcp/445	Extrae datos de NTLMv2 auth mensajes
RTSP	tcp/554	Envía OPTIONS solicitudes
SSDP	udp/1900	Envía M-SEARCH
ARD	udp/3283	Envía Start paquetes
RDP	tcp/3389	Envía Connection Request y lee Connection Confirm
WSD	udp/3702	Envía wsd:Probe mensajes
AirPlay	tcp/5000 , tcp/7000	Envía wsd:Probe mensajes
MDNS	udp/5353	Envía PTR mensajes
iRobot	udp/5678	Envía iRobot paquetes de descubrimiento irobotmsc

© Acronis International GmbH, 2003-2025

Nombre	Puertos	Comentario
VNC	udp/5900	Envía RFB ProtocolVersion y mensajes de seguridad
MIIO	udp/54321	Envía Hello paquetes

Vista de la información sobre los dispositivos detectados

Puede utilizar los filtros que se incorporan en la página de **Dispositivos detectados** para encontrar rápidamente dispositivos específicos en la lista y ver sus detalles.

Pasos para buscar un dispositivo detectado y ver sus detalles

1. En la consola de Protección, haga clic en **Dispositivos detectados**.
   De forma predeterminada, se abre la pestaña **Dispositivos sin agente**.
2. [Opcional] Para buscar dispositivos de una categoría específica, haga clic en la pestaña correspondiente.

Pestaña	Descripción
Dispositivos sin agente	En esta pestaña figuran todos los equipos detectados en los que se puede instalar un agente de protección, sin importar qué método de detección se utilizó para detectarlos.
Active Directory	Esta pestaña muestra la lista de los equipos que se detectaron al analizar el Active Directory.
Red local	Esta pestaña enumera los dispositivos (equipos u otros dispositivos de red) que se detectaron al analizar las redes corporativas locales mediante el uso de Device Sense ™.
Manual/Desde archivo de texto	Esta pestaña muestra una lista de los equipos que se detectaron manualmente o desde un archivo de texto.
Exclusiones	Esta pestaña enumera los dispositivos que se excluyeron de la búsqueda.

3. [Opcional] Para buscar por nombre de dispositivo, en el campo **Buscar**, introduzca el nombre del dispositivo.
   Los resultados de la lista se filtran de forma dinámica.
4. [Opcional] Para buscar los resultados utilizando filtros, haga clic en **Filtro**, seleccione uno o varios filtros y, a continuación, haga clic en **Aplicar**.

Filtro	Descripción
Tipo de dispositivo	Para buscar uno o varios tipos de dispositivos, haga clic en el campo y seleccione los tipos de dispositivos correspondientes de la lista. Este filtro no está disponible en la pestaña **Manual/Desde archivo de**

© Acronis International GmbH, 2003-2025

Filtro	Descripción
	texto.
Tipo de detección	Para filtrar los resultados según el método de detección, haga clic en el campo y seleccione uno de los siguientes métodos. • **Active Directory** • **Manual** • **Red local pasiva** • **Red local activa** Este filtro solo está disponible en la pestaña **Dispositivos sin agente**.
Dirección MAC	Para buscar un dispositivo que tenga una dirección MAC específica, introduzca la dirección MAC en este campo. Este filtro no está disponible en la pestaña **Manual/Desde archivo de texto**.
Rango de direcciones IP	Para filtrar los resultados en función de la dirección IP del dispositivo, introduzca la dirección IP de inicio en el primer campo y la dirección IP de fin en el segundo campo.
Primera detección	Para filtrar los resultados según la fecha en que se detectó el dispositivo por primera vez, haga clic en el campo y use un rango predefinido o personalizado.
Última detección	Para filtrar los resultados en función de la fecha en la que se detectó el dispositivo por última vez, haga clic en el campo y, a continuación, utilice un rango predefinido o personalizado.
Unidad organizativa	La unidad organizativa en Active Directory a la que pertenece el dispositivo. Este filtro solo está disponible en la pestaña **Active Directory**.

5. Haga clic en el dispositivo y, a continuación, haga clic en **Detalles**.
6. En el panel **Datos sin procesar**, haga clic en el icono de flecha.
7. Para descargar los datos sin procesar en un archivo JSON, haga clic en **Descargar**.
   El archivo se guarda en el directorio de descarga predeterminado en el equipo desde el que ha iniciado sesión en la consola de Protección.

Instalación remota de agentes

Después del proceso de detección de dispositivos, puede instalar agentes en dispositivos Windows detectados de forma remota.

La instalación remota de agentes se realiza de la siguiente manera:

1. El agente de detección se conecta a los equipos de destino mediante el nombre de servidor, la dirección IP y las credenciales de administrador especificadas en el asistente de detección y, a

© Acronis International GmbH, 2003-2025

continuación, descarga el archivo `web_installer.exe` en esos equipos.

2. El archivo `web_installer.exe` se ejecuta en los equipos de destino en el modo desatendido.
3. El instalador web recupera los paquetes de instalación adicionales de la nube y los instala en los equipos de destino con el comando `msiexec`.
4. Cuando se completa la instalación, los componentes se registran en la nube.

Nota
La instalación remota de agentes no es compatible con los controladores de dominio debido a los otros permisos necesarios para que se ejecute el servicio de agente.

Preparación de los equipos para la instalación remota manual

- Para que la instalación se realice correctamente en una máquina remota que ejecute Windows 7 o una versión posterior, la opción **Panel de control** > **Opciones de carpeta** > **Ver** > **Usar Asistente para compartir** debe estar *desactivada* en esa máquina.
- Para una instalación correcta en un equipo remoto que *no* sea miembro de un dominio de Active Directory, el control de cuentas de usuario (UAC) debe estar *deshabilitado* en ese equipo. Para obtener más información sobre cómo deshabilitarlo, consulte "Requisitos del control de cuentas de usuario (UAC)" > Para deshabilitar el UAC.
- De forma predeterminada, se necesitan las credenciales de la cuenta de administrador incorporada para la instalación remota de cualquier equipo Windows. Para llevar a cabo la instalación remota usando las credenciales de otra cuenta de administrador, las restricciones remotas del control de cuentas de usuario (UAC) deben estar *deshabilitadas*. Para obtener más información sobre cómo deshabilitarlas, consulte "Requisitos del control de cuentas de usuario (UAC)" > Para deshabilitar las restricciones remotas de UAC.
- El uso compartido de archivos e impresoras deben estar *habilitado* en el equipo remoto. Para acceder a esta opción:
  - En una máquina que ejecute Windows 2003 Server: vaya a **Panel de control** > **Cortafuegos de Windows** > **Excepciones** > **Compartir archivos e impresoras**.
  - En una máquina que ejecute Windows Server 2008, Windows 7 o una versión posterior: vaya a **Panel de control** > **Cortafuegos de Windows** > **Centro de redes y recursos compartidos** > **Cambiar las configuraciones avanzadas de uso compartido**.
- Cyber Protection utiliza los puertos TCP 445, 25001 y 43234 para la instalación remota.

  El puerto 445 se abre automáticamente cuando habilita Compartir archivos e impresoras. Los puertos 43234 y 25001 se abren automáticamente por medio del cortafuegos de Windows. Si usa un cortafuegos diferente, asegúrese de que estos tres puertos estén abiertos (añadidos a excepciones) para las solicitudes entrantes y salientes.

  Una vez finalizada la instalación remota, el puerto 25001 se cierra automáticamente mediante el cortafuegos de Windows. Los puertos 445 y 43234 deberán permanecer abiertos si desea actualizar el agente de forma remota en el futuro. El puerto 25001 se abre y se cierra automáticamente mediante el cortafuegos de Windows en cada actualización. Si usa otro cortafuegos, mantenga los tres puertos abiertos.

© Acronis International GmbH, 2003-2025

Preparación de equipos para la instalación remota mediante el uso de un GPO

Puede configurar y aplicar un objeto de directiva de grupo (GPO) de Active Directory para preparar un conjunto de equipos que son miembros de Active Directory para la instalación remota de los agentes de Protección.

Requisitos previos

- Su usuario es miembro del grupo de administradores de dominio o es un administrador de dominio.
- La **consola de administración de directivas de grupo** (GPMC) está instalada en el equipo en el que ha iniciado sesión para crear la GPO.

Pasos ara preparar equipos para la instalación remota mediante el uso de una GPO

1. Para abrir la GPMC, presione **Win** + **R**, escriba `gpmc.msc` y luego presione **Intro**.
2. En el árbol de la consola, haga clic con el botón derecho en el dominio o en la unidad organizativa (UO) a la que desee aplicar un GPO.
3. Haga clic en **Crear un GPO en este dominio y vincularlo aquí...**.
4. En el mensaje emergente **Nuevo GPO**, introduzca un nombre para el GPO y haga clic en **Aceptar**.
5. En el árbol de la consola, haga clic con el botón derecho en el GPO que creó en el paso anterior y después haga clic en **Editar...**.
6. Desactive **Usar el asistente para compartir** mediante los pasos que se indican a continuación.
   a. En el árbol de la consola, vaya a **Configuración de usuario** > **Preferencias** > **Configuración de Windows** > **Registro**.
   b. Haga clic con el botón derecho en **Registro** y después haga clic en **Nuevo** > **Elemento del registro**.
   c. En la ventana **Nuevas propiedades del registro**, en la pestaña **General**, configure el elemento del registro de la siguiente manera.

Parámetro	Valor
Acción	Actualización
Hive	`HKEY_CURRENT_USER`
Ruta clave	Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Nombre del valor	SharingWizardOn
Tipo de valor	`REG_DWORD`
Datos del valor	0

   d. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

© Acronis International GmbH, 2003-2025

7. [Para Windows Vista y versiones posteriores] Deshabilite el control de cuentas de usuario (UAC). Para ello, siga estos pasos:
   a. En el árbol de la consola, vaya a **Configuración del ordenador** > **Preferencias** > **Configuración de Windows** > **Registro**.
   b. Haga clic con el botón derecho en **Registro** y después haga clic en **Nuevo** > **Elemento del registro**.
   c. En la ventana **Nuevas propiedades del registro**, en la pestaña **General**, configure el elemento del registro de la siguiente manera.

Parámetro	Valor
Acción	Actualización
Hive	HKEY_LOCAL_MACHINE
Ruta clave	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
Nombre del valor	EnableLUA
Tipo de valor	REG_DWORD
Datos del valor	0

   d. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
8. [Para Windows Vista y versiones posteriores] Deshabilite las restricciones remotas del control de cuentas de usuario (UAC). Para ello, siga estos pasos:
   a. En el árbol de la consola, vaya a **Configuración del ordenador** > **Preferencias** > **Configuración de Windows** > **Registro**.
   b. Haga clic con el botón derecho en **Registro** y después haga clic en **Nuevo** > **Elemento del registro**.
   c. En la ventana **Nuevas propiedades del registro**, en la pestaña **General**, configure el elemento del registro de la siguiente manera.

Parámetro	Valor
Acción	Actualización
Hive	HKEY_LOCAL_MACHINE
Ruta clave	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Nombre del valor	LocalAccountTokenFilterPolicy
Tipo de valor	REG_DWORD
Datos del valor	1

   d. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
9. Habilite **Compartir impresoras y archivos**.Para ello, siga estos pasos:

© Acronis International GmbH, 2003-2025

a. En el árbol de la consola, vaya a **Configuración del ordenador** > **Directivas** > **Configuración de Windows** > **Configuración de seguridad** > **Cortafuegos de Windows Defender con seguridad avanzada** > **Reglas de entrada**.
b. Haga clic con el botón derecho en **Reglas de entrada** y después en **Nueva regla**.
c. En el **Asistente para nueva regla de entrada**, configure la regla de la siguiente manera:
d. En la pestaña **Tipo de regla**, seleccione **Predefinido**, luego **Compartir impresoras y archivos** y haga clic en **Siguiente**.
e. En la pestaña **Reglas predefinidas**, haga clic en **Siguiente**.
f. En la pestaña **Acción**, seleccione **Permitir la conexión** y, a continuación, haga clic en **Finalizar**.
g. En el árbol de la consola, vaya a **Configuración del ordenador** > **Directivas** > **Configuración de Windows** > **Configuración de seguridad** > **Cortafuegos de Windows Defender con seguridad avanzada** > **Reglas de salida**.
h. Haga clic con el botón derecho en **Reglas de salida** y seleccione **Nueva regla**.
i. En **Asistente para nueva regla de salida**, configure la regla. Para ello, lleve a cabo las mismas acciones que en los pasos d - f.

10. Vincule el GPO al dominio o a la UO con los pasos que se indican a continuación.
    a. En el árbol de la consola, haga clic con el botón derecho en el dominio o la UO de destino y, a continuación, haga clic en **Vincular un GPO existente...**
    b. En la pantalla **Seleccionar GPO**, seleccione el GPO que creó y haga clic en **Aceptar**.
11. En los equipos de destino que desee preparar para una instalación de agente remoto, fuerce la actualización de la directiva de grupo con los pasos que se indican a continuación.
    a. Ejecute el **símbolo del sistema** como administrador.
    b. Ejecute el siguiente comando:

    ```
    gpupdate /force
    ```

Instalación remota de agentes

Nota
La instalación remota de agentes es compatible solo con los dispositivos Windows.

La instalación de agentes en varios dispositivos solo está disponible para dispositivos que se encuentran en la misma red y que se han detectado mediante el mismo método de detección.

Puede incorporar de forma remota varios dispositivos detectados a la vez. El proceso de incorporación consiste en la instalación del agente, la aplicación de planes y el registro del dispositivo.

Incorporación automática completa a través de Active Directory

Requisitos previos

© Acronis International GmbH, 2003-2025

En Active Directory debe estar disponible al menos un controlador de dominio en el que se haya instalado agente de protección.

Pasos para agregar varios dispositivos mediante la incorporación automática completa a través de Active Directory

1. En la consola de Protección, vaya a **Dispositivos** > **Dispositivos detectados** > **Dispositivos sin agente**.
2. Seleccione los dispositivos que quiera proteger.
3. Haga clic en **Instalar agente**.
4. En la pestaña **Seleccionar opción deincorporación**, haga clic en **Incorporación automática completa a través de Active Directory**.
5. En el campo **Controlador de dominio**, seleccione el controlador de dominio.
6. En el campo **Credenciales de administrador de dominio**, haga clic en **Seleccionar**.
7. En la pantalla **Lista de credenciales**, seleccione las credenciales de la cuenta del administrador del controlador de dominio y haga clic en **Seleccionar credenciales**.
   El controlador de dominio analiza Active Directory en busca de dispositivos y los muestra en una lista. De manera predeterminada, todos los dispositivos detectados están preseleccionados, pero puede desmarcar la selección de los dispositivos que no desee registrar ni proteger.
8. En la lista de dispositivos, asegúrese de que estén seleccionados los dispositivos que desea incorporar.
9. Haga clic en **Siguiente**.
10. En la pestaña **Seleccionar componentes de agente**, haga lo siguiente:
    a. Para seleccionar los componentes que desea instalar, haga clic en **Componentes para instalar** y, a continuación, selecciónelos. Para obtener más información sobre los componentes disponibles, consulte "Componentes del agente" (p. 193).
    b. En el panel **Configuración**, configure las opciones de instalación.

Opción	Descripción
Cuenta de inicio de sesión en el servicio	La cuenta bajo la cual se ejecutarán los servicios. De manera predeterminada, se selecciona **Usar cuentas de usuario del servicio**. Para cambiar el valor predeterminado, haga clic en **Modificar**. Para obtener más información sobre todas las opciones, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 67).
Reiniciar el dispositivo cuando sea necesario	Seleccione esta opción si desea que el dispositivo se reinicie cuando la instalación de un componente lo requiera.
No reiniciar el dispositivo si un usuario está conectado	Seleccione esta opción si no desea que el dispositivo se reinicie cuando un usuario inicie sesión en él.

© Acronis International GmbH, 2003-2025

c. Seleccione una cuenta de usuario en la que desee registrar los dispositivos.

d. Haga clic en **Siguiente**.

11. [Opcional] En la pestaña **Seleccionar planes**, para seleccionar los planes que se aplicarán a los equipos automáticamente, en el campo de selección de planes del tipo de plan correspondiente, haga clic en **Modificar**, seleccione el plan y, a continuación, haga clic en **Modificar** de nuevo.

Nota
La selección de planes solo está permitida si la autenticación de doble factor (2FA) está configurada para el inquilino. Si la 2FA no está configurada, debe configurarla primero e iniciar sesión en la consola de Cyber Protect y comenzar este procedimiento desde el principio.

12. Haga clic en **Siguiente**.

13. En la pantalla **Revisar y registrar**, compruebe las cuotas requeridas y, a continuación, realice una de las siguientes acciones:
    - Para registrar las cargas de trabajo, haga clic en **Registrar**.
      Si ha iniciado sesión como administrador de partner, se habilitarán automáticamente los paquetes Advanced necesarios para el inquilino en el que registre la carga de trabajo.
      Si no ha iniciado sesión como administrador de partner, no se habilitarán automáticamente los paquetes avanzados requeridos. Aún puede aplicar los planes seleccionados, pero es posible que no funcionen correctamente. Para resolver este problema, pida a su administrador de partner que habilite los paquetes avanzados requeridos o que cambie los planes preseleccionados.
    - Para seleccionar diferentes planes, vaya a la pestaña **Seleccionar planes** y continúe con este procedimiento.

Preconfiguración manual e incorporación automática

Requisitos previos

Los dispositivos que desea agregar están configurados para la instalación remota del agente, tal y como se describe en "Preparación de equipos para la instalación remota mediante el uso de un GPO" (p. 203).

Pasos para agregar varios dispositivos mediante la preconfiguración manual y la incorporación automática

1. En la consola de Protección, vaya a **Dispositivos** > **Dispositivos detectados** > **Dispositivos sin agente**.
2. Seleccione los dispositivos que quiera proteger.
3. Haga clic en **Instalar agente**.
4. En la pestaña **Seleccionar opción de incorporación**, haga clic en **Preconfiguración manual e incorporación automática** y, a continuación, haga clic en **Siguiente**.
5. En la pestaña **Seleccionar componentes de agente**, haga lo siguiente:

© Acronis International GmbH, 2003-2025

a. En el campo **Agente de detección**, seleccione el recurso informático que se utilizará para la instalación y el registro del agente remoto de los equipos.

Nota
Un agente de detección es un recurso informático en el que se instala un agente de protección.
A nivel de cliente, puede seleccionar un agente que esté asociado con la unidad seleccionada.
A nivel de partner, puede seleccionar un agente que esté asociado con el cliente seleccionado.

b. Para seleccionar los componentes que desea instalar, haga clic en **Componentes para instalar** y, a continuación, selecciónelos. Para obtener más información sobre los componentes disponibles, consulte "Componentes del agente" (p. 193).

c. En el panel **Configuración**, configure las opciones de instalación.

Opción	Descripción
Cuenta de inicio de sesión en el servicio	La cuenta bajo la cual se ejecutarán los servicios. De manera predeterminada, se selecciona **Usar cuentas de usuario del servicio**. Para cambiar el valor predeterminado, haga clic en **Modificar**. Para obtener más información sobre todas las opciones, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 67).
Reiniciar el dispositivo cuando sea necesario	Seleccione esta opción si desea que el dispositivo se reinicie cuando la instalación de un componente lo requiera.
No reiniciar el dispositivo si un usuario está conectado	Seleccione esta opción si no desea que el dispositivo se reinicie cuando un usuario inicie sesión en él.

d. Seleccione una cuenta de usuario en la que desee registrar los dispositivos.

e. Haga clic en **Siguiente**.

6. [Opcional] En la pestaña **Seleccionar planes**, para seleccionar los planes que se aplicarán a los equipos automáticamente, en el campo de selección de planes del tipo de plan correspondiente, haga clic en **Modificar**, seleccione el plan y, a continuación, haga clic en **Modificar** de nuevo.

Nota
La selección de planes solo está permitida si la autenticación de doble factor (2FA) está configurada para el inquilino. Si la 2FA no está configurada, debe configurarla primero e iniciar sesión en la consola de Cyber Protect y comenzar este procedimiento desde el principio.

7. Haga clic en **Siguiente**.

© Acronis International GmbH, 2003-2025

8. En la pestaña **Credenciales**, haga lo siguiente:
   a. Haga clic en **Agregar credenciales**.
   b. Seleccione las credenciales de un usuario con derechos de administrador para los dispositivos seleccionados y después haga clic en **Seleccionar credenciales**.

      Importante
      La instalación remota de agentes solo funciona sin ninguna preparación si se especifican las credenciales de la cuenta de administrador incorporada (la primera cuenta que se crea cuando se instala el sistema operativo). Si desea definir credenciales de administrador personalizadas, debe hacer preparativos adicionales de forma manual. Para obtener más información, consulte "Preparación de los equipos para la instalación remota manual" (p. 202).

   c. Haga clic en **Siguiente**.
      El sistema realiza comprobaciones preliminares en los dispositivos seleccionados para asegurarse de que son adecuados y de que tienen la configuración correcta para la instalación remota del agente y los componentes seleccionados.
9. En la pestaña **Conectividad**, realice uno de los siguientes procedimientos:
   - Si hay problemas de conectividad, resuélvalos al hacer clic en **Cambiar credenciales para todos los dispositivos** y, a continuación, en Siguiente.
   - Si no se identifican problemas de conectividad, haga clic en **Siguiente**.
10. En la pantalla **Revisar y registrar**, compruebe las cuotas requeridas y, a continuación, realice una de las siguientes acciones:
    - Para registrar las cargas de trabajo, haga clic en **Registrar**.
      - Si ha iniciado sesión como administrador de partner, se habilitarán automáticamente los paquetes Advanced necesarios para el inquilino en el que registre la carga de trabajo.
      - Si no ha iniciado sesión como administrador de partner, no se habilitarán automáticamente los paquetes avanzados requeridos. Aún puede aplicar los planes seleccionados, pero es posible que no funcionen correctamente. Para resolver este problema, pida a su administrador de partner que habilite los paquetes avanzados requeridos o que cambie los planes preseleccionados.
    - Para seleccionar diferentes planes, vaya a la pestaña **Seleccionar planes** y continúe con este procedimiento.

Exclusión de dispositivos de la detección

Cuando excluya dispositivos de la búsqueda, no se incluirán en los resultados de los dispositivos encontrados cuando se ejecute un análisis de búsqueda de dispositivos.

Pasos para excluir un dispositivo de la búsqueda

© Acronis International GmbH, 2003-2025

1. En la consola de Protección, vaya a **Dispositivos detectados**.
2. Haga clic en el dispositivo que desea excluir de la búsqueda y, a continuación, haga clic en **Excluir de la búsqueda**.
   El dispositivo se excluye de la búsqueda y se añade a la lista de dispositivos de la página **Exclusiones**.

Conexión remota a dispositivos descubiertos

Puede conectarse de forma remota a dispositivos Windows o macOS descubiertos y proporcionar asistencia única.

Requisitos previos

- [Para conexiones RDP] RDP está habilitado en el dispositivo Windows.
- [Para conexiones a través del uso compartido de pantalla de Apple] El uso compartido de pantalla de Apple está activado en el dispositivo macOS.

Pasos para conectarse de forma remota a un dispositivo descubierto

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Dispositivos detectados**.
2. Haga clic en el dispositivo al que desee conectarse remotamente.
3. Haga clic en **Escritorio remoto** y luego, dependiendo del sistema operativo del dispositivo, seleccione el modo de vista.

Sistema operativo	Protocolo de conexión	Modo Ver
Windows	RDP	**Control**: en este modo, podrá observar y ejecutar operaciones en el dispositivo remoto.
macOS	Uso compartido de pantalla de Apple	**Control**: en este modo, podrá observar y ejecutar operaciones en el dispositivo remoto. **Solo visualización**: en este modo, solo podrá observar el dispositivo remoto. **Cortina**: disponible solo para dispositivos macOS. Si se conecta al dispositivo remoto en modo cortina, la pantalla del dispositivo remoto se atenuará y el usuario remoto no podrá ver sus acciones en el dispositivo.

4. [Si Cliente de Connect no está instalado en su dispositivo] En el cuadro de diálogo **Conectarse a la carga de trabajo**, haga clic en **Descargar Cliente de Connect**, descargue e instale el cliente en su dispositivo y luego pulse en **Conectar**.
5. [Si aparece un mensaje de confirmación emergente] Haga clic en **Abrir Cliente de Connect**.
6. [Para dispositivos Windows] En la ventana emergente de **Autenticación RDP**, introduzca el nombre de usuario, la contraseña y el dominio, y luego haga clic en **Conectar**.
7. [Para dispositivos macOS] En la ventana de **Autenticación**, seleccione una opción de

© Acronis International GmbH, 2003-2025

autenticación, proporcione las credenciales requeridas dependiendo de la opción que seleccionó, y luego haga clic en **Conectar**.

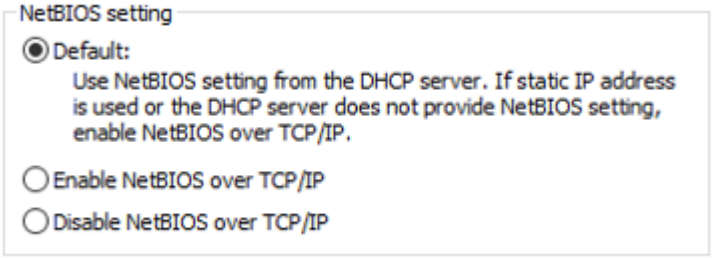
Opción de autenticación	Descripción
Con credenciales de macOS	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador del dispositivo remoto.
pidiendo observar	Se le permitirá establecer la conexión remota en el modo de observación después de que el usuario que ha iniciado sesión en el dispositivo remoto lo permita.
con contraseña de VNC	Se le permitirá establecer la conexión remota después de proporcionar la contraseña de VNC.

Nota
Las opciones de autenticación que verá dependen de las opciones de compartición de pantalla que están configuradas en el dispositivo macOS remoto.

Detección pasiva de la solución de problemas

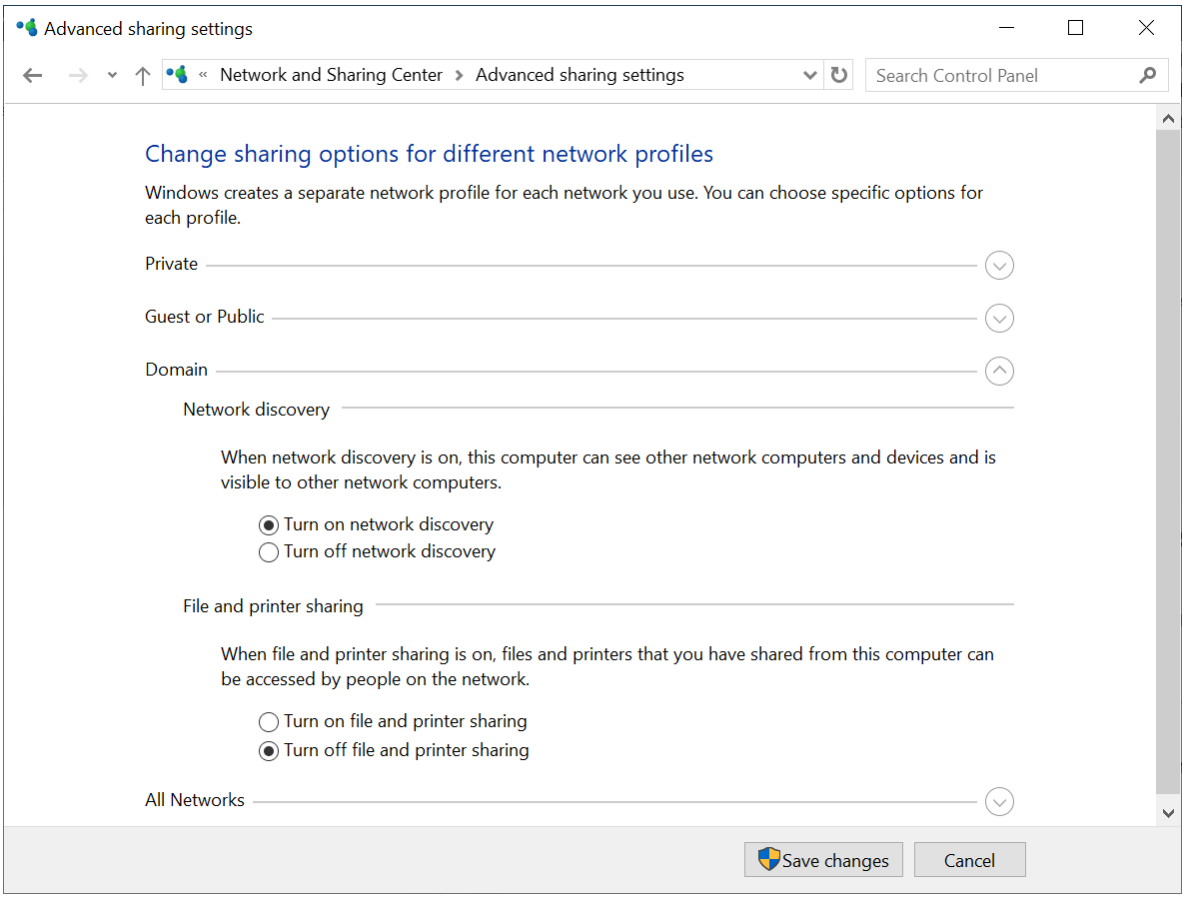
Si tiene algún problema relacionado con la funcionalidad de detección, intente comprobar lo siguiente:

- Compruebe si NetBIOS en TCP/IP está habilitado o establecido como predeterminado.



- En "Panel de control\Centro de redes y recursos compartidos\Configuraciones compartidas avanzadas", active la detección de redes.

© Acronis International GmbH, 2003-2025



- Compruebe si el servicio Function Discovery Provider Host se está ejecutando en el equipo que se encarga de las detecciones y en los equipos que se van a detectar.
- Compruebe si el servicio Function Discovery Resource Publication se está ejecutando en los equipos que se van a detectar.

Evitar la desinstalación o modificación de agentes no autorizadas

El agente de Cyber Protection para Windows está protegido contra desinstalaciones o modificaciones no autorizadas mediante la opción **Protección de desinstalación del agente** en los planes de protección. Para todos los planes de protección creados después de noviembre de 2024, esta opción está habilitada de forma predeterminada. En los planes de protección heredados, debe habilitarla manualmente para mejorar la seguridad de sus recursos informáticos.

Nota
Esta opción está disponible solo si se habilita la configuración **Autoprotección**.

Pasos para habilitar la protección de desinstalación del agente

1. En un plan de protección, amplíe el módulo **Protección antivirus y antimalware** (módulo **Active Protection** para ediciones Cyber Backup).

© Acronis International GmbH, 2003-2025

2. Asegúrese de que el interruptor **Autoprotección** esté habilitado.
3. Seleccione la casilla de verificación **Protección de desinstalación del agente**.
4. En el panel **Autoprotección**, haga clic en **Listo**.
5. Guarde el plan de protección.

La protección de desinstalación del agente se habilitará para los equipos Windows a los que se aplique este plan de protección. Se prohibirán todas las modificaciones a menos que un administrador las autorice. Consulte "Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada" (p. 213).

Puede aplicar un plan de protección con la opción **Protección de desinstalación del agente** activada a un equipo que ejecute macOS o Linux, pero no se le ofrecerá protección.

Tampoco puede aplicar más de un plan de protección con Protección de desinstalación del agente habilitado a un mismo equipo Windows. Para obtener información sobre cómo resolver un posible conflicto, consulte Resolución de problemas de compatibilidad.

Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada

1. Después de un intento fallido de modificar el agente de protección, navegue hasta la pestaña **Alertas**.
2. Ubique la alerta relacionada con el intento de modificación/desinstalación fallido.
   Gravedad de la alerta: Aviso
   Título de la alerta: se ha evitado el intento de desinstalación o actualización del agente
3. Haga clic en la alerta y seleccione una medida de respuesta de la lista desplegable:
   - **Permitir cambios de agente durante 1 hora**: para permitir modificaciones en el agente de protección en la siguiente hora.
   - **Ir a la configuración de actualización del agente**: para configurar una ventana de mantenimiento de mayor duración.
     La duración puede ser de entre 1 hora y 7 días a partir del momento actual.
     Las modificaciones o desinstalación del agente solo se permitirán durante este período a menos que habilite las actualizaciones automáticas para el agente de protección.
4. [Solo si ha seleccionado ir a la configuración de actualización del agente] En el diálogo de configuración del agente, seleccione la duración del período de mantenimiento para las actualizaciones manuales o habilite la opción **Actualizar automáticamente los agentes**.
   - Si configura un período de mantenimiento sin habilitar las actualizaciones automáticas, solo se permitirán las modificaciones manuales durante el período de mantenimiento que haya configurado.
   - Si habilita las actualizaciones automáticas sin configurar una ventana de mantenimiento, las actualizaciones automáticas pueden ocurrir en cualquier momento dado.
   - Si configura una ventana de mantenimiento y actualizaciones automáticas, tanto las actualizaciones automáticas como las manuales solo pueden ocurrir durante la ventana de mantenimiento.

© Acronis International GmbH, 2003-2025

5. Haga clic en **Aplicar**.

Pasos para deshabilitar la protección de desinstalación del agente

Advertencia.
Si deshabilita la **Protección de desinstalación del agente** pone en riesgo la seguridad de los recursos informáticos protegidos.

1. Abra el plan de protección para editar y ampliar el módulo **Protección antivirus y antimalware** (módulo **Active Protection** para las ediciones Cyber Backup).
2. Expanda la sección **Autoprotección**.
3. Desactive la casilla de verificación **Protección de desinstalación del agente**.
4. En el panel **Autoprotección**, haga clic en **Listo**.
5. Guarde el plan de protección.

Cambiar la cuota de servicio de cargas de trabajo

Una cuota de servicio se asigna automáticamente cuando se aplica un plan de protección a una carga de trabajo por primera vez.

Se asigna la cuota más apropiada, según el tipo de carga de trabajo protegida, su sistema operativo, el nivel de protección requerido y la disponibilidad de la cuota. Si la cuota más adecuada no está disponible en su organización, se asignará la segunda mejor cuota. Por ejemplo, si la cuota más adecuada es **Servidores de alojamiento web**, pero no está disponible, se asignará la cuota **Servidores**.

Ejemplos de asignación de cuotas:

- A un equipo físico que ejecuta un sistema operativo Windows Server o Linux se le asigna la cuota **Servidores**.
- A un equipo físico que ejecuta un sistema operativo Windows de escritorio se le asigna la cuota **Estaciones de trabajo**.
- A un equipo físico que ejecuta Windows 10 con el rol Hyper-V habilitado se le asigna la cuota **Estaciones de trabajo**.
- A un equipo de escritorio que se ejecuta en una infraestructura de escritorio virtual y cuyo agente de protección se instala dentro del sistema operativo invitado (por ejemplo, Agente para Windows) se le asigna la cuota **Equipos virtuales**. Este tipo de equipo también puede utilizar la cuota **Estaciones de trabajo** cuando la cuota **Equipos virtuales** no está disponible.
- A un equipo de escritorio que se ejecuta en una infraestructura de escritorio virtual y de cuyo agente se hace una copia de seguridad en el modo sin agente (por ejemplo, por Agente para VMware o Agente para Hyper-V) se le asigna la cuota **Equipos virtuales**.
- A un servidor Hyper-V o vSphere se le asigna la cuota **Servidores**.

© Acronis International GmbH, 2003-2025

- A un servidor con cPanel o Plesk se le asigna la cuota **Servidores de alojamiento web**. También puede utilizar la cuota **Equipos virtuales** o la cuota **Servidores**, según el tipo de equipo en el que se ejecute el servidor web, si la cuota **Servidores de alojamiento web** no está disponible.
- La copia de seguridad con información de aplicaciones requiere la cuota **Servidores**, incluso para una estación de trabajo.

Puede cambiar manualmente la asignación original más adelante. Por ejemplo, para aplicar un plan de protección más avanzado a la misma carga de trabajo, es posible que tenga que mejorar la cuota de servicio de la misma. Si las características que necesita este plan de protección no son compatibles con la cuota de servicio asignada en ese momento, el plan de protección fallará.

Otra posibilidad es cambiar la cuota de servicio si adquiere una cuota más apropiada después de haber asignado la original. Por ejemplo, a un equipo virtual se le asigna la cuota **Estaciones de trabajo**. Después de adquirir una cuota de **Equipos virtuales**, puede asignarla manualmente a la carga de trabajo en lugar de la cuota **Estaciones de trabajo** original.

También puede liberar la cuota de servicio asignada actualmente para asignarla a otra carga de trabajo.

Puede cambiar la cuota de servicio de una carga de trabajo individual o de un grupo de cargas de trabajo.

Pasos para cambiar la cuota de servicio de una carga de trabajo individual

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Seleccione una carga de trabajo y haga clic en **Detalles**.
3. En la sección **Cuota de servicio**, haga clic en **Modificar**.
4. En la ventana **Cambiar cuota**, seleccione la cuota de servicio o **Sin cuota** y, a continuación, haga clic en **Modificar**.

Pasos para cambiar la cuota de servicio de un grupo de cargas de trabajo

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Seleccione más de una carga de trabajo y haga clic en **Asignar cuota**.
3. En la ventana **Cambiar cuota**, seleccione la cuota de servicio o **Sin cuota** y, a continuación, haga clic en **Modificar**.

Configuración de la protección

Para configurar los ajustes generales sobre protección para Cyber Protection, vaya a **Configuración** > **Protección** en la consola de Cyber Protect.

Actualizaciones automáticas de los componentes

De forma predeterminada, todos los agentes se pueden conectar a Internet y descargar actualizaciones.

© Acronis International GmbH, 2003-2025

Un administrador puede minimizar el tráfico de ancho de banda de red al seleccionar uno o varios agentes en el entorno y asignarles el rol de actualizador. Así, los agentes dedicados se conectarán a Internet y descargarán actualizaciones. El resto de los agentes se conectará a los agentes del actualizador dedicado mediante tecnología de par a par y descargarán las actualizaciones.

Los agentes sin el rol de actualizador se conectarán a Internet si no hay un agente actualizador dedicado en el entorno o si no se puede establecer la conexión a un agente actualizador dedicado durante aproximadamente cinco minutos.

El agente de actualización distribuye las actualizaciones y los parches para la protección antivirus y antimalware, la evaluación de vulnerabilidades y la gestión de parches, pero no incluye actualizaciones de la versión del agente.

Nota
Un agente con el rol de actualizador puede descargar y distribuir parches solo para productos Windows de terceros. En el caso de los productos de Microsoft, la distribución de parches no es compatible con el agente actualizador.

Antes de asignar el rol de actualizador a un agente, asegúrese de que el equipo en el que se ejecuta el agente es lo suficientemente potente y de que tenga una conexión a internet de alta velocidad estable y espacio suficiente en el disco.

Para preparar un equipo para el rol de actualizador

1. En el equipo del agente en el que quiera habilitar el rol de actualizador, aplique las siguientes reglas del cortafuegos:
   - Entrada "updater_incoming_tcp_ports": Permite la conexión a los puertos TCP 18018 y 6888 para todos los perfiles de cortafuegos (público, privado, y dominio).
   - Entrada "updater_incoming_udp_ports": Permite la conexión al puerto UDP 6888 para todos los perfiles de cortafuegos (público, privado, y dominio).
2. Reinicie Acronis Agent Core Service.
3. Reinicie el servicio de cortafuegos.

Si no aplica estas reglas y habilita el cortafuegos, los agentes del mismo nivel descargarán las actualizaciones de la nube.

Pasos para asignar el rol de actualizador a un agente de protección

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione el equipo con el agente al que desea asignar el rol de actualizador.
3. Haga clic en **Detalles** y habilite el conmutador **Utilice este agente para descargar y distribuir parches y actualizaciones**.

La actualización de par a par funciona del siguiente modo:

1. El agente con el rol de actualizador comprueba, mediante la planificación, el archivo del índice proporcionado por el proveedor de servicios para actualizar los componentes principales.

© Acronis International GmbH, 2003-2025

2. El agente con el rol de actualizador empieza a descargar y distribuir las actualizaciones a todos los agentes.

Puede asignar el rol de actualizador a varios agentes en el entorno. De este modo, si un agente con el rol de actualizador no está conectado, otros agentes con este mismo rol serán la fuente para las actualizaciones de definición.

Recopilación automática de datos de rendimiento

En los equipos protegidos que ejecutan Microsoft Windows, los administradores de la empresa pueden habilitar o deshabilitar la recopilación automática de registros de rendimiento. La recopilación de datos comienza si el rendimiento del sistema cae por debajo de los umbrales esperados durante un período establecido de hasta 3600 segundos. El período establecido se especifica en la plataforma y los umbrales de rendimiento se configuran en el equipo donde se ejecuta el agente de protección.

La recopilación automática de registros de rendimiento está deshabilitada de manera predeterminada.

Pasos para habilitar la recopilación automática de datos de rendimiento

Rol necesario: administrador de empresa

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione el equipo en el que desea habilitar la supervisión de rendimiento.
3. Haga clic en **Detalles** y, a continuación, habilite el interruptor **Permitir que este agente recopile automáticamente los registros de rendimiento**.

La supervisión de rendimiento funciona de la siguiente manera.

1. El agente de protección supervisa varios parámetros de rendimiento en el equipo (como el uso de la memoria y la carga de la CPU).
2. Si los parámetros caen por debajo de un umbral determinado durante un período de tiempo, el agente recopila una traza ETL.
3. Una alerta (información) indica que se ha iniciado la recopilación de datos de rendimiento. La recopilación automática dura 1 hora (3600 segundos) y este período no se puede modificar.
4. Una alerta (información) indica que la recopilación de datos de rendimiento ha finalizado. Los datos recopilados automáticamente se almacenan en el disco local del equipo protegido, en la carpeta `C:\ProgramData\Acronis\ETLTool\ETL\`

Actualización de las definiciones de Cyber Protection mediante la planificación

En la pestaña **Planificación**, puede configurar la planificación de modo que actualice automáticamente las definiciones de Cyber Protection de los siguientes componentes:

© Acronis International GmbH, 2003-2025

- Antimalware
- Evaluación de vulnerabilidades
- Gestión de parches

Para cambiar la configuración de las actualizaciones de definiciones, vaya a **Configuración** > **Protección** > **Actualización de definiciones de protección** > **Planificación**.

Tipo de planificación:

- **Diaria**: defina en qué días de la semana desea que se actualicen las definiciones.
  Iniciar a las: seleccione a qué hora desea que se actualicen las definiciones.
- **Cada hora**: defina una planificación por horas más granular para las actualizaciones.
  Ejecutar cada: defina la periodicidad de las actualizaciones.
  Desde... **Hasta**: defina un intervalo de tiempo específico para las actualizaciones.

Actualización de las definiciones de Cyber Protection bajo demanda

Pasos para actualizar las definiciones de Cyber Protection para un equipo concreto bajo demanda

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione los equipos en los que desea actualizar las definiciones de protección y haga clic en **Actualizar definiciones**.

Almacenamiento en caché

La ubicación de los datos en caché es la siguiente:

- En equipos Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- En equipos Linux: `/opt/acronis/var/atp-downloader/Cache`
- En equipos macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Para cambiar la configuración del almacenamiento en caché, vaya a **Configuración** > **Protección** > **Actualización de definiciones de protección** > **Almacenamiento en caché**.

En **Datos obsoletos de los archivos de actualización y la gestión de parches**, especifique después de qué periodo desea que se eliminen los datos de la caché.

Tamaño máximo de almacenamiento en caché (GB) para agentes:

- **Función de actualizador**: defina el tamaño de almacenamiento para la caché en equipos con el rol de actualizador.
- **Otras funciones**: defina el tamaño de almacenamiento de la caché en otros equipos.

© Acronis International GmbH, 2003-2025

Nota
Cyber Protection recopila muestras de malware detectado para realizar análisis adicionales que nos permitan mejorar nuestro software. Puede cambiar esta configuración en cualquier momento en la pestaña **Protección**; para ello, desactive la opción **Recopilar y cargar muestras de malware en CPOC**.

servicios de Cyber Protection instalados en su entorno

Cyber Protection instala todos o algunos de los siguientes servicios, en función de las opciones de Cyber Protection que utilice.

Servicios instalados en Windows

Nombre del servicio	Propósito
Acronis Managed Machine Service	Ofrece copia de seguridad, recuperación, replicación, retención, función de validación
Acronis Scheduler2 Service	Ejecuta tareas programadas en ciertos eventos
Acronis Active Protection Service	Protección demostrada frente al ransomware
Acronis Cyber Protection Service	Proporciona protección antimalware

Servicios instalados en macOS

El nombre y la ubicación del servicio	Propósito
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Sirve para facilitar la comunicación entre los componentes de gestión y el agente
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Proporciona detección de malware
`/Library/LaunchDaemons/com.acronis.mms.plist`	Proporciona funcionalidades de copia de seguridad y recuperación
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Ejecuta tareas programadas

Guardar un archivo de registro del agente

Puede guardar un registro de agente en un archivo .zip. Si una copia de seguridad falla por una razón desconocida, este archivo ayudará al personal de soporte técnico a identificar el problema.

© Acronis International GmbH, 2003-2025

De forma predeterminada, la información del registro está optimizada para los últimos tres días, pero puede cambiar este período.

Cargas de trabajo en línea

Para recoger registros de agentes

1. Realice uno de los siguientes procedimientos:
   - En **Dispositivos**, seleccione la carga de trabajo de la que quiera recoger los registros y luego haga clic en **Actividades**.
   - En **Configuración** > **Agentes**, seleccione la carga de trabajo de la que quiera recoger los registros y luego haga clic en **Detalles**.
2. [Opcional] Para cambiar el período predeterminado para el cual se incluye la información del sistema, haga clic en la flecha junto al botón **Recopilar información del sistema** y luego seleccione el período.
3. Haga clic en **Recopilar información del sistema**.
4. Si se lo pide el navegador web, indique dónde quiere guardar el archivo.

Cargas de trabajo offline y dispositivos de arranque

Para recoger registros de agentes

- Siga los pasos de este artículo de la base de conocimiento.

Gestión de licencias para servidores de gestión locales

Para obtener información detallada sobre cómo activar un servidor de gestión local o cómo asignarle licencias, consulte la sección Administración de licencias en la guía del usuario de Cyber Protect.

© Acronis International GmbH, 2003-2025

Trabajo con planes

Compresión de los planes

Nota
La disponibilidad de algunas de las funciones depende de los elementos de oferta que estén habilitados para su cuenta y del nivel de administración en la consola de Cyber Protect.

Un plan es un conjunto de ajustes y reglas que puede aplicar en una o varias cargas de trabajo para alcanzar diferentes objetivos, como hacer una copia de seguridad de una carga de trabajo, proteger una carga de trabajo de malware, supervisar el rendimiento de la carga de trabajo, etc.

Un plan consta de módulos que puede habilitar o deshabilitar. Cada módulo contiene ajustes que están relacionados con una funcionalidad específica.

Todos los planes que ha creado son visibles en la pestaña **Gestión**.

Plan	Descripción	Disponible a nivel de administración		
		Socio (Todos los clientes)	Cliente	Unidad
Plan de protección	Protege los datos en la carga de trabajo. A nivel de partner, un plan de protección incluye el siguiente módulo: • **Protección antivirus y antimalware** Existen limitaciones. Para obtener más información, consulte "Uso de comodines para definir exclusiones" (p. 382). A nivel de cliente y de unidad, un plan de protección incluye los siguientes módulos: • Copia de seguridad • "Implementación de la recuperación ante desastres" (p. 1010) • Endpoint Detection and Response (EDR) • Protección antivirus y antimalware • Filtrado de URL • Antivirus Windows Defender	Sí, con limitaciones	Sí	Sí

© Acronis International GmbH, 2003-2025

Plan	Descripción	Disponible a nivel de administración		
		Socio (Todos los clientes)	Cliente	Unidad
	• Microsoft Security Essentials • Evaluación de vulnerabilidades • Gestión de parches • Mapa de protección de datos • Control de dispositivos • Advanced Data Loss Prevention Para obtener más información sobre los planes de protección, consulte "Planes de protección y módulos" (p. 249).			
Plan de administración remota	Habilita la funcionalidad de escritorio remoto y asistencia en tus cargas de trabajo gestionadas. Para obtener más información, consulte "Planes de administración remota" (p. 1450).	Sí	Sí	Sí
Plan de programación	Permite la ejecución de scripts en múltiples cargas de trabajo, la ejecución programada de scripts y la configuración de ajustes adicionales de scripts. Para obtener más información, consulte "Planes de programación" (p. 489).	Sí	Sí	Sí
Plan de supervisión	Monitorea el rendimiento, hardware, software, sistema y parámetros de seguridad de tus cargas de trabajo gestionadas. Para obtener más información, consulte "Planes de supervisión" (p. 1545).	Sí	Sí	Sí
Plan de implementación de software	Automatiza el proceso de despliegue de software y garantiza que la distribución de software en sus cargas de trabajo gestionadas sea coherente.	Sí	Sí	Sí
Copia de seguridad de aplicaciones en la nube	Realiza copias de seguridad de las aplicaciones que se ejecutan en la nube mediante agentes que funcionan en la nube y utiliza el almacenamiento en la nube como ubicación de copia de seguridad. Para obtener más información, consulte "Planes de copias	No	Sí	Sí

© Acronis International GmbH, 2003-2025

Plan	Descripción	Disponible a nivel de administración		
		Socio (Todos los clientes)	Cliente	Unidad
	de seguridad para aplicaciones en la nube" (p. 278)			
Plan de archivos comprimidos	Con el archivado de correo electrónico, todos los correos electrónicos de una organización de Microsoft 365 se conservan en un archivo comprimido externo que se almacena en la nube. Los nuevos correos electrónicos se añaden al archivo comprimido de forma continua, a medida que se envían o reciben. Para obtener más información, consulte "Archivado de correos electrónicos" (p. 762).	Sí	Sí	No
Plan de análisis de copias de seguridad	Analiza las copias de seguridad en busca de malware (incluyendo ransomware). Para obtener más información, consulte "Planes de análisis de copia de seguridad" (p. 277).	No	Sí	Sí
Plan de reenvío de SIEM	Configura cómo la información de alertas, eventos, tareas y registro de auditoría de Acronis se reenvía para su consumo por parte de plataformas de Gestión de Eventos e Incidentes de Seguridad (SIEM) de terceros. Para más información, consulte planes de reenvío de SIEM.	Sí	No	No
Réplica de copia de seguridad	Replica una copia de seguridad en otra ubicación. Para obtener más información, consulte "Réplica de copia de seguridad" (p. 261).	No	Sí	Sí
Validación	Valida una copia de seguridad y verifica que los datos de la copia de seguridad se pueden recuperar. Para obtener más información, consulte "Validación" (p. 264).	No	Sí	Sí
Limpieza	Elimina las copias de seguridad obsoletas de acuerdo con las reglas de	No	Sí	Sí

© Acronis International GmbH, 2003-2025

Plan	Descripción	Disponible a nivel de administración		
		Socio (Todos los clientes)	Cliente	Unidad
	retención. Este plan solo es aplicable a agentes y cargas de trabajo, y no a las copias de seguridad de nube a nube. Para obtener más información, consulte "Limpieza" (p. 272).			
Conversión a máquina virtual	Este plan es aplicable solo para copias de seguridad a nivel de disco. Verifica si una copia de seguridad incluye el volumen del sistema y contiene toda la información necesaria para que el sistema operativo pueda iniciar, de modo que la máquina virtual resultante se pueda iniciar por sí misma. Para obtener más información, consulte "Conversión a equipo virtual" (p. 273).	No	Sí	Sí
Replicación de equipos virtuales	Analiza las copias de seguridad en busca de malware (incluyendo ransomware). Para obtener más información, consulte "Replicación de equipos virtuales" (p. 955).	No	Sí	Sí

Planes integrados

Los planes integrados son aquellos que están preconfigurados con algunas de las configuraciones más utilizadas o recomendadas. Los planes integrados están disponibles para su selección de inmediato. No los puede cambiar, pero después de aplicar un plan integrado a una carga de trabajo, puede editar la configuración.

Los planes integración están disponibles para los siguientes tipos de planes: planes de protección, planes de supervisión y planes de administración remota.

Planes de protección integrados

La siguiente tabla proporciona más información sobre los planes de protección integrados.

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Copia de seguridad	Activado	Activado	Activado	Activado
Qué incorporar en la copia de seguridad Elementos que se incluirán en la copia de seguridad	Todo el equipo	Todo el equipo	Todo el equipo	Todo el equipo
Protección continua de datos (CDP)	Deshabilitado	Deshabilitado	Habilitado	Habilitado
Dónde guardar las copias de seguridad	Almacenamiento en la nube	Almacenamiento en la nube	Almacenamiento en la nube	Almacenamiento en la nube
Planificación	De lunes a viernes, a las 12:00 Otras opciones y condiciones de inicio habilitadas: • Si el equipo está apagado, ejecutar las	De lunes a viernes, a las 00:00 Otras opciones y condiciones de inicio habilitadas: • Si el equipo está apagado, ejecutar las tareas perdidas	De lunes a viernes, a las 00:00 Otras opciones y condiciones de inicio habilitadas: • Si el equipo está apagado, ejecutar las tareas perdidas	De lunes a viernes, a las 00:00 Otras opciones y condiciones de inicio habilitadas: • Si el equipo está apagado, ejecutar las tareas perdidas

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
	tareas perdidas al iniciar el equipo • Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada. • Ahorrar batería: No iniciar con alimentación por batería • No iniciar con conexiones de uso medido	al iniciar el equipo • Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada. • Ahorrar batería: No iniciar con alimentación por batería • No iniciar con conexiones de uso medido	al iniciar el equipo • Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada. • Ahorrar batería: No iniciar con alimentación por batería • No iniciar con conexiones de uso medido	al iniciar el equipo • Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada. • Ahorrar batería: No iniciar con alimentación por batería • No iniciar con conexiones de uso medido
Esquema de copias de seguridad	Siempre incremental	Siempre incremental	Siempre incremental	Siempre incremental

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Cuánto tiempo se conservarán	Conserve durante 90 días todas las copias de seguridad	Conserve durante 90 días todas las copias de seguridad	Conserve durante 90 días todas las copias de seguridad	Conserve durante 90 días todas las copias de seguridad
Opciones de copia de seguridad	Opciones predeterminadas	Opciones predeterminadas, más: • Ventana de copia de seguridad y rendimiento (el conjunto verde): Prioridad de la CPU: Bajo Velocidad de salida: 50 %	Opciones predeterminadas, más: • Ventana de copia de seguridad y rendimiento (el conjunto verde): Prioridad de la CPU: Bajo Velocidad de salida: 50 %	Opciones predeterminadas, más: • Ventana de copia de seguridad y rendimiento (el conjunto verde): Prioridad de la CPU: Bajo Velocidad de salida: 50 %
EDR	Desactivado	Desactivado	Activado	
Protección antivirus y antimalware	Activado	Activado	Activado	

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Active Protection	Activado	Activado	Activado	
Antimalware avanzado	Activado	Activado	Activado	
Protección de carpetas de red	Activado	Activado	Activado	
Protección del servidor	Desactivado	Desactivado	Desactivado	
Autoprotección	Activado	Activado	Activado	
Detección del proceso de criptominería	Activado	Activado	Activado	
Cuarentena	Eliminar archivos en cuarentena después de 30 días	Eliminar archivos en cuarentena después de 30 días	Eliminar archivos en cuarentena después de 30 días	
Motor de comportamiento	Cuarentena	Cuarentena	Cuarentena	
Prevención de vulnerabilidades	Notificar y detener el proceso	Notificar y detener el proceso	Notificar y detener el proceso	

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Protección en tiempo real	Cuarentena	Cuarentena	Cuarentena	
Planificar análisis	Análisis rápido: Cuarentena A las 20:00, de domingo a sábado Análisis completo: Cuarentena A las 21:00, miércoles y viernes Otras opciones y condiciones de inicio habilitadas: Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad	Análisis rápido: Cuarentena A las 20:00, de domingo a sábado Análisis completo: Cuarentena A las 21:00, miércoles y viernes Otras opciones y condiciones de inicio habilitadas: Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada.	Análisis rápido: Cuarentena A las 20:00, de domingo a sábado Análisis completo: Cuarentena A las 21:00, miércoles y viernes Otras opciones y condiciones de inicio habilitadas: Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada.	

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
	planificada.			
Exclusiones	Ninguno	Ninguno	Ninguno	
Filtrado de URL	Desactivado	Activado	Activado	
Acceso a sitio web malicioso	Bloquear	Bloquear	Bloquear	
Categorías que se pueden filtrar	Opciones predeterminadas	Opciones predeterminadas	Opciones predeterminadas	
Exclusiones	Ninguno	Ninguno	Ninguno	
Antivirus Microsoft Defender	Desactivado	Desactivado	Desactivado	
Gestión del cortafuegos	Desactivado	Activado	Activado	
Microsoft Security Essentials	Desactivado	Desactivado	Desactivado	
Evaluación de vulnerabilidades	Activado	Activado	Activado	

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Ámbito de evaluación de vulnerabilidades	Productos de Microsoft, productos de terceros para Windows, productos de Apple, productos de terceros para macOS, paquete de análisis para Linux.	Productos de Microsoft, productos de terceros para Windows, productos de Apple, productos de terceros para macOS, paquete de análisis para Linux.	Productos de Microsoft, productos de terceros para Windows, productos de Apple, productos de terceros para macOS, paquete de análisis para Linux.	
Planificación	A las 11:00, solo los miércoles y viernes	A las 11:00, solo los miércoles y viernes	A las 11:00, solo los miércoles y viernes	
Gestión de parches	Activado	Activado	Activado	
Productos de Microsoft	Todas las actualizaciones	Todas las actualizaciones	Todas las actualizaciones	
Productos de terceros a Windows	Todas las actualizaciones	Todas las actualizaciones	Todas las actualizaciones	

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Planificación	A las 12:30, solo los miércoles y viernes	A las 12:30, solo los miércoles y viernes	A las 12:30, solo los miércoles y viernes	
Copia de seguridad anterior a la actualización	Activado	Activado	Activado	
Mapa de protección de datos	Desactivado	Desactivado	Activado	
Extensiones y reglas de excepción	–	–	Opciones predeterminadas (66 extensiones a detectar)	
Planificación	–	–	De lunes a viernes, a las 15:40	
Control de dispositivos	Desactivado	Desactivado	Desactivado	
Configuración del acceso	Permitido: todos	Permitido: todos	Permitido: todos	

© Acronis International GmbH, 2003-2025

Módulos y configuración	Planes de protección integrados			
	Protección esencial	**Protección ampliada**	**Protección completa**	**Realice una copia de seguridad de toda la carga de trabajo**
	Tiempo de inactividad mínimo y pérdida de datos, recuperación sin esfuerzo con un objetivo de punto de recuperación (RPO) corto y mantenimiento fácil	**Segundo nivel de protección: continuidad del negocio, mitigación proactiva de riesgos de seguridad y cumplimiento**	**Tercer nivel de protección: Continuidad del negocio, objetivo de punto de recuperación (RPO) casi nulo, mitigación proactiva de riesgos de seguridad, prevención de fugas de datos y cumplimiento normativo**	**Realiza una copia de seguridad de todos los recursos informáticos en la nube**
Lista de tipos de dispositivo permitidos	1 USB HID (ratón, teclado, etc.) permitido	1 USB HID (ratón, teclado, etc.) permitido	1 USB HID (ratón, teclado, etc.) permitido	
Lista de dispositivos USB permitidos	Vacío	Vacío	Vacío	
Exclusión	Ninguno	Ninguno	Ninguno	
Prevención de pérdida de datos	Desactivado	Desactivado	Desactivado	
Modo	–	–	–	
Configuraciones avanzadas	–	–	–	
Disaster Recovery	Desactivado	Desactivado	Desactivado	

Para obtener más información sobre los planes de protección, consulte "Planes de protección y módulos" (p. 249).

Planes de supervisión integrados

La siguiente tabla proporciona más información sobre los planes de supervisión integrados.

© Acronis International GmbH, 2003-2025

Nombre	Descripción	Supervisiones habilitadas
Recomendado para la supervisión de Windows	Supervisa el estado y el rendimiento de los equipos Windows	Las siguientes 13 supervisiones están habilitadas en este plan: • Estado de software antimalware • Estado de la función de AutoRun • Temperatura de CPU • Uso de la CPU • Espacio de disco • Velocidad de transferencia del disco • Error al iniciar sesión • Estado del cortafuegos • Temperatura de GPU • Último reinicio del sistema • Uso de la memoria • Uso de la red • Estado de Windows Update
Recomendado para la supervisión de macOS	Supervisa el estado y el rendimiento de los equipos macOS	Las siguientes 10 supervisiones están habilitadas en este plan: • Estado de software antimalware • Temperatura de CPU • Uso de la CPU • Espacio de disco • Velocidad de transferencia del disco • Estado del cortafuegos • Temperatura de GPU • Último reinicio del sistema • Uso de la memoria • Uso de la red
Recomendado para la supervisión de servidores	Supervisa el estado y el rendimiento de los servidores de Windows	Las siguientes 20 supervisiones están habilitadas en este plan: • Estado de software antimalware • Temperatura de la CPU, 2 monitores: 80 grados, 10 minutos, advertencia

© Acronis International GmbH, 2003-2025

Nombre	Descripción	Supervisiones habilitadas
		90 grados, 10 minutos, crítico • Uso de CPU, 3 monitores: Menos del 20 %, 10 min, información Más del 80 %, 10 min, advertencia Más del 90 %, 10 min, crítico • Espacio en disco, 2 monitores: Menos del 20 %, 30 min, advertencia Menos del 10%, 30 min, crítico • Velocidad de transferencia del disco • Inicios de sesión fallidos, 3 monitores: 5 intentos, 1 hora, información 10 intentos, 1 hora, advertencia 20 intentos, 1 hora, crítico • Estado del cortafuegos • Cambios del hardware • Software instalado • Uso de memoria, 3 monitores: Menos del 20 %, 10 min, información Más del 80 %, 10 min, advertencia Más del 90 %, 10 min, crítico • Uso de la red • Estado de Windows Update

Para obtener más información sobre los planes de supervisión, consulte "Planes de supervisión" (p. 1545).

Planes de administración remota integrados

La siguiente tabla proporciona más información sobre el plan de administración remota integrada.

Nombre	Descripción	Configuración
Escritorio remoto esencial	Habilita las capacidades de escritorio remoto y transferencia de archivos	Protocolos de conexión **Permitir conexiones a través de NEAR**: activado Configuración de seguridad NEAR

© Acronis International GmbH, 2003-2025

Nombre	Descripción	Configuración
		• **Bloquear carga de trabajo cuando el usuario se desconecta de la sesión de consola**: desactivado • **Permitir que solo un usuario se conecte con NEAR o transferir archivos a la vez**: desactivado • **Permitir al administrador de carga de trabajo conectarse a cualquier sesión**: activado • **Permitir la creación de sesiones del sistema**: desactivado • **Permitir la sincronización del portapapeles**: activado **Permitir conexiones a través de RDP**: activado **Permitir conexiones a través del uso compartido de pantalla de Apple**: desactivado Configuración de seguridad • **Mostrar si la carga de trabajo se controla de forma remota**: activado • **Solicitar permiso al usuario para tomar capturas de pantalla de la carga de trabajo**: activado Gestión de la carga de trabajo • **Transferencia de archivos**: activado • **Transmisión de capturas de pantalla**: desactivado Configuración de pantalla • **Usar deduplicación de escritorio para la captura de escritorio**: activado • **Usar aceleración OpenCL**: activado • **Usar codificación de hardware H.264**: activado Caja de herramientas **Mostrar los últimos usuarios que han iniciado sesión**: desactivado

Para obtener más información sobre los planes de administración remota, consulte "Planes de administración remota" (p. 1450).

© Acronis International GmbH, 2003-2025

Planes predeterminados

El plan predeterminado es un plan que está preseleccionado y se muestra primero en las listas de planes y en los campos de selección de planes. Puede tener un solo plan predeterminado por inquilino y tipo de plan admitido a la vez.

La lista de planes y el plan predeterminado que verá dependerán del nivel en el que esté utilizando la consola de Protección.

Por ejemplo, si está utilizando la consola en el nivel de partner, verá los planes que se crearon en los niveles de partner, cliente y unidad, pero los planes predeterminados serán los que se establecieron como predeterminados en el nivel de partner. Si está utilizando la consola en el nivel de cliente, no verá ningún plan que se haya creado en el nivel de partner, incluidos los planes predeterminados en el nivel de partner. Del mismo modo, si está utilizando la consola en el nivel de unidad, no verá ningún plan que se haya creado en los niveles de partner o cliente, incluidos los planes predeterminados en estos niveles.

Los planes predeterminados son compatibles con los siguientes tipos de planes: planes de protección, planes de supervisión y planes de administración remota.

Establecimiento de planes como predeterminados

Puede establecer un plan de los tipos de planes admitidos (plan de protección, plan de supervisión o plan de administración remota) como predeterminado.

Nota
La función no está disponible para los usuarios a los que se les ha asignado el rol de **Administrador de solo lectura** para el servicio de protección.

Planes de protección

Requisitos previos

Se ha creado al menos un plan de protección para su inquilino. Para obtener más información, consulte "Creación de un plan de protección" (p. 250).

Para establecer un plan de protección como predeterminado

1. En la pantalla de **Planes de protección**, seleccione el plan que desee establecer como predeterminado y luego haga clic en **Detalles**.
2. Haga clic en el icono de puntos suspensivos y, luego, en **Establecer como predeterminado**.
3. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla **Planes de protección**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Planes de administración remota

Requisitos previos

© Acronis International GmbH, 2003-2025

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se crea al menos un plan de administración remota para su inquilino. Para obtener más información, consulte "Creación de un plan de administración remota" (p. 1450).

Para establecer un plan de administración remota como predeterminado

1. En la pantalla **Planes de administración remota**, localice el plan que desee establecer como predeterminado.
2. En la misma fila, haga clic en el icono de **Más acciones**.
3. Haga clic en **Establecer como predeterminado**.
4. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla **Planes de administración remota**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Planes de supervisión

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se crea al menos un plan de supervisión para su inquilino. Para obtener más información, consulte "Crear un plan de supervisión" (p. 1545).

Para establecer un plan de supervisión como predeterminado

1. En la pantalla **Planes de supervisión**, localice el plan que desee establecer como predeterminado.
2. En la misma fila, haga clic en el icono de **Más acciones**.
3. Haga clic en **Establecer como predeterminado**.
4. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla de **Planes de supervisión**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Borrado de planes predeterminados

Puede borrar el plan de protección predeterminado. Después de hacerlo, el plan dejará de estar preseleccionado en los campos de selección de planes.

Nota
La función no está disponible para los usuarios a los que se les ha asignado el rol de **Administrador de solo lectura** para el servicio de protección.

Planes de protección

Requisitos previos

Se crea un plan de protección para su inquilino y se establece como predeterminado. Para obtener más información, consulte "Creación de un plan de protección" (p. 250).

© Acronis International GmbH, 2003-2025

Pasos para borrar un plan de protección predeterminado

1. En la pantalla **Planes de protección**, seleccione el plan predeterminado y haga clic en **Detalles**.
2. Haga clic en el icono de puntos suspensivos (...) y, luego, en **Borrar predeterminado**.
3. En la ventana de confirmación, haga clic en **Borrar**.
   En la pantalla **Planes de protección**, desaparece la etiqueta **Predeterminado** situada junto al nombre del plan.

Planes de administración remota

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se crea un plan de administración remota para su inquilino y se establece como predeterminado. Para obtener más información, consulte "Creación de un plan de administración remota" (p. 1450).

Para desasignar un plan de administración remota como predeterminado

1. En la pantalla **Planes de administración remota**, localice el plan predeterminado que desee desasignar como tal.
2. En la misma fila, haga clic en el icono de puntos suspensivos (...).
3. Haga clic en **Borrar predeterminado**.
4. En la ventana de confirmación, haga clic en **Borrar**.
   En la pantalla **Planes de administración remota**, desaparece la etiqueta **Predeterminado** que había junto al nombre del plan.

Planes de supervisión

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se crea un plan de supervisión para su inquilino y se establece como predeterminado. Para obtener más información, consulte "Crear un plan de supervisión" (p. 1545).

Pasos para desasignar un plan de protección como predeterminado

1. En la pantalla **Planes de supervisión**, localice el plan que desee quitar como predeterminado.
2. En la misma fila, haga clic en el icono de puntos suspensivos (...).
3. Haga clic en **Borrar predeterminado**.
4. En la ventana de confirmación, haga clic en **Borrar**.
   En la pantalla **Planes de supervisión**, desaparece la etiqueta **Predeterminado** que había junto al nombre del plan.

© Acronis International GmbH, 2003-2025

Planes favoritos

Los planes favoritos aparecen en la parte superior de la lista de planes, después de los planes predeterminados. Puede añadir un plan a los favoritos si desea asegurarse de que sea visible y fácil de encontrar, incluso cuando su organización tenga muchos planes.

La lista de planes y los planes favoritos que verá dependerán del nivel en el que esté utilizando la consola de Protección.

Por ejemplo, si está utilizando la consola en el nivel de partner, verá los planes que se crearon en todos los niveles (partner, cliente y unidad), pero los planes favoritos serán los planes que se agregaron a favoritos en el nivel de partner. Si está utilizando la consola en el nivel de cliente, no verá ningún plan que se haya creado en el nivel de partner, incluidos los planes favoritos en el nivel de partner. Del mismo modo, si está utilizando la consola en el nivel de unidad, no verá ningún plan que se haya creado en los niveles de partner o cliente, incluidos los planes favoritos en estos niveles.

Los planes favoritos son compatibles con los siguientes tipos de planes: planes de protección, planes de supervisión y planes de administración remota.

Establecimiento de planes como favoritos

Puede configurar hasta 10 planes favoritos por tipo de plan admitido (plan de protección, plan de supervisión o plan de administración remota) por inquilino.

Nota
La función no está disponible para los usuarios a los que se les ha asignado el rol de **Administrador de solo lectura** para el servicio de protección.

Planes de protección

Requisitos previos

Se ha creado al menos un plan de protección para su inquilino. Para obtener más información, consulte "Creación de un plan de protección" (p. 250).

Para establecer un plan de protección como favorito

1. En la pantalla de **Planes de protección**, haga clic en el plan que desee establecer como favorito y luego haga clic en **Detalles**.
2. Haga clic en el icono de puntos suspensivos (...) y, luego, en **Añadir a favoritos**.
   En la pantalla **Planes de protección**, aparece un icono de estrella junto al nombre del plan.

Planes de administración remota

Requisitos previos

© Acronis International GmbH, 2003-2025

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se crea al menos un plan de administración remota para su inquilino. Para obtener más información, consulte "Crear un plan de supervisión" (p. 1545).

Para establecer un plan de administración remota como favorito

1. En la pantalla **Planes de administración remota**, localice el plan que desee añadir a favoritos.
2. En la fila del plan, haga clic en el icono de puntos suspensivos (...).
3. Haga clic en **Agregar a favoritos**.
   En la pantalla **Planes de administración remota**, aparece un icono de estrella junto al nombre del plan.

Planes de supervisión

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se crea al menos un plan de administración para su inquilino. Para obtener más información, consulte "Crear un plan de supervisión" (p. 1545).

Para marcar un plan de supervisión como favorito

1. En la pantalla de **Planes de supervisión**, localice el plan que desee establecer como favorito.
2. En la fila del plan, haga clic en el icono de puntos suspensivos (...).
3. Haga clic en **Agregar a favoritos**.
   En la pantalla de **Planes de supervisión**, aparece un icono de estrella junto al nombre del plan.

Eliminación de planes de favoritos

Puede eliminar planes de protección favoritos, planes de supervisión y planes de administración remota de la lista de favoritos.

Nota
La función no está disponible para los usuarios a los que se les ha asignado el rol de **Administrador de solo lectura** para el servicio de protección.

Planes de protección

Requisitos previos

Al menos un plan de protección está establecido como favorito para su inquilino.

Para eliminar un plan de protección de los favoritos

1. En la pantalla de **Planes de protección**, haga clic en el plan que desea eliminar de favoritos y luego, en **Detalles**.
2. Haga clic en el icono de puntos suspensivos (...) y luego en **Eliminar de favoritos**.

© Acronis International GmbH, 2003-2025

En la pantalla de **Planes de protección**, el icono de estrella junto al nombre del plan desaparece.

Planes de administración remota

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Al menos un plan de administración remota está establecido como favorito para su inquilino.

Para eliminar un plan de administración remota de los favoritos

1. En la pantalla de **Planes de administración remota**, localice el plan que desea eliminar de tus favoritos.
2. En la fila del plan, haga clic en el icono de puntos suspensivos (...).
3. Haga clic en **Eliminar de favoritos**.
   En la pantalla de **Planes de administración remota**, el icono de estrella junto al nombre del plan desaparece.

Planes de supervisión

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Al menos un plan de supervisión está establecido como favorito para su inquilino.

Para eliminar un plan de supervisión de los favoritos

1. En la pantalla de **Planes de supervisión**, localice el plan que desea eliminar de tus favoritos.
2. En la fila del plan, haga clic en el icono de puntos suspensivos (...).
3. Haga clic en **Eliminar de favoritos**.
   En la pantalla de **Planes de supervisión**, el icono de estrella junto al nombre del plan desaparece.

Establecer el orden de los planes favoritos

Puede establecer el orden en que se mostrarán los planes que se han establecido como favoritos en los campos de selección de planes.

Puede configurar hasta 10 planes favoritos por tipo de plan admitido (plan de protección, plan de supervisión o plan de administración remota) por inquilino.

Nota
La función no está disponible para los usuarios a los que se les ha asignado el rol de **Administrador de solo lectura** para el servicio de protección.

Planes de protección

Requisitos previos

© Acronis International GmbH, 2003-2025

Se han establecido al menos dos planes como favoritos.

Para establecer el orden de los planes favoritos

1. En la pantalla de planes de la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Haga clic en **Gestionar favoritos**.
3. Arrastre y suelte los planes para establecer el orden en el que aparecerán en los campos de selección de planes.

   Nota
   Para poder arrastrar un plan, haga clic en el área de arrastre antes del nombre del plan.

4. Haga clic en **Guardar**.

Planes de administración remota

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se han establecido al menos dos planes como favoritos.

Para establecer el orden de los planes favoritos

1. En la pantalla de planes de la consola de Cyber Protect, vaya a **Gestión** > **Planes de administración remota**.
2. Haga clic en **Gestionar favoritos**.
3. Arrastre y suelte los planes para establecer el orden en el que aparecerán en los campos de selección de planes.

   Nota
   Para poder arrastrar un plan, haga clic en el área de arrastre antes del nombre del plan.

4. Haga clic en **Guardar**.

Planes de supervisión

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Se han establecido al menos dos planes como favoritos.

Para establecer el orden de los planes favoritos

1. En la pantalla de planes de la consola de Cyber Protect, vaya a **Gestión** > **Planes de supervisión**.
2. Haga clic en **Gestionar favoritos**.
3. Arrastre y suelte los planes para establecer el orden en el que aparecerán en los campos de selección de planes.

© Acronis International GmbH, 2003-2025

Nota
Para poder arrastrar un plan, haga clic en el área de arrastre antes del nombre del plan.

4. Haga clic en **Guardar**.

Planes preseleccionados

Si la autenticación de doble factor (2FA) está habilitada para su cuenta, se preseleccionan un plan de protección, un plan de supervisión y un plan de administración remota cuando registra una carga de trabajo en la consola de Cyber Protect.

Puede cambiar la selección o elegir no aplicar un plan a la carga de trabajo. Para obtener más información, consulte "Registro de cargas de trabajo utilizando la interfaz gráfica de usuario" (p. 110).

Los planes preseleccionados dependen de lo siguiente:

- Rol del usuario que registra la carga de trabajo.
- Cuenta bajo la cual se registrará la carga de trabajo.
- Disponibilidad del plan.

La siguiente tabla resume las opciones posibles, que se enumeran jerárquicamente. Si una opción no está disponible, se aplica la siguiente de la lista. Si todas las opciones posibles no están disponibles, no se preseleccionará ningún plan.

Rol del usuario que registra la carga de trabajo	Cuenta bajo la cual se registrará la carga de trabajo	
	Cuenta en un inquilino-cliente	**Cuenta en una unidad**
Cuenta a nivel de partner con uno de los siguientes roles en el servicio **Protección**: • **Administrador de la empresa** • **Administrador de cibernética** • **Administrador**	1. Plan predeterminado a nivel de cliente 2. Plan predeterminado a nivel de partner 3. Primer plan favorito a nivel de cliente 4. Primer plan favorito a nivel de partner 5. Plan seleccionado aleatoriamente a nivel de cliente 6. Plan seleccionado aleatoriamente a nivel de partner 7. Plan integrado* (aplicado como plan a nivel de cliente)	1. Plan predeterminado a nivel de unidad 2. Plan predeterminado a nivel de cliente 3. Plan predeterminado a nivel de partner 4. Primer plan favorito a nivel de unidad 5. Primer plan favorito a nivel de cliente 6. Primer plan favorito a nivel de partner 7. Plan seleccionado aleatoriamente a nivel de unidad 8. Plan seleccionado aleatoriamente a nivel de cliente 9. Plan seleccionado aleatoriamente a

© Acronis International GmbH, 2003-2025

Rol del usuario que registra la carga de trabajo	Cuenta bajo la cual se registrará la carga de trabajo	
	Cuenta en un inquilino-cliente	**Cuenta en una unidad**
		nivel de partner 10. Plan integrado* (aplicado como plan a nivel de cliente)
Cuenta a nivel de cliente con uno de los siguientes roles en el servicio **Protección**: • **Administrador de la empresa** • **Administrador de cibernética** • **Administrador**	1. Plan predeterminado a nivel de cliente 2. Primer plan favorito a nivel de cliente 3. Plan seleccionado aleatoriamente a nivel de cliente 4. Plan integrado*	1. Plan predeterminado a nivel de unidad 2. Plan predeterminado a nivel de cliente 3. Primer plan favorito a nivel de unidad 4. Primer plan favorito a nivel de cliente 5. Plan seleccionado aleatoriamente a nivel de unidad 6. Plan seleccionado aleatoriamente a nivel de cliente 7. Plan integrado*
Cuenta a nivel de cliente con el rol de **Usuario** en el servicio **Protección**	1. Plan predeterminado a nivel de cliente (si el plan es creado por ese usuario) 2. Primer plan favorito a nivel de cliente (si el plan es creado por ese usuario) 3. Plan seleccionado aleatoriamente que es creado por ese usuario a nivel de cliente 4. Plan integrado*	N/D
Cuenta a nivel de unidad con uno de los siguientes roles en el servicio **Protección**: • **Administrador de unidad** • **Administrador de cibernética** • **Administrador**	N/D	1. Plan predeterminado a nivel de unidad 2. Primer plan favorito a nivel de unidad 3. Plan seleccionado aleatoriamente a nivel de unidad 4. Plan integrado*
Cuenta a nivel de	N/D	1. Plan predeterminado a nivel de

© Acronis International GmbH, 2003-2025

Rol del usuario que registra la carga de trabajo	Cuenta bajo la cual se registrará la carga de trabajo	
	Cuenta en un inquilino-cliente	Cuenta en una unidad
unidad con el rol de **Usuario** en el servicio **Protección**		unidad (si el plan es creado por ese usuario) 2. Primer plan favorito a nivel de unidad (si el plan es creado por ese usuario) 3. Plan seleccionado aleatoriamente que es creado por ese usuario a nivel de unidad 4. Plan integrado*

* Solo disponible para planes de protección.

Planes en diferentes niveles de administración

Dependiendo de su nivel jerárquico, los administradores pueden crear y gestionar planes en los siguientes niveles:

- Nivel de partner (**Todos los clientes**)
- Nivel de cliente
- Nivel de unidad

Para obtener más información, consulte "Niveles de administración en la consola de Cyber Protect" (p. 373).

Los administradores de nivel superior pueden crear y aplicar planes en su propio inquilino y en los inquilinos secundarios que gestionan. Los administradores de nivel inferior tienen acceso de solo lectura a los planes que aplican los administradores de nivel superior y no pueden eliminar, editar o revocar estos planes.

Cuando trabaja en un nivel de administración inferior, un administrador de nivel superior tiene los derechos del administrador de nivel inferior. Por ejemplo, cuando un administrador de partner trabaja a nivel de cliente, el administrador de partner tiene los derechos de un administrador de clientes.

La siguiente tabla resume los planes en diferentes niveles de administración, según la jerarquía de administradores.

Jerarquía de administradores	Nivel de administración	Planes	Access
Cuenta a nivel de partner con uno de los siguientes roles en el servicio **Protección**:	Nivel de partner	Planes de partner (propietario*)	Acceso completo

© Acronis International GmbH, 2003-2025

Jerarquía de administradores	Nivel de administración	Planes	Access
• **Administrador de la empresa** • **Administrador de cibernética** • **Administrador**			
		Planes de cliente, incluidos los planes de las unidades	Acceso completo
		Planes de unidad	Acceso completo
	Nivel de cliente (para clientes gestionados por el proveedor de servicios)	Planes de partner que se aplican a las cargas de trabajo de este cliente	Sólo lectura
		Planes de cliente, incluidos los planes de las unidades (propietario*)	Acceso completo
		Planes de unidad	Acceso completo
	Nivel de unidad (para clientes gestionados por el proveedor de servicios)	Planes de partner que se aplican a las cargas de trabajo de esta unidad	Sólo lectura
		Planes de cliente que se aplican a las cargas de trabajo de esta unidad	Sólo lectura
		Planes de unidad (propietario*)	Acceso completo
Cuenta a nivel de cliente con uno de los siguientes roles en el servicio **Protección**: • **Administrador de la empresa** • **Administrador de cibernética** • **Administrador**	Nivel de cliente	Planes de partner que se aplican a las cargas de trabajo de este cliente o unidad	Sólo lectura
		Planes de cliente, incluidos los planes de las unidades (propietario*)	Acceso completo
		Planes de unidad	Acceso completo
	Nivel de unidad	Planes de partner que se aplican a las cargas de trabajo de esta unidad	Sólo lectura
		Planes de cliente que se aplican a las cargas de trabajo de esta unidad	Sólo lectura
		Planes de unidad (propietario*)	Acceso

© Acronis International GmbH, 2003-2025

Jerarquía de administradores	Nivel de administración	Planes	Access
			completo
Cuenta a nivel de unidad con uno de los siguientes roles en el servicio **Protección**: • **Administrador de unidad** • **Administrador de cibernética** • **Administrador**	Nivel de unidad	Planes de partner que se aplican a las cargas de trabajo de esta unidad	Sólo lectura
		Planes de cliente que se aplican a las cargas de trabajo de esta unidad	Sólo lectura
		Planes de unidad (propietario*)	Acceso completo

* El propietario de un plan es el inquilino en el que se creó el plan. Por ejemplo, si un administrador de partner crea un plan a nivel de cliente, el inquilino del cliente es el propietario de ese plan. Si un administrador de partner crea un plan a nivel de partner (**Todos los clientes**), el inquilino del partner es el propietario del plan.

No todos los tipos de planes están disponibles en todos los niveles de administración. Para obtener más información, consulte "Compresión de los planes" (p. 221).

Estado del plan

Para algunos planes, como los planes de protección y los planes de replicación de máquinas virtuales, hay disponible una barra de estado con códigos de color en la que puede pulsar. Indica el estado del plan en todos las cargas de trabajo en las que se aplica dicho plan, de la siguiente manera:

- Correcto (verde)
- Advertencia (naranja)
- Error (rojo)
- El plan se está ejecutando (azul)
- El plan está deshabilitado (gris)

Puede hacer clic en una sección de la barra de estado para ver el número de cargas de trabajo que tienen el correspondiente estado.

Nota
El estado de un plan puede no corresponder con el estado de la carga de trabajo. Por ejemplo, un plan de protección puede aplicarse correctamente a una carga de trabajo, por lo que su estado aparecerá como **CORRECTO** (verde). Al mismo tiempo, la carga de trabjo podría estar sin conexión, por lo que su estado en la pestaña **Dispositivos** será rojo.

© Acronis International GmbH, 2003-2025

Planes de protección y módulos

Para proteger sus datos, debe crear planes de protección y luego aplicarlos a sus cargas de trabajo.

Un plan de protección consiste en distintos módulos de protección. Habilite los módulos que necesite y configúrelos para crear planes de protección adaptados a sus necesidades específicas.

Los siguientes módulos están disponibles:

- Copia de seguridad. Realiza copias de seguridad de sus orígenes de datos a un almacenamiento local o en la nube.
- "Implementación de la recuperación ante desastres" (p. 1010). Inicia copias exactas de los equipos en el sitio de la nube y traslada la carga de trabajo de los equipos originales dañados a los servidores de recuperación en la nube.
- Protección antivirus y antimalware. Comprueba sus cargas de trabajo con una solución antimalware integrada.
- Endpoint Detection and Response (EDR). Detecta actividad sospechosa en la carga de trabajo, incluidos los ataques que no se han detectado, y genera incidentes que le ayudan a entender cómo ocurrió un ataque y cómo impedir que vuelva a ocurrir.
- Filtrado de URL. Protege sus máquinas de amenazas que se originan en Internet, bloqueando el acceso a URL maliciosas y contenido descargable.
- Antivirus Windows Defender. Gestiona la configuración del antivirus Windows Defender para proteger su entorno.
- Microsoft Security Essentials. Gestiona la configuración de Microsoft Security Essentials para proteger su entorno.
- Evaluación de vulnerabilidades. Realiza comprobaciones en los productos de Windows, Linux, macOS, de terceros de Microsoft y de terceros de macOS instalados en sus equipos por si hay vulnerabilidades y le envía notificaciones sobre ellas.
- Gestión de parches. Instala parches y actualizaciones para productos de Windows, Linux, macOS, de terceros de Microsoft y de terceros de macOS en sus equipos con el fin de resolver las vulnerabilidades detectadas.
- Mapa de protección de datos. Detecta datos para supervisar el estado de la protección de archivos importantes.
- Control de dispositivos. Especifica los dispositivos que pueden utilizar o no lo usuarios en sus equipos.
- Advanced Data Loss Prevention. Evita la filtración de datos confidenciales a través de dispositivos periféricos (como impresoras o almacenamiento extraíble) o mediante transferencias de red internas y externas, según una directiva de flujo de datos.

Nota
La disponibilidad del módulo depende de los elementos de oferta que están habilitados para su cuenta y el nivel de administración en la consola de Cyber Protect. Para obtener más información, consulte "Compresión de los planes" (p. 221).

© Acronis International GmbH, 2003-2025

Creación de un plan de protección

Puede crear un plan de protección de las siguientes formas:

- En la pestaña **Dispositivos**. Seleccione una o más cargas de trabajo que desee proteger y, a continuación, cree un plan de protección para ellas.
- En la pestaña **Gestión** > **Planes de protección**. Cree un plan de protección y seleccione una o más cargas de trabajo a las que se va a aplicar el plan.

Al crear un plan de protección, solo se muestran los módulos aplicables a su tipo de carga de trabajo.

Puede aplicar un plan de protección a más de una carga de trabajo. También puede aplicar múltiples planes de protección a la misma carga de trabajo. Para obtener más información acerca de posibles conflictos, consulte "Resolver problemas de compatibilidad" (p. 258).

Pasos crear un plan de protección

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las cargas de trabajo que quiera proteger y, a continuación, haga clic en **Proteger**.
3. [Si ya hay planes aplicados] Haga clic en **Agregar plan**.
4. Haga clic en **Crear plan** > **Protección**.
   Se abre el panel del plan de protección.
5. [Opcional] Para cambiar el nombre del plan de protección, haga clic en el icono del lápiz y luego introduzca el nuevo nombre.
6. [Opcional] Para habilitar o deshabilitar un módulo del plan, active el conmutador que se encuentra junto al nombre del módulo.
7. [Opcional] Para configurar un módulo, haga clic en él para ampliarlo y cambie los ajustes según sus necesidades.
8. Cuando tenga todo listo, haga clic en **Crear**.

Nota
Para crear un plan de protección con cifrado, especifique una contraseña de cifrado. Para más información, consulte "Cifrado" (p. 583).

Administración > Planes de protección

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Haga clic en **Crear plan**.
   Se abrirá la plantilla del plan de protección.
3. [Opcional] Para cambiar el nombre del plan de protección, haga clic en el icono del lápiz y luego introduzca el nuevo nombre.

© Acronis International GmbH, 2003-2025

4. [Opcional] Para habilitar o deshabilitar un módulo del plan, active el conmutador que se encuentra junto al nombre del módulo.
5. [Opcional] Para configurar un módulo, haga clic en él para ampliarlo y cambie los ajustes según sus necesidades.
6. [Opcional] Haga clic en **Añadir dispositivos** para seleccionar las cargas de trabajo en las que desee que se aplique el plan.

   Nota
   Puede crear un plan sin aplicarlo a ninguna carga de trabajo. Puede agregar cargas de trabajo más tarde editando el plan. Para obtener más información sobre cómo agregar una carga de trabajo a un plan, consulte "Aplicación de un plan de protección a una carga de trabajo" (p. 252).

7. Cuando tenga todo listo, haga clic en **Crear**.

   Nota
   Para crear un plan de protección con cifrado, especifique una contraseña de cifrado. Para más información, consulte "Cifrado" (p. 583).

Para ejecutar un módulo bajo demanda (como los de **Copia de seguridad**, **Protección antivirus y antimalware**, **Evaluación de vulnerabilidades**, **Gestión de parches** o **Mapa de protección de datos**) haga clic en **Ejecutar ahora**.

Vea el vídeo explicativo Creación del primer plan de protección.

Para obtener más información sobre el módulo de recuperación ante desastres, consulte "Creación de un plan de protección de recuperación ante desastres" (p. 1016).

Para obtener más información sobre el módulo de control de dispositivos, consulte "Cómo trabajar con el módulo de control de dispositivos" (p. 434).

Acciones con planes de protección

Tras crear un plan de protección, puede llevar a cabo las siguientes acciones:

- Aplicar un plan a una carga de trabajo o grupo de dispositivos.
- Cambiar el nombre a un plan.
- Editar un plan.
  Puede habilitar y deshabilitar los módulos de un plan y cambiar su configuración.
- Habilitar o deshabilitar un plan.
  Un plan deshabilitado no se ejecutará en las cargas de trabajo a las que se aplica.
  Esta acción es útil para aquellos administradores que pretenden proteger la misma carga de trabajo con el mismo plan más adelante. El plan no se revoca de la carga de trabajo y solo tiene que volver a habilitarlo para restaurar la protección.
- Revocar un plan de una carga de trabajo.
  Un plan revocado deja de aplicarse a la carga de trabajo.

© Acronis International GmbH, 2003-2025

Esta acción es útil para aquellos administradores que no necesitan proteger la misma carga de trabajo rápidamente con el mismo plan de nuevo. Para restaurar la protección de un plan revocado, debe saber el nombre del plan, seleccionarlo de la lista de planes disponibles y luego volver a aplicarlo a la carga de trabajo correspondiente.

- Detener un plan.
  Esta acción detiene todas las operaciones de copia de seguridad en ejecución de todas las cargas de trabajo a las que se aplica el plan. Las copias de seguridad comenzarán de nuevo según la planificación del plan.
  Esta acción no afectará al análisis antimalware, que se llevará a cabo según se haya configurado en el plan.
- Clonar un plan.
  Puede crear una copia exacta de un plan ya existente. El nuevo plan no se asigna a ninguna carga de trabajo.
- Exportar e importar un plan.
  Puede exportar un plan como un archivo JSON, que más adelante podrá importar de nuevo. Por lo tanto, no tiene que crear un nuevo plan manualmente ni configurarlo.

Nota
Esta función no está disponible para planes a nivel de partner. Para obtener más información sobre este nivel, consulte "Niveles de administración en la consola de Cyber Protect" (p. 373).

- Comprobar los detalles de un plan.
- Comprobar las actividades y alertas relacionadas con un plan.
- Eliminar un plan.

Aplicación de un plan de protección a una carga de trabajo

Para proteger una carga de trabajo, debe aplicarle un plan de protección.

Puede aplicar un plan desde la pestaña **Dispositivos** y la pestaña **Gestión** > **Planes de protección**.

Dispositivos

1. Seleccione una o más cargas de trabajo que desee proteger.
2. Haga clic en **Proteger**.
3. [Si ya se aplica un plan de protección común a las cargas de trabajo seleccionadas] Haga clic en **Agregar plan**.
   Se muestra una lista con los planes de protección disponibles.
4. Seleccione el plan de protección que desee aplicar y, a continuación, haga clic en **Aplicar**.

Administración > Planes de protección

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Seleccione el plan de protección que desee aplicar.

© Acronis International GmbH, 2003-2025

3. Haga clic en **Editar**.
4. Haga clic en **Gestionar dispositivos**.
5. En la ventana **Dispositivos**, haga clic en **Agregar**.
6. Seleccione las cargas de trabajo a las que quiera aplicar el plan y, a continuación, haga clic en **Agregar**.
7. En la ventana **Dispositivos**, haga clic en **Listo**.
8. En el panel del plan de protección, haga clic en **Guardar**.

Para obtener información sobre cómo aplicar un plan de protección a un grupo de dispositivos, consulte "Aplicar un plan a un grupo" (p. 433).

Edición de un plan de protección

Cuando edite un plan, puede habilitar y deshabilitar los módulos que contenga y cambiar su configuración.

Puede editar un plan de protección para todas las cargas de trabajo a las que se aplique o solo para algunas.

Puede editar un plan desde la pestaña **Dispositivos** y desde la pestaña **Gestión** > **Planes de protección**.

Dispositivos

1. Seleccione una o más cargas de trabajo a las que se aplica el plan.
2. Haga clic en **Proteger**.
3. Seleccione el plan de protección que desee editar.
4. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan y, a continuación, haga clic en **Editar**.
5. Haga clic en un módulo que quiera editar y configúrelo según sea necesario.
6. Haga clic en **Guardar**.
7. [Si no ha seleccionado todas las cargas de trabajo a las que se aplica el plan] Seleccione el ámbito de edición:
   - Para editar el plan para todas las cargas de trabajo a las que se aplica, haga clic en **Aplicar los cambios a este plan de protección (esto afectará a otros dispositivos)**.
   - Para cambiar el plan solo para algunas cargas de trabajo, haga clic en **Crear un nuevo plan de protección solamente para los dispositivos seleccionados**.

     Como resultado, el plan existente se revocará de las cargas de trabajo seleccionadas. Se creará un nuevo plan de protección con la configuración que haya realizado y se aplicará a estas cargas de trabajo.

Administración > Planes de protección

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Seleccione el plan de protección que desee editar.
3. Haga clic en **Editar**.
4. Haga clic en los módulos que quiera editar y configúrelos según sea necesario.
5. Haga clic en **Guardar**.

Nota
Editar un plan en la pestaña **Gestión** > **Planes de protección** afecta a todas las cargas de trabajo a las que se aplica ese plan.

Exportar un plan de protección

Puede exportar un plan de protección en un archivo JSON.

Nota
Esta función no está disponible para planes a nivel de partner. Para obtener más información sobre este nivel, consulte "Niveles de administración en la consola de Cyber Protect" (p. 373).

Requisitos previos

Al menos un plan de protección está disponible para su inquilino.

Para exportar un plan de protección

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Haga clic en el plan que desee exportar y luego, en el menú **Acciones**, haga clic en **Exportar**.
   Se crea un archivo JSON que contiene la configuración y se guarda en la carpeta de descarga predeterminada de su equipo.

Importar un plan de protección

Puede importar planes de protección que se exportaron en un archivo JSON. Así, puede ahorrar tiempo y garantizar la coherencia de la configuración entre inquilinos.

Nota
Esta función no está disponible para planes a nivel de partner. Para obtener más información sobre este nivel, consulte "Niveles de administración en la consola de Cyber Protect" (p. 373).

Requisitos previos

Un archivo JSON con la configuración del plan está disponible en el equipo desde el que ha iniciado sesión en la consola.

Para importar un plan de protección

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. En el menú **Acciones**, haga clic en **Importar**.
3. En la ventana que se abre, busque el archivo JSON.
4. Haga clic en el archivo y luego en **Abrir**.
   El plan de protección aparece en la pantalla. Ahora puede aplicarlo a las cargas de trabajo.

Revocación de un plan de protección

Cuando revoque un plan, lo eliminará de una o más cargas de trabajo. El plan seguirá protegiendo las demás cargas de trabajo a las que se aplique.

Puede revocar un plan en la pestaña **Dispositivos** y la pestaña **Gestión** > **Planes de protección**.

Dispositivos

1. Seleccione las cargas de trabajo de las que desee revocar el plan.
2. Haga clic en **Proteger**.
3. Seleccione el plan de protección que desee revocar.
4. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan y, a continuación, haga clic en **Revocar**.

Administración > Planes de protección

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Seleccione el plan de protección que desee revocar.
3. Haga clic en **Editar**.
4. Haga clic en **Gestionar dispositivos**.
5. En la ventana **Dispositivos**, seleccione las cargas de trabajo en las que quiera revocar el plan.
6. Haga clic en **Eliminar**.
7. En la ventana **Dispositivos**, haga clic en **Listo**.
8. En la plantilla del plan de protección, haga clic en **Guardar**.

Habilitar o deshabilitar un plan de protección

Un plan habilitado está activado y se ejecuta en las cargas de trabajo a las que se aplica. Un plan deshabilitado está inactivo: se sigue aplicando a las cargas de trabajo, pero no se ejecuta en ellas.

Cuando habilite o deshabilite un plan de protección desde la pestaña **Dispositivos**, la acción solo afectará a las cargas de trabajo seleccionadas.

Cuando habilite o deshabilite un plan de protección desde la pestaña **Gestión** > **Planes de protección**, la acción afectará a todas las cargas de trabajo a las que se aplique este plan. Además, puede habilitar o deshabilitar múltiples planes de protección.

Dispositivos

© Acronis International GmbH, 2003-2025

1. Seleccione la carga de trabajo cuyo plan quiera deshabilitar.
2. Haga clic en **Proteger**.
3. Seleccione el plan de protección que quiera deshabilitar.
4. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan y, a continuación, haga clic en **Habilitar** o **Deshabilitar**, según corresponda.

Administración > Planes de protección

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Seleccione uno o más planes de protección que desee habilitar o deshabilitar.
3. Haga clic en **Editar**.
4. Haga clic en **Habilitar** o **Deshabilitar**, según corresponda.

Nota
Esta acción no afecta a los planes de protección que ya se encontraban en el estado de destino. Por ejemplo, si la selección incluye tanto planes habilitados como deshabilitados y hace clic en **Habilitar**, se habilitarán todos los planes seleccionados.

Eliminación de un plan de protección

Cuando elimine un plan, se revocará de todas las cargas de trabajo y se borrará de la consola de Cyber Protect.

Puede eliminar un plan en la pestaña **Dispositivos** y la pestaña **Gestión** > **Planes de protección**.

Dispositivos

1. Seleccione cualquiera de las cargas de trabajo a las que se les aplica el plan de protección que desea eliminar.
2. Haga clic en **Proteger**.
3. Seleccione el plan de protección que desee eliminar.
4. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan y, a continuación, haga clic en **Eliminar**.

Administración > Planes de protección

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Seleccione el plan de protección que desee eliminar.
3. Haga clic en **Eliminar**.
4. Para confirmar su elección, seleccione la casilla de verificación **Confirmo la eliminación del plan** y haga clic en **Eliminar**.

© Acronis International GmbH, 2003-2025

Planes de protección individual para integraciones del panel de control de alojamiento

Cuando habilita integraciones del panel de control de alojamiento en los servidores de alojamiento web que utilizan DirectAdmin, cPanel o Plesk, el servicio de Cyber Protection automáticamente crea un plan de protección individual con su cuenta de usuario para cada carga de trabajo. Este plan de protección está vinculado a la carga de trabajo específica que inició la creación del plan de protección y no se puede revocar ni asignar a otras cargas de trabajo.

Para dejar de usar un plan de protección individual, puede eliminarlo de la consola de Cyber Protect. Puede identificar los planes de protección individual por el símbolo que se muestra junto a su nombre.

Si quiere un plan de protección para proteger varios servidores de alojamiento web que utilizan integraciones del panel de control de alojamiento, puede crear un plan de protección regular en la consola de Cyber Protect y asignarle estas cargas de trabajo. No obstante, solo se puede modificar un plan de protección compartido por varios paneles de control de alojamiento web a través de la consola de Cyber Protect, pero no desde las integraciones.

Problemas de compatibilidad con los planes

En algunos casos, aplicar un plan de en un recurso informático podría causar problemas de compatibilidad.

Es posible que observe los siguientes problemas:

- Plan en conflicto: hay un conflicto entre el plan que está aplicando y un plan ya aplicado.
  Por ejemplo, algunas configuraciones del plan podrían entrar en conflicto con las configuraciones del plan ya aplicado, o puede que el mismo recurso informático ya haya sido protegido como parte de un grupo de dispositivos.
- Sistema operativo incompatible: el sistema operativo del recurso informático no es compatible.
- Agente no compatible: la versión del agente de protección del recurso informático está obsoleta y no es compatible con la funcionalidad configurada.
- Cuota insuficiente: no hay cuota de servicio suficiente en el inquilino para asignarla a los recursos informáticos seleccionados.
- Tipo de recurso informático incompatible: la funcionalidad seleccionada no está disponible para este tipo de recurso informático.
- Falta el paquete Advanced: la funcionalidad seleccionada no está disponible porque el paquete Advanced necesario no está habilitado para este cliente.

La siguiente tabla resume los posibles problemas de compatibilidad de los diferentes tipos de planes.

© Acronis International GmbH, 2003-2025

Problema/Tipo de plan	Plan de protección	Plan de programación	Plan de supervisión	Plan de administración remota	Plan de implementación de software
Plan en conflicto	+*	-	-	+	-
Sistema operativo no compatible	+	+	+	+	+
Agente no compatible	+	+	+	+	+
Cuota insuficiente	+	+	+	+	-
Tipo de carga de trabajo incompatible	+	+	+	+	-
Falta el paquete avanzado	+	-	-	-	-

* No se generan conflictos si se configuran distintas opciones de copia de seguridad en varios planes de protección para el mismo recurso informático.

Si se aplica el plan hasta 150 recursos informáticos seleccionados individualmente, se le pedirá que resuelva los conflictos existentes antes de guardar el plan. Para resolver un conflicto, elimine la causa raíz o los recursos informáticos afectados del plan. Para obtener más información, consulte "Resolver problemas de compatibilidad" (p. 258). Si no logra resolver los conflictos, en función del tipo de problema de compatibilidad, se deshabilitará todo el plan o algunos de sus módulos en los recursos informáticos no compatibles y se mostrarán alertas.

Si el plan se aplica a más de 150 recursos informáticos o a grupos de dispositivos, primero se guardará y después se comprobará su compatibilidad. Dependiendo del tipo de problema de compatibilidad, se deshabilitará todo el plan o algunos de sus módulos en los recursos informáticos no compatibles y se mostrarán alertas.

Resolver problemas de compatibilidad

Según la causa de los problemas de compatibilidad, puede ejecutar diferentes acciones para resolverlos como parte del proceso de creación o edición de un plan.

Pasos para resolver problemas de compatibilidad

Plan en conflicto

© Acronis International GmbH, 2003-2025

1. Haga clic en **Revise los problemas**.
2. [Pasos para resolver el problema eliminando recursos informáticos del nuevo plan]
   a. En la pestaña **Plan en conflicto**, seleccione los recursos informáticos que desee eliminar.

   Nota
   No puede eliminar recursos informáticos que forman parte de un grupo de dispositivos.

   b. Haga clic en **Eliminar los recursos informáticos seleccionados del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
3. [Pasos para resolver el problema deshabilitando los planes que ya se aplicaron al recurso informático]
   a. Haga clic en **Deshabilitar los planes aplicados**.
   b. Haga clic en **Deshabilitar** y, a continuación, haga clic en **Cerrar**.

SO incompatible

1. Haga clic en **Revise los problemas**.
2. [Pasos para resolver el problema eliminando recursos informáticos del plan]
   a. En la pestaña **Sistema operativo no compatible**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
3. [Para planes de supervisión] [Pasos para resolver el problema deshabilitando un monitor en el plan]
   a. En la pestaña **Sistema operativo no compatible**, seleccione los monitores que desee eliminar.
   b. Haga clic en **Deshabilitar monitor**.
   c. Haga clic en **Deshabilitar** y, a continuación, haga clic en **Cerrar**.
4. [Para planes distintos a la supervisión] [Pasos para resolver el problema deshabilitando un módulo en el plan]
   a. En la pestaña **Sistema operativo no compatible**, amplíe el módulo en conflicto.
   b. Haga clic en **Deshabilitar el módulo en el plan**.
   c. Haga clic en **Deshabilitar** y, a continuación, haga clic en **Cerrar**.

Agente no compatible

1. Haga clic en **Revise los problemas**.
2. En la pestaña **Agente no compatible**, seleccione los recursos informáticos que desee eliminar.
3. Haga clic en **Eliminar cargas de trabajo del plan**.
4. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.

Cuota insuficiente

© Acronis International GmbH, 2003-2025

1. Haga clic en **Revise los problemas**.
2. En la pestaña **Cuota insuficiente**, seleccione las cargas de trabajo que desee eliminar.
3. Haga clic en **Eliminar cargas de trabajo del plan**.
4. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.

Tipo de carga de trabajo incompatible

1. Haga clic en **Revise los problemas**.
2. En la pestaña **Cuota insuficiente**, seleccione las cargas de trabajo que desee eliminar.
3. Haga clic en **Eliminar cargas de trabajo del plan**.
4. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.

Falta el paquete avanzado

1. Haga clic en **Revise los problemas**.
2. [Pasos para resolver el problema eliminando recursos informáticos del nuevo plan] En la pestaña **Paquete Advanced que falta**, seleccione los recursos informáticos que desee eliminar.
   - Haga clic en **Eliminar cargas de trabajo del plan**.
   - Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
3. [Pasos para resolver el problema al habilitar el paquete Advanced necesario]
   - [Para los administradores de los partners] Vaya al portal de administración y habilite el paquete Advanced necesario para este cliente.

Planes de protección de datos fuera del host

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

La replicación, validación y limpieza suelen ser realizadas por el agente de protección que realiza la copia de seguridad. Esto impone una carga adicional sobre el equipo en el que se está ejecutando el agente, incluso después de que se complete el proceso de copia de seguridad. Para aliviar la carga del equipo, puede crear planes de protección de datos fuera del host, es decir, planes independientes para la replicación, validación, limpieza y conversión a una máquina virtual.

Con los planes de protección de datos fuera del host, puede hacer lo siguiente:

- Elija diferentes agentes para las operaciones de copia de seguridad y protección de datos fuera del host.
- Planifique las operaciones de procesamiento de datos fuera del host durante las horas de menor actividad para minimizar el consumo de ancho de banda de red.

© Acronis International GmbH, 2003-2025

- Planifique las operaciones de procesamiento de datos fuera del host durante horas no laborables, si no desea instalar un agente dedicado para el procesamiento de datos fuera del host.

Nota
Los planes de procesamiento de datos fuera del host se ejecutan de acuerdo con la configuración de tiempo (incluida la zona horaria) del equipo en el que está instalado el agente de protección. Para un dispositivo virtual (por ejemplo, Agent for VMware o Agent for Scale Computing HC3), puede configurar la zona horaria en la interfaz de usuario gráfica del agente.

Réplica de copia de seguridad

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

La réplica de copia de seguridad está copiando una copia de seguridad a otra ubicación. Como una operación de procesamiento de datos fuera del host, se configura en un plan de réplica de copia de seguridad.

La réplica de copia de seguridad también puede formar parte de un plan de protección. Para obtener más información sobre esta opción, consulte "Replicación" (p. 581).

Creación de un plan de réplica de copia de seguridad

Para replicar copias de seguridad como una operación de procesamiento de datos fuera del host, se crea un plan de replicación de copias de seguridad.

Pasos para crear un plan de replicación de copias de seguridad

1. En la consola de Cyber Protect, haga clic en **Gestión** > **Réplica de copia de seguridad**.
2. Haga clic en **Crear plan**.
3. En **Agente**, seleccione el agente que realizará la replicación.
   Puede seleccionar cualquier agente que tenga acceso tanto a la ubicación de origen como a las ubicaciones de replicación.
4. En **Elementos para replicar**, seleccione los archivos comprimidos o las ubicaciones de las copias de seguridad que hay que replicar.
   Para cambiar entre archivos comprimidos y ubicaciones, utilice la opción **Ubicaciones** / **Copias de seguridad** de la esquina superior derecha.
   Si selecciona varios archivos cifrados, su contraseña de cifrado debe ser la misma. Para los archivos comprimidos que utilicen contraseñas de cifrado diferentes, cree planes separados.
5. En **Destino**, especifique la ubicación de replicación.

© Acronis International GmbH, 2003-2025

6. En **Cómo replicar**, seleccione qué copias de seguridad (también conocidas como puntos de recuperación) hay que replicar.

   Las siguientes opciones están disponibles:

   - **Todas las copias de seguridad**
   - **Solo copias de seguridad completas**
   - **Solo la última copia de seguridad**

   Para obtener más información sobre estas opciones, consulte "Qué replicar" (p. 262).
7. En **Planificación**, configure la planificación de la replicación.

   Al configurar la planificación del plan de replicación de copias de seguridad, asegúrese de que la última copia de seguridad replicada siga estando disponible en su ubicación original cuando se inicie la replicación de copias de seguridad. Si esta copia de seguridad no está disponible en la ubicación original, porque, por ejemplo, una regla de retención la eliminó, todo el archivo comprimido se replicará como una copia de seguridad completa. Esto puede requerir mucho tiempo y espacio de almacenamiento adicional.
8. En **Normas de retención**, especifique las reglas de retención para la ubicación de destino.

   Las siguientes opciones están disponibles:

   - **Por número de copias de seguridad**
   - **Por antigüedad de la copia de seguridad** (configuración independiente para las copias de seguridad mensuales, semanales, diarias y horarias)
   - **Por tamaño total de las copias de seguridad**
   - **Mantener las copias de seguridad indefinidamente**

     Nota
     Si selecciona esta opción, aumentará el uso de almacenamiento. Deberá eliminar manualmente las copias de seguridad innecesarias.
9. [Si ha seleccionado archivos comprimidos cifrados en **Elementos para replicar**] Active la opción **Contraseña de la copia de seguridad** y, a continuación, proporcione la contraseña de cifrado.
10. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje y, a continuación, configure las opciones como desee.
11. Haga clic en **Crear**.

Qué replicar

Nota
Algunas operaciones de replicación, como la replicación de toda la ubicación o la de todas las copias de seguridad de un conjunto de copias de seguridad, lo que puede suponer mucho tiempo.

Puede replicar conjuntos de copias de seguridad individuales o ubicaciones de copias de seguridad completas. Cuando replica una ubicación de copia de seguridad, se replican todos los conjuntos de copias de seguridad almacenadas en ella.

© Acronis International GmbH, 2003-2025

Los conjuntos de copias de seguridad están formados por copias de seguridad (también conocidas como puntos de recuperación). Debe seleccionar qué copias de seguridad hay que replicar.

Las siguientes opciones están disponibles:

- **Todas las copias de seguridad**
  Todas las copias de seguridad del conjunto de copias de seguridad se replican cada vez que se ejecuta el plan de replicación.
- **Solo copias de seguridad completas**
  Solo se replican las copias de seguridad completas del conjunto de copias de seguridad.
- **Solo la última copia de seguridad**
  Solo se replica la copia de seguridad más reciente del conjunto de copias de seguridad, independientemente del tipo (completa, diferencial o incremental).

Seleccione una opción según sus necesidades y el esquema de copias de seguridad que utiliza. Por ejemplo, si utiliza el esquema de copias de seguridad **Siempre incremental (un archivo)** y desea replicar solo la copia de seguridad incremental más reciente, seleccione **Solo la última copia de seguridad** en el plan de replicación de copia de seguridad.

La siguiente tabla resume qué copias de seguridad se replicarán con los diferentes esquemas de copias de seguridad.

	Siempre incremental (un archivo)	**Siempre completa**	**Completa semanal, incremental diaria**	**Completa mensual, diferencial semanal, incremental diaria (GFS)**
Todas las copias de seguridad	Todas las copias de seguridad del conjunto de copias de seguridad	Todas las copias de seguridad del conjunto de copias de seguridad	Todas las copias de seguridad del conjunto de copias de seguridad	Todas las copias de seguridad del conjunto de copias de seguridad
Solo copias de seguridad completas	Solo la primera copia de seguridad completa	Todas las copias de seguridad	Una copia de seguridad por semana*	Una copia de seguridad por mes*
Solo la última copia de seguridad	Solo la copia de seguridad más reciente del conjunto de copias de seguridad*	Solo la copia de seguridad más reciente del conjunto de copias de seguridad*	Solo la más reciente del conjunto de copias de seguridad, independientemente del tipo*	Solo la más reciente del conjunto de copias de seguridad, independientemente del tipo*

*Al configurar la planificación del plan de replicación de copias de seguridad, asegúrese de que la última copia de seguridad replicada siga estando disponible en su ubicación original cuando se inicie la replicación de copias de seguridad. Si esta copia de seguridad no está disponible en la

© Acronis International GmbH, 2003-2025

ubicación original, porque, por ejemplo, una regla de retención la eliminó, todo el archivo comprimido se replicará como una copia de seguridad completa. Esto puede requerir mucho tiempo y espacio de almacenamiento adicional.

Ubicaciones admitidas para el procesamiento de datos fuera del host

La siguiente tabla resume las ubicaciones de copia de seguridad admitidas en los planes de replicación de copias de seguridad de procesamiento de datos fuera del host.

Ubicación de la copia de seguridad	Admitido como origen	Admitido como destino
Almacenamiento en la nube	+	+
Carpeta local	+	+
Carpeta de red	+	+
Nube pública	+	+
Carpeta NFS	–	–
Secure Zone	–	–

Validación

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

Puede validar una copia de seguridad para verificar que puede recuperar los datos.

Cuando valida una copia de seguridad, aplica un método de validación a un archivo comprimido de copia de seguridad o a una ubicación de copia de seguridad. La validación de una ubicación de copia de seguridad valida todos los archivos comprimidos de esta ubicación.

Para validar una copia de seguridad como una operación de procesamiento de datos fuera del host, se crea un plan de validación. Para obtener más información, consulte "Creación de un plan de validación" (p. 270).

Para validar una copia de seguridad sin crear un plan de validación, siga el procedimiento en "Validación de copias de seguridad" (p. 725).

Ubicaciones admitidas para la validación

La siguiente tabla resume las ubicaciones de copias de seguridad y los métodos de validación compatibles.

© Acronis International GmbH, 2003-2025

Nota

La opción de validación no está disponible para las copias de seguridad en la nube pública debido a los elevados costes que supondría la lectura de todo un archivo comprimido de una nube pública.

Ubicación de la copia de seguridad	Verificación de suma de comprobación	Ejecutar como equipo virtual	
		Latido del equipo virtual	Validación de captura de pantalla
Almacenamiento en la nube	+	+	+
Carpeta local	+	+	+
Carpeta de red	+	+	+
Carpeta NFS	–	–	–
Secure Zone	–	–	–

Métodos de validación

Puede seleccionar uno o más métodos de validación. Si se seleccionan varios, se aplican en el siguiente orden:

- Latido de la máquina virtual (parte de la opción de validación **Ejecutar como máquina virtual**)
- Validación de captura de pantalla (parte de la opción de validación **Ejecutar como máquina virtual**)
- Verificación de suma de comprobación

La opción de validación **Ejecutar como máquina virtual** está disponible solo para las copias de seguridad a nivel de disco que contienen un sistema operativo. Puede utilizarla en los hosts ESXi o Hyper-V que están gestionados por un agente de protección (agente para VMware o agente para Hyper-V).

Latido del equipo virtual

Con este método de validación, el agente ejecuta una máquina virtual desde la copia de seguridad, se conecta a las herramientas de VMware o los servicios de integración de Hyper-V y, a continuación, comprueba la respuesta del latido para asegurarse de que el sistema operativo se ha iniciado correctamente. Si la conexión falla, el agente intentará conectarse cada dos minutos en un máximo de cinco intentos. Si no se conecta en ninguno de estos intentos, la validación fallará.

Independientemente de la cantidad de planes de validación y copias de seguridad validadas, el agente que realiza la validación ejecuta una máquina virtual cada vez. En cuanto el resultado de la validación esté disponible, el agente elimina la máquina virtual y ejecuta la siguiente.

© Acronis International GmbH, 2003-2025

Nota
Utilice este método sólo cuando valide las copias de seguridad de las máquinas virtuales VMware ejecutándolas como máquinas virtuales en un host ESXi, y las copias de seguridad de las máquinas virtuales Hyper-V ejecutándolas como máquinas virtuales en un host Hyper-V.

Validación de captura de pantalla

Con este método de validación, el agente ejecuta una máquina virtual desde la copia de seguridad y, mientras la máquina virtual se está iniciando, se toman capturas de pantalla durante un período específico. Para obtener más información sobre este período, consulte "Cambio del tiempo de espera para el Latido del equipo virtual y la validación de la captura de pantalla" (p. 267).

Un módulo de inteligencia automática (MI) comprueba las capturas de pantalla y se adjunta una captura de pantalla a cada copia de seguridad validada (punto de recuperación).

Si una captura de pantalla contiene una pantalla de inicio de sesión, no se toman más capturas y se adjunta dicha captura. Si ninguna captura de pantalla contiene una pantalla de inicio de sesión, se toman capturas hasta que finaliza el período de tiempo de espera y luego se adjunta la última captura de pantalla.

En la consola de Cyber Protect, puede descargar la captura de pantalla adjunta en un plazo de un año de la validación. Para obtener más información sobre cómo ver la captura de pantalla, consulte "Comprobación del estado de validación" (p. 269).

Si tiene activadas las notificaciones para su cuenta de usuario, recibirá un correo electrónico acerca del estado de validación de la copia de seguridad, en el que irá adjunta la captura de pantalla. Para obtener más información acerca de las notificaciones, consulte Cambiar los ajustes de notificaciones para un usuario.

La validación de captura de pantalla es compatible con el agente de la versión 15.0.30971 (publicada en novimebre de 2022) y posteriores.

Nota
La validación de captura de pantalla funciona mejor con las copias de seguridad de los sistemas Windows y Linux con pantallas de inicio de sesión basadas en GUI. Este método no está optimizado para los sistemas Linux con consola con una consola con pantalla de inicio.

Verificación de suma de comprobación

La validación por suma de verificación calcula una suma de verificaciones para cada bloque de datos que se puede recuperar de la copia de seguridad, y luego la compara con la suma de verificación original de ese bloque de datos, que se escribió durante el proceso de copia de seguridad. La única excepción es la validación de las copias de seguridad a nivel de archivo que se encuentran en el almacenamiento en la nube. Estas copias de seguridad se validan comprobando la coherencia de los metadatos que se guardan en la copia de seguridad.

© Acronis International GmbH, 2003-2025

La validación mediante la verificación de la suma de comprobación es una operación que consume tiempo, incluso para las copias de seguridad incrementales o diferenciales, que suelen ser de tamaño reducido. La operación de validación incluye todos los datos que deben recuperarse. En el caso de las copias de seguridad incrementales y diferenciales, estos datos podrían encontrarse en más de una copia de seguridad.

Una correcta validación por suma de verificación garantiza una alta probabilidad de recuperar los datos. Sin embargo, la validación mediante este método no comprueba todos los factores que pueden afectar al proceso de recuperación.

Si realiza la copia de seguridad de un sistema operativo, le recomendamos que utilice algunas de las siguientes operaciones adicionales:

- Probar la recuperación desde el soporte de arranque a un disco duro.
- Ejecutar una máquina virtual desde la copia de seguridad en un entorno ESXi o Hyper-V.
- Ejecutar un plan de validación en el que el método de validación **Ejecutar como equipo virtual** esté activado.

Cambio del tiempo de espera para el Latido del equipo virtual y la validación de la captura de pantalla

Cuando valida una copia de seguridad al ejecutarla como una máquina virtual, puede configurar el tiempo de espera entre el arranque de la máquina virtual y el envío de la solicitud de latido o la captura de pantalla.

El período predeterminado es el siguiente:

- Un minuto: para copias de seguridad almacenadas en una carpeta local o un recurso de red compartido.
- Cinco minutos: para copias de seguridad almacenadas en el almacenamiento en la nube.

Pasos para cambiar el tiempo de espera

1. Abra el archivo de configuración del Agente para VMware o el Agente para Hyper-V para editarlo.
   El archivo de configuración está disponible en las siguientes ubicaciones:
   - [Para el Agente para VMware o el Agente para Hyper-V que se ejecute en Windows] `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - [Para Agente para VMware (dispositivo virtual)] `/bin/mms_settings.config`
     Para obtener más información sobre cómo acceder al archivo de configuración en un dispositivo virtual, consulte "Conexiones SSH a un dispositivo virtual" (p. 185).
2. Vaya a `<validation>` y cambie los valores de las copias de seguridad y las copias de la nube según sea necesario:

```
<validation>
<run_vm>
<initial_timeout_minutes>
```


© Acronis International GmbH, 2003-2025

```
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. Guarde el archivo de configuración.
4. Reinicie el agente:
   - [Para el Agente para VMware o el Agente para Hyper-V que se ejecute en Windows] Ejecute los siguientes comandos en el símbolo del sistema:

     ```
     net stop mms
     ```

     ```
     net start mms
     ```

   - [Para Agente para VMware (dispositivo virtual)] Reinicie el dispositivo virtual.

Configuración del número de reintentos en caso de error

Para maximizar el número de validaciones satisfactorias, puede configurar la cantidad reintentos automáticos para las operaciones de validación que terminan con un error.

Pasos para configurar reintentos automáticos

1. Al crear un plan de validación, haga clic en el icono de engranaje.
2. En el panel **Opciones**, seleccione **Control de errores**.
3. En, **Reintentar si se produce un error**, haga clic en **Sí**.
4. En **Número de intentos**, configure el número máximo de reintentos si ocurre un error.
   La operación de validación volverá a ejecutarse hasta que finalice correctamente o hasta que se alcance el número máximo de reintentos.
5. En **Intervalo entre intentos**, configure el tiempo de espera entre dos reintentos consecutivos.
6. Haga clic en **Listo**.

Estado de validación

A las copias de seguridad para las que se completó una validación se les asigna un estado de validación.

Tras una correcta validación, la copia de seguridad se marca con un punto verde y la etiqueta **Validada**.

Si la validación no se completa correctamente, la copia de seguridad se marca con un punto rojo.

El estado de la validación se actualiza después de cada operación de validación. El estado de cada método de validación se actualiza por separado. La validación no se completa si uno de los métodos de validación configurados no funciona. En algunos casos, una validación incompleta puede

© Acronis International GmbH, 2003-2025

deberse a una mala configuración del plan de validación. Por ejemplo, si utiliza el método **Latido de máquina virtual** para máquinas virtuales en un host incorrecto.

Nota
Si uno de los métodos de validación configurados no funciona, el estado de la validación de la copia de seguridad se mostrará como fallido. Este estado persistirá incluso si reconfigura el plan de validación deshabilitando el método que falló y la validación a través de otros métodos se completa correctamente. Para lograr un estado **validado**, el método de validación que falló debe completarse correctamente para la misma copia de seguridad.

Comprobación del estado de validación

Puede comprobar el estado de validación de una copia de seguridad desde la pestaña **Dispositivos** o desde la pestaña **Almacenamiento de la copia de seguridad**.

Puede ver el estado de cada método de validación y descargar la captura de pantalla cuando se utiliza el método de validación de capturas de pantalla.

Para comprobar el estado de la validación

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un recurso informático y haga clic en **Recuperación**.
3. [Si hay disponible más de una ubicación para las copias de seguridad] Seleccione la ubicación de la copia de seguridad.
4. Seleccione la copia de seguridad para la que desee comprobar el estado de la validación.

Almacenamiento de copias de seguridad

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación de la copia de seguridad.
3. Seleccione el archivo de la copia de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
4. Seleccione la copia de seguridad para la que desee comprobar el estado de la validación.

Estado de la actividad de validación

Un plan de validación puede incluir varias copias de seguridad. Todas las copias de seguridad se procesan de manera secuencial, una por una, en una única actividad de validación.

Un agente de protección puede ejecutar solo una actividad de validación a la vez. Por ejemplo, dos actividades de validación simultáneas requieren dos agentes y tres actividades simultáneas requieren tres agentes.

La siguiente tabla resume los posibles estados de una actividad de validación.

© Acronis International GmbH, 2003-2025

Resultado de la actividad	Plan con una copia de seguridad	Plan con varias copias de seguridad
Correcto	Todos los métodos de validación se han ejecutado correctamente	Todos los métodos de validación se han ejecutado correctamente en todas las copias de seguridad
Se han completado correctamente con advertencias	N/D	Al menos un métdo de validación no se ejecutó correctamente en al menos una copia de seguridad
Fallo	Al menos un métdo de validación no se ejecutó correctamente	Al menos un métdo de validación no se ejecutó correctamente en las copias de seguridad

Creación de un plan de validación

Para validar un archivo de copias de seguridad como una operación de procesamiento de datos fuera del host, debe crear un plan de validación.

Un plan de validación puede incluir varias copias de seguridad y una copia de seguridad se puede validar mediante varios planes de validación.

Si quiere crear un plan de validación

1. En la consola de Cyber Protect, vaya a **Gestión** > **Validación**.
2. Haga clic en **Crear plan**.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado y, a continuación, especifique un nombre nuevo.
4. En **Agente**, seleccione el agente que llevará a cabo la validación y, a continuación, haga clic en **Aceptar**.
   - Si desea realizar la validación ejecutando una máquina virtual desde una copia de seguridad, debe seleccionar un equipo con agente para VMware o agente para Hyper-V.
   - Si no desea realizar la validación ejecutando una máquina virtual desde una copia de seguridad, seleccione cualquier equipo que tenga acceso a la ubicación de la copia de seguridad.
5. En **Elementos para validar**, seleccione los archivos de copias de seguridad que quiera validar.
   a. Seleccione el ámbito de validación: Ubicaciones o archivos de copias de seguridad, al hacer clic en **Copias de seguridad** o **Ubicaciones** en la esquina superior derecha.
      Si las copias de seguridad seleccionadas están cifradas, todas deben usar la misma contraseña de cifrado. En el caso de archivos que utilizan contraseñas de cifrado diferentes, cree planes independientes.
   b. Haga clic en **Agregar**.
   c. En función del ámbito de validación, seleccione una o varias ubicaciones, o una ubicación y

© Acronis International GmbH, 2003-2025

uno o varios archivos de copia de seguridad, y haga clic en **Listo**.

d. Haga clic en **Listo**.

6. En **Qué validar**, seleccione las copias de seguridad (también conocidas como puntos de recuperación) que desea validar entre los archivos seleccionados. Las siguientes opciones están disponibles:
   - **Todas las copias de seguridad**
   - **Solo la última copia de seguridad**
7. En **Cómo validar**, seleccione el método de validación.
   Puede seleccionar uno de los métodos siguientes o ambos:
   - **Verificación de suma de comprobación**
   - **Ejecutar como equipo virtual**
     La opción **Ejecutar como máquina virtual** proporciona los métodos **Latido de máquina virtual** y **Validación de captura de pantalla**. Para obtener más información, consulte "Métodos de validación" (p. 265).
8. [Si seleccionó **Verificación de suma de comprobación**] Haga clic en **Listo**.
9. [Si seleccionó **Ejecutar como máquina virtual**]. Configure los ajustes para esta opción.
   a. En **Equipo de destino** seleccione el tipo de máquina virtual (ESXi o Hyper-V), el host y la plantilla del nombre del equipo y, a continuación, haga clic en **Aceptar**.
      El nombre predeterminado es **[Nombre del equipo]_validate**.
   b. En **Almacén de datos** (para ESXi) o **Ruta** (para Hyper-V), seleccione el almacén de datos para la máquina virtual.
   c. Seleccione uno o ambos métodos de validación:
      - **Latido del equipo virtual**
      - **Validación de captura de pantalla**
   d. [Opcional] Haga clic en **Configuración de VM** para modificar el tamaño de la memoria y las conexiones de red de la máquina virtual.
      De forma predeterminada, el equipo virtual no está conectado a una red y el tamaño de la memoria del equipo virtual es igual a la memoria del equipo original.
   e. Haga clic en **Listo**.
10. [Opcional] En el plan de validación, haga clic en **Planificación** y, a continuación, configúrela.
11. [Si los archivos seleccionados en **Elementos para validar** están cifrados] Active la opción **Contraseña de la copia de seguridad** y, a continuación, introduzca la contraseña de cifrado.
12. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
13. Haga clic en **Crear**.

Como resultado, se creará el plan de validación y se ejecutará según la programación que haya configurado. Para ejecutar el plan inmediatamente, selecciónelo en **Gestión** > **Validación** y haga clic en **Ejecutar ahora**. Después de que la validación comience, puede comprobar la actividad en ejecución y desglosar sus detalles en la consola de Cyber Protect, en **Supervisión** > **Actividades**.

© Acronis International GmbH, 2003-2025

Limpieza

La limpieza es una operación que elimina las copias de seguridad obsoletas de acuerdo con las reglas de retención. Esta operación solo se aplica a agentes y cargas de trabajo, y no a copias de seguridad de la nube a la nube (que solo pueden eliminarse manualmente).

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

Ubicaciones compatibles

Los planes de limpieza admiten todas las ubicaciones de copias de seguridad, salvo para las carpetas NFS y Secure Zone.

Pasos para crear un plan de limpieza

1. En la consola de Cyber Protect, haga clic en **Gestión** > **Limpieza**.
2. Haga clic en **Crear plan**.
3. En **Agente**, seleccione el agente que llevará a cabo la limpieza.
   Puede seleccionar cualquier agente que tenga acceso a la ubicación de la copia de seguridad.
4. En **Elementos para limpiar**, seleccione los archivos comprimidos o ubicaciones de las copias de seguridad que desee limpiar.
   Para cambiar entre archivos comprimidos y ubicaciones, utilice la opción **Ubicaciones** / **Copias de seguridad** de la esquina superior derecha.
   Si selecciona varios archivos cifrados, su contraseña de cifrado debe ser la misma. Para los archivos comprimidos que utilicen contraseñas de cifrado diferentes, cree planes separados.
5. En **Planificación**, configure la planificación para la limpieza.
6. En **Normas de retención**, especifique las reglas de retención.
   Las siguientes opciones están disponibles:
   - **Por número de copias de seguridad**
   - **Por antigüedad de la copia de seguridad** (configuración independiente para las copias de seguridad mensuales, semanales, diarias y horarias)
   - **Por tamaño total de las copias de seguridad**
7. [Si ha seleccionado archivos comprimidos cifrados en **Elementos para replicar**] Active la opción **Contraseña de la copia de seguridad** y, a continuación, proporcione la contraseña de cifrado.
8. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje y, a continuación, configure las opciones como desee.
9. Haga clic en **Crear**.

© Acronis International GmbH, 2003-2025

Conversión a equipo virtual

La conversión a un equipo virtual está disponible solo para copias de seguridad de nivel del disco. Si una copia de seguridad incluye el volumen del sistema y contiene toda la información necesaria para el inicio del sistema operativo, el equipo virtual resultante podrá iniciarse por su cuenta. De lo contrario, puede añadir sus discos virtuales a otro equipo virtual.

Nota
No pueden hacerse copias de seguridad de máquinas virtuales replicadas a través de la funcionalidad de replicación nativa de máquinas virtuales de Scale Computing.

Puede crear un plan independiente para la conversión a un equipo virtual y ejecutarlo manualmente o de forma planificada.

Para obtener información sobre los requisitos previos y limitaciones, consulte "Lo que necesita saber sobre conversión" (p. 274).

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

Pasos para crear un plan de conversión a equipo virtual

1. Haga clic en **Gestión** > **Conversión a equipo virtual**.
2. Haga clic en **Crear plan**.
   El software muestra una nueva plantilla de plan.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado.
4. En **Convertir a**, seleccione el tipo de equipo virtual de destino. **Puede seleccionar una de las siguientes opciones**:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **Archivos VHDX**

     Nota
     Para ahorrar espacio de almacenamiento, cada conversión a archivos VHDX o VMware Workstation sobrescribe los archivos VHDX/VMDK que se encuentran en la ubicación de destino que se creó durante la conversión anterior.
5. Realice uno de los siguientes procedimientos:

© Acronis International GmbH, 2003-2025

- [Para VMware ESXi, Hyper-V y Scale Computing HC3] Haga clic en **Servidor**, seleccione el servidor de destino y, a continuación, especifique la nueva plantilla del nombre del equipo.
- [Para otros tipos de equipos virtuales] En **Ruta**, especifique el lugar en que guardar los archivos de la máquina virtual y la plantilla de los nombres de los archivos.

El nombre predeterminado es **[Machine Name]_converted**.

6. Haga clic en **Agente** y, a continuación, seleccione el agente que realizará la conversión.
7. Haga clic en **Elementos para convertir** y seleccione las copias de seguridad que este plan convertirá en equipos virtuales.

   Puede alternar entre la selección de copias de seguridad y de ubicaciones enteras mediante el enlace **Ubicaciones** / **Copias de seguridad** ubicado en la esquina superior derecha.

   Si las copias de seguridad seleccionadas están cifradas, todas deben usar la misma contraseña de cifrado. En el caso de las copias de seguridad que utilizan contraseñas de cifrado diferentes, cree planes independientes.
8. [Únicamente para VMware ESXi y Hyper-V] Haga clic en **Almacén de datos** para ESXi o **Ruta** para Hyper-V y, a continuación, seleccione el almacén de datos (almacenamiento) para el equipo virtual.
9. [Solo para VMware ESXi y Hyper-V] Seleccione el modo de aprovisionamiento de disco. El valor predeterminado es **Ligero** para VMware ESXi y **Expansión dinámica** para Hyper-V.
10. [Opcional] [Para VMware ESXi, Hyper-V y Scale Computing HC3] Haga clic en **Configuración de VM** para cambiar el tamaño de la memoria, el número de procesadores o las conexiones de red de la máquina virtual.
11. [Opcional] Haga clic en **Planificación** y, a continuación, cambie la planificación.
12. Si las copias de seguridad seleccionadas en **Elementos para convertir** están cifradas, active la opción **Contraseña de la copia de seguridad** y, a continuación, introduzca la contraseña de cifrado. De lo contrario, omita este paso.
13. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
14. Haga clic en **Crear**.

Lo que necesita saber sobre conversión

Tipos de equipos virtuales admitidos

La conversión de una copia de seguridad a un equipo virtual la puede realizar el mismo agente que creó la copia de seguridad u otro.

Para realizar una conversión a VMware ESXi, Hyper-V o Scale Computing HC3, necesitará un servidor ESXi, Hyper-V o Scale Computing HC3 respectivamente y un agente de protección (Agente para VMware, Agente para Hyper-V o Agente para Scale Computing HC3) que gestione el servidor.

Al realizar una conversión a archivos VHDX, se asume que los archivos se conectarán como unidades de disco virtuales a un equipo virtual Hyper-V.

© Acronis International GmbH, 2003-2025

En esta tabla se resumen los tipos de máquinas virtuales que puede crear con la operación **Conversión a equipo virtual**. Las filas de la tabla muestran el tipo de máquinas virtuales convertidas. Las columnas muestran los agentes que realizaron la conversión.

Tipo de VM	Agente para VMware	Agente para Hyper-V	Agente para Windows	Agente para Linux	Agente para Mac	Agente para Scale Computing HC3	Agente para oVirt (KVM)	Agente para la Virtuozzo Hybrid Infrastructure	Agente para Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
Archivos VHDX	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

Limitaciones

- Las copias de seguridad almacenadas en un NFS no se pueden convertir.
- Las copias de seguridad almacenadas en Secure Zone únicamente pueden convertirse mediante el agente que se ejecute en el mismo equipo.
- Las copias de seguridad que contienen volúmenes lógicos (LVM) de Linux se pueden convertir únicamente si las ha creado Agente para VMware, Agente para Hyper-V o Agente para Scale Computing HC3 y se dirigen al mismo hipervisor. No se admite la conversión entre hipervisores.
- Cuando las copias de seguridad de un equipo Windows se convierten en archivos VHDX o VMware Workstation, el equipo virtual resultante hereda el tipo de CPU del equipo que realiza la conversión. Como resultado, los controladores de la CPU correspondiente se instalan en el sistema operativo invitado. Si se inicia en un servidor cuyo tipo de CPU es diferente, aparece un error relacionado con el controlador en el sistema invitado. Actualice este controlador de forma manual.

© Acronis International GmbH, 2003-2025

Conversión periódica a máquina virtual frente a ejecución de una máquina virtual desde una copia de seguridad

Ambas operaciones proporcionan un equipo virtual que puede iniciarse en cuestión de segundos si falla el equipo original.

La conversión periódica a máquina virtual consume recursos de la CPU y la memoria. Los archivos del equipo virtual ocupan espacio constantemente en el almacén de datos (almacenamiento). Esto podría no ser práctico si se utiliza un servidor de producción para la conversión. Sin embargo, el rendimiento del equipo virtual está limitado únicamente por los recursos del servidor.

La ejecución de una máquina virtual desde una copia de seguridad solo consume recursos mientras se ejecuta la máquina virtual. El espacio del almacén de datos (almacenamiento) es necesario únicamente para mantener los cambios en las unidades de disco virtuales. Sin embargo, el equipo virtual podría ejecutarse con mayor lentitud debido a que el servidor no accede a los discos virtuales directamente, sino que se comunica con el agente que lee datos de la copia de seguridad. Además, el equipo virtual es temporal.

Cómo funciona la conversión periódica a una máquina virtual

La forma en la que funciona la conversión periódica depende de en dónde decide crear el equipo virtual.

- **Si escoge guardar el equipo virtual como un conjunto de archivos:** cada conversión recrea el equipo virtual desde cero.
- **Si escoge crear el equipo virtual en un servidor de virtualización:** al convertir una copia de seguridad incremental o diferencial, el software actualiza de forma incremental el equipo virtual en vez de recrearlo. Dicha conversión generalmente es más rápida. Ahorra tráfico de la red y recursos de la CPU del servidor que lleva a cabo la conversión. Si no es posible actualizar un equipo virtual, el software lo recreará desde cero.

A continuación encontrará una descripción detallada de ambos casos.

Si escoge guardar el equipo virtual como un conjunto de archivos

Como resultado de esta primero conversión, se creará una nueva equipo virtual. Todos las conversiones posteriores recrearán este equipo de cero. Primero, el equipo antiguo cambia de nombre temporalmente. A continuación, se crea un equipo virtual nuevo que tiene el nombre anterior del equipo antiguo. Si esta operación se realiza correctamente, se eliminará el equipo anterior. Si esta operación no se completa, el equipo nuevo se elimina y el equipo antiguo recupera su nombre anterior. De esta manera, la conversión siempre termina con un único equipo. Sin embargo, se necesita espacio de almacenamiento adicional durante la conversión para almacenar el equipo antiguo.

© Acronis International GmbH, 2003-2025

Si escoge crear el equipo virtual en un servidor de virtualización

La primero conversión crea un nuevo equipo virtual. Cualquier conversión subsiguiente funciona de la siguiente manera:

- Si existe *una copia de seguridad completa* desde la última conversión, la máquina virtual se recreará desde cero, como se describe en la sección anterior.
- De lo contrario, el equipo virtual existente se actualiza para reflejar los cambios desde la último conversión. Si no es posible realizar la actualización (por ejemplo, si eliminó las instantáneas intermedias, consulte a continuación), el equipo virtual se recreará desde cero.

Instantáneas intermedias

Para poder actualizar la máquina virtual de forma segura, el software almacena una instantánea intermedia de la misma. La instantánea tiene el nombre **Réplica...** y debe conservarse.

La instantánea **Réplica...** corresponde al resultado de la última conversión. Puede ir a esta instantánea si desea volver el equipo a ese estado; por ejemplo, si trabajó con el equipo y ahora desea eliminar los cambios que le realizó.

Para las máquinas virtuales de Scale Computing HC3 convertidas, se crea una **Instantánea de utilidad**. Solo la usa el servicio Cyber Protection.

Planes de análisis de copia de seguridad

Para analizar las copias de seguridad en busca de malware (incluido el ransomware), cree un plan de análisis de copias de seguridad.

Importante
Los planes de análisis de copias de seguridad no son compatibles con todas las cargas de trabajo y todos los tipos de almacenamiento de copias de seguridad. Para obtener más información, consulte "Limitaciones" (p. 1214).

Pasos para crear un plan de análisis de copias de seguridad

1. En la consola de Cyber Protect, vaya a **Gestión** > **Análisis de copia de seguridad**.
2. En el panel **Acciones**, haga clic en **Crear plan**.
3. [Opcional] Cambie el nombre del plan predeterminado.
4. En **Copias de seguridad para escanear**, haga clic en **Especificar**.
   a. [Opcional] Para añadir una ubicación nueva, haga clic en **Agregar**, seleccione la ubicación y, a continuación, haga clic en **Listo**.
   b. Haga clic en **Ubicaciones** o **Copias de seguridad** para seleccionar el ámbito del plan.
   c. Seleccione la ubicación completa o los archivos comprimidos individuales en una ubicación.

© Acronis International GmbH, 2003-2025

Puede seleccionar uno o más elementos.

d. Haga clic en **Listo**.

5. [Si los archivos comprimidos seleccionados están cifrados] En **Cifrado**, habilite el conmutador y, a continuación, introduzca la contraseña de cifrado.

   La contraseña que especifique se utilizará para el análisis de todas las copias de seguridad del plan, por lo que todos los archivos comprimidos seleccionados deben utilizar la misma contraseña de cifrado. Cree distintos planes para los archivos comprimidos que utilicen contraseñas de cifrado diferentes.

6. Haga clic en **Crear**.

Como resultado, se crea un plan de análisis de copias de seguridad. El agente de la nube analizará automáticamente los archivos comprimidos seleccionados cada hora. No puede cambiar la programación del plan ni el periodo entre dos análisis consecutivos.

Planes de copias de seguridad para aplicaciones en la nube

La pestaña **Gestión** > **Copia de seguridad de aplicaciones en la nube** muestra planes de copia de seguridad de la nube a la nube. Estos planes realizan copias de seguridad de aplicaciones que se ejecutan en la nube mediante agentes que se ejecutan en la nube y usan el almacenamiento de la nube como una ubicación de copia de seguridad.

En esta sección, puede realizar las siguientes operaciones:

- Crear, ver, ejecutar, detener, editar y eliminar un plan de copias de seguridad
- Ver actividades relacionadas con cada plan de copias de seguridad
- Ver alertas relacionadas con cada plan de copias de seguridad

Para obtener más información acerca de la copia de seguridad de aplicaciones en la nube, consulte:

- Protección de los datos de Microsoft 365
- Protección de los datos de Google Workspace

Ejecución de copias de seguridad de nube a nube de forma manual

Para evitar que se interrumpa el servicio Cyber Protection, el número de copias de seguridad de la nube a la nube se limita a 10 ejecuciones por organización de Microsoft 365 o Google Workspace durante una hora. Después de que se alcance este número, el número de ejecuciones permitido se restablece durante una hora, y después una ejecución adicional pasa a estar disponible por cada hora a partir de entonces (por ejemplo, primera hora, 10 ejecuciones, segunda hora, 1 ejecución, tercera hora, 2 ejecuciones) hasta que se alcanza un total de 10 ejecuciones por hora.

Los planes de copias de seguridad que se han aplicado a grupos de dispositivos (buzones de correo, unidades o sitios) o que incluyan más de 10 dispositivos no se pueden ejecutar manualmente.

© Acronis International GmbH, 2003-2025

Protección de aplicaciones de colaboración y comunicación

Zoom, Cisco Webex Meetings, Citrix Workspace y Microsoft Teams son aplicaciones de comunicación, videoconferencia y conferencia web muy extendidas. El servicio Cyber Protection le permite proteger sus herramientas de colaboración.

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La configuración de protección para Zoom, Cisco Webex Meetings, Citrix Workspace y Microsoft Teams es similar. En el ejemplo siguiente, veremos la configuración correspondiente a Zoom.

Pasos para configurar la protección de Zoom

1. Instale el agente de protección en el equipo donde está instalada la aplicación de colaboración.
2. Inicie sesión en la consola de Cyber Protect y aplique un plan de protección que tenga habilitado alguno de los módulos siguientes:
   - **Protección antimalware y antivirus** (con las opciones **Autoprotección** y **Active Protection** habilitadas): si tiene una de las ediciones de Cyber Protect.
   - **Active Protection** (con la opción **Autoprotección** habilitada): si tiene una de las ediciones de Cyber Backup.
3. [Opcional] Para instalar las actualizaciones automáticamente, configure el módulo **Gestión de parches** en el plan de protección.

Como resultado, su aplicación Zoom quedará bajo una protección que incluye las actividades siguientes:

- Instalación automática de actualizaciones del cliente de Zoom
- Protección de los procesos de Zoom frente a inyecciones de código
- Prevención de operaciones sospechosas por parte de los procesos de Zoom
- Protección del archivo de "servidores" para que no se añadan dominios relacionados con Zoom

Planes de reenvío de SIEM

Importante
Esta opción solo está disponible para administradores de partner con acceso a Cyber Protection.

Las plataformas SIEM (Gestión de Información y Eventos de Seguridad) son soluciones de ciberseguridad que proporcionan una administración centralizada de registros, ofrecen detección de amenazas en tiempo real, facilitan investigaciones de incidentes y ayudan a las organizaciones a

© Acronis International GmbH, 2003-2025

cumplir con los requisitos de cumplimiento. Funcionan consolidando y analizando datos de seguridad, como registros de firewalls, sistemas de detección de intrusiones, servidores y aplicaciones. Esto se realiza en tiempo real, para generar alertas priorizadas para cualquier actividad sospechosa y amenazas potenciales. Los equipos de seguridad luego utilizan los datos consolidados y las alertas para investigar los incidentes de ciberseguridad señalados, entender su ámbito y tomar medidas oportunas para contener y mitigar amenazas.

Las plataformas SIEM proporcionan una vista completa de la postura de seguridad de una organización, permitiendo la detección temprana de amenazas avanzadas y anomalías. Ayudan a las organizaciones a cumplir con los estándares de cumplimiento de seguridad regulatorios y específicos del sector, proporcionando datos centralizados y generación de informes. Ofrecen una consola centralizada para gestionar eventos de seguridad, proporcionando mejor visibilidad en el centro de operaciones de seguridad (SOC).

Capacidades SIEM de Acronis

Algunos inquilinos de clientes utilizan plataformas SIEM de terceros, por lo que las alertas, eventos, tareas e información de registro de auditoría de Acronis pueden ser enviados a estas plataformas para su procesamiento.

El cumplimiento regulatorio para el envío de datos a plataformas SIEM exige que cada cliente tenga su propio "lago de datos" SIEM. Esto significa que debe definir un plan de envío para cada cliente.

Los planes de reenvío a SIEM de Acronis definen la ubicación del almacén de datos o los detalles de su servidor syslog dedicado.

Listas de planes de reenvío SIEM

Las listas de planes de reenvío SIEM proporcionan un resumen de los planes de reenvío SIEM. Puede ver una lista a nivel de partner, que detalla los planes de reenvío SIEM que ha creado y aplicado para todos sus clientes. También puede ver la lista a nivel de cliente. Por lo general, los clientes tienen un único plan de reenvío SIEM. Sin embargo, si es necesario, puede crear dos planes para un cliente (cada uno utilizando un método diferente). Para más información sobre los métodos de los planes de reenvío SIEM, consulte "Métodos de planes de reenvío SIEM" (p. 286).

Pasos para abrir una lista de planes de reenvío SIEM

1. Abra la consola de Protección ya sea a nivel de partner o a nivel de cliente.
2. Seleccione **Gestión** en el menú principal.
3. Seleccione **Planes de reenvío SIEM** del submenú.

La lista de planes de reenvío SIEM a nivel de partner incluye los siguientes detalles:

- **Nombre**
  El nombre del plan de reenvío SIEM.
- **Método**
  Si el plan de reenvío SIEM utiliza el método de archivos o el método de servidor syslog.

© Acronis International GmbH, 2003-2025

- **Clientes**
  El cliente o clientes para los cuales se aplicó el plan.
- **Datos**
  Los datos de Acronis reenviados como parte del plan de reenvío SIEM.

Las listas de planes de reenvío SIEM a nivel de cliente incluyen los siguientes detalles:

- **Nombre**
  El nombre del plan de reenvío SIEM.
- **Método**
  Si el plan de reenvío SIEM utiliza el método de archivos o el método de servidor syslog.
- **Dispositivo de escritura syslog**
  El dispositivo utilizado para escribir y almacenar los datos SIEM de Acronis.
- **Datos**
  Los datos de Acronis reenviados como parte del plan de reenvío SIEM.

Creación de un plan de reenvío SIEM genérico para múltiples clientes

Para ahorrar tiempo, puede crear un único plan de reenvío SIEM genérico y aplicarlo a múltiples clientes.

Pasos para crear un plan de reenvío SIEM genérico para múltiples clientes

1. Abra su lista de planes de reenvío SIEM de partner.
2. Haga clic en **Crear**.
3. [Opcional] Cambie el nombre predeterminado del plan.
   a. Haga clic en el icono del lápiz.
   b. Edite el nombre.
   c. Haga clic en la marca de verificación para aceptar los cambios.
4. Seleccione **Método** para el plan de reenvío SIEM:
   - **Archivos**
   - **Servidor de syslog**
     Para más información, consulte métodos de plan de reenvío SIEM.
5. ***Método de archivos***
   a. Haga clic en el campo **Cliente**.
      Aparece una lista de todos sus clientes. Cada cliente tiene una lista desplegable correspondiente de todos los dispositivos protegidos que puede seleccionar como el dispositivo escritor.
   b. Desde las listas desplegables, seleccione un dispositivo escritor para cada cliente al que desee aplicar el plan de reenvío SIEM.

© Acronis International GmbH, 2003-2025

Nota
El plan no se aplica a aquellos clientes para los cuales no especifique un dispositivo escritor.

c. Haga clic en **Listo**.

d. [Opcional] Haga clic en **Especificar** para cambiar los valores predeterminados de **Ruta de archivo** para los almacenes de datos SIEM en los dispositivos escritores y luego pulse en **Listo**.

Método del servidor syslog

a. Haga clic en el campo **Cliente**.
Aparece una lista de todos sus clientes. Cada cliente tiene una lista desplegable correspondiente de todos los dispositivos Linux protegidos que puede seleccionar como el dispositivo escritor.

b. Desde las listas desplegables, seleccione un dispositivo escritor para cada cliente al que desee aplicar el plan de reenvío SIEM.

Nota
El plan no se aplica a aquellos clientes para los cuales no especifique un dispositivo escritor.

c. Haga clic en **Listo**.

6. [Opcional] Cambie el **Formato del archivo**.
   - **JSON** (predeterminado)
     Formato altamente flexible que permite datos personalizados y complejos.
     Ideal para plataformas modernas de gestión de registros.
   - **CEF**
     Formato estandarizado y neutral del proveedor, diseñado para eventos de seguridad y análisis detallado de eventos.
7. [Opcional] Seleccione los tipos de datos de Acronis para incluir en el plan de reenvío SIEM.
   Por defecto, todos los tipos de datos de Acronis disponibles están incluidos.
   a. Haga clic en el campo **Datos**.
   b. Desmarque las casillas de verificación de los tipos de datos de Acronis que no desea incluir en el plan de reenvío SIEM. Los tipos de datos de Acronis son:
      - **Alertas**
        Actualizaciones de mensajes críticos o de error que requieren una respuesta rápida.
      - **Eventos**
        Datos de registro de eventos con información sobre el rendimiento del sistema y las interacciones del usuario.
      - **Actividades**
        Todos los mensajes de éxito, informativos, de aviso, críticos y de error (por ejemplo, DLP, filtrado de URL, copias de seguridad).
      - **Registro de auditoría**
        Eventos relevantes para la seguridad interna que puedan afectar la seguridad e integridad

© Acronis International GmbH, 2003-2025

de la organización.

Nota
Los datos del registro de auditoría pueden almacenarse para fines de cumplimiento con HIPAA si utiliza el método **Archivos**.

c. Haga clic en **Listo**.

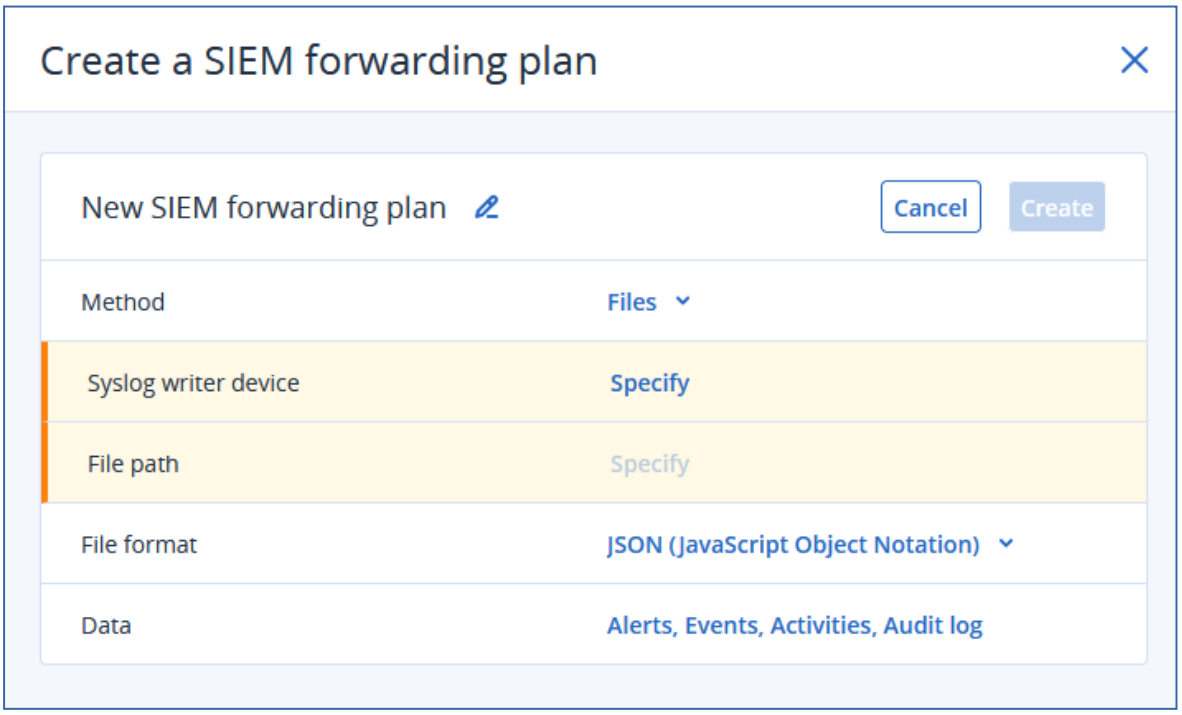
8. Cuando haya terminado, haga clic en **Crear**.

Creación de un plan SIEM para un cliente individual

Nota
Normalmente, un cliente tiene un único plan de reenvío SIEM. Sin embargo, si es necesario, puede crear dos planes para un cliente: cada uno utilizando un método diferente. Para más información sobre los métodos de plan de reenvío SIEM, consulte "Métodos de planes de reenvío SIEM" (p. 286). Puede decidir hacer esto si está realizando una migración de un cliente de una plataforma SIEM a otra. De esta manera, puede tener un período durante el cual está utilizando dos plataformas SIEM al mismo tiempo.

Pasos para crear un plan para un cliente individual

1. Abra la consola de Acronis Protección para el cliente.
2. Seleccione **Gestión** en el menú principal.
3. Seleccione **planes de reenvío SIEM**.
4. Haga clic en **Crear**.



© Acronis International GmbH, 2003-2025

5. [Opcional] Cambie el nombre predeterminado del plan.
   a. Haga clic en el icono del lápiz.
   b. Edite el nombre.
   c. Haga clic en la marca de verificación para aceptar los cambios.
6. Seleccione el **Método**.
   - **Archivos**
   - **Servidor de syslog**

   Para más información, consulte métodos de plan de reenvío SIEM.
7. ***Método de archivos***
   a. Haga clic en **Especificar** para seleccionar el **dispositivo escritor de Syslog** de la lista de dispositivos disponibles protegidos por Acronis y luego pulse en **Listo**.
   b. [Opcional] Haga clic en **Especificar** para cambiar la **ruta de archivo** predeterminada para el almacén de datos SIEM en el dispositivo escritor y luego pulse en **Listo**.

   Importante
   Si se elimina el directorio especificado, el reenvío SIEM se detiene hasta que restaure el directorio eliminado o modifique la **ruta de archivo** a un directorio válido.

   Método del servidor syslog
   a. Haga clic en **Especificar** para seleccionar un equipo Linux como el servidor syslog.
   b. Haga clic en **Listo**.
8. [Opcional] Cambie el **Formato del archivo**.
   - **JSON** (predeterminado)
     Formato altamente flexible que permite datos personalizados y complejos.
     Ideal para plataformas modernas de gestión de registros.
   - **CEF**
     Formato estandarizado y neutral del proveedor, diseñado para eventos de seguridad y análisis detallado de eventos.
9. [Opcional] Seleccione los tipos de datos de Acronis para incluir en el plan de reenvío SIEM.
   Por defecto, todos los tipos de datos de Acronis disponibles están incluidos.
   a. Haga clic en el campo **Datos**.

      Desmarque las casillas de verificación de los tipos de datos de Acronis que no desea incluir en el plan de reenvío SIEM.
   b.

      Los tipos de datos de Acronis son:
      - **Alertas**
        Actualizaciones de mensajes críticos o de error que requieren una respuesta rápida.
      - **Eventos**
        Datos de registro de eventos con información sobre el rendimiento del sistema y las interacciones del usuario.

© Acronis International GmbH, 2003-2025

- **Actividades**
  Todos los mensajes de éxito, informativos, de aviso, críticos y de error (por ejemplo, DLP, filtrado de URL, copias de seguridad).
- **Registro de auditoría**
  Eventos internos relevantes para la seguridad que puedan afectar la salvaguarda e integridad de la organización.

Nota
Los datos del registro de auditoría se pueden almacenar para fines de cumplimiento de HIPAA.

c. Haga clic en **Listo**.

10. Haga clic en **Crear**.

Renombrar un plan de reenvío SIEM

Pasos para renombrar un plan de reenvío SIEM

1. Abra su lista de planes de reenvío SIEM de partner o la lista específica del cliente.
2. Haga clic en el plan que desea renombrar.
   Se abre la barra lateral de detalles y acciones.
3. Haga clic en **Cambiar nombre**.
4. Edite el nombre del plan.
5. Haga clic en **Cambiar nombre**.

Modificación de un plan de reenvío SIEM

Nota
No puede cambiar el **Método**. Para cambiarlo, debe crear un nuevo plan de reenvío SIEM para el inquilino del cliente.
Si hace esto, recomendamos eliminar el antiguo plan de reenvío SIEM.

Pasos para editar un plan de reenvío SIEM

1. Abra su lista de planes de reenvío SIEM de partner o la lista específica del cliente.
2. Haga clic en el plan que desea editar.
   Se abre la barra lateral de detalles y acciones.
3. Haga clic en **Editar**.
4. Realice sus cambios y haga clic en **Confirmar**.

© Acronis International GmbH, 2003-2025

Eliminación de un plan SIEM

Nota
Cuando elimina un plan de reenvío SIEM, el reenvío de datos cesa, pero los datos que ya se han reenviado no se eliminan.

Pasos para eliminar un plan de reenvío SIEM

1. Abra su lista de planes de reenvío SIEM de partner o la lista específica del cliente.
2. Haga clic en el plan que desea eliminar.
   Se abre la barra lateral de detalles y acciones.
3. Haga clic en **Eliminar**.
4. Seleccione la casilla de confirmación para habilitar el botón **Confirmar**.
5. Haga clic en **Confirmar**.

Métodos de planes de reenvío SIEM

Hay dos métodos de planes de reenvío SIEM. Con ambos métodos, el agente de Acronis escribe datos SIEM en el dispositivo gestionado.

Importante
El dispositivo de reenvío SIEM debe tener el agente de Acronis instalado y debe estar en línea cuando cree el plan de reenvío SIEM.
Debe permanecer en línea en todo momento para que el plan de reenvío SIEM funcione correctamente.

- **Archivos**

  Los datos SIEM se escriben como archivos en un directorio que puede especificar. Solo los administradores pueden acceder a estos archivos.

  Este método se puede implementar en dispositivos Windows o Linux.

  Nota
  Para un dispositivo escritor de syslog de Windows, la ruta de archivo predeterminada es `C:\`.
  Para un dispositivo escritor de syslog de Linux, la ruta predeterminada es `/usr/local/bin`.

- **Servidor de syslog**

  Un servidor syslog es un sistema centralizado que recibe y almacena mensajes de registro utilizando el protocolo Syslog.

  Solo se pueden usar dispositivos Linux para este método.

© Acronis International GmbH, 2003-2025

Nota

Para revisar el contenido de los datos reenviados, ejecute:

```
cat /var/log/syslog
```

```
cat /var/log/messages
```


© Acronis International GmbH, 2003-2025

Cómo comprender el nivel de protección actual

Supervisión

La pestaña **Supervisión** ofrece información importante acerca de su nivel actual de protección e incluye los siguientes paneles de control:

- **Información general**
- **Actividades**
- **Alertas**
- **Fuente de amenazas** (para obtener más información, consulte "Fuente de amenazas" (p. 352))

Panel de control de Información general

El panel de control **Información general** proporciona una serie de widgets personalizables que dan una imagen general de las operaciones relacionadas con el servicio Cyber Protection. Los widgets de otros servicios estarán disponibles en próximas versiones.

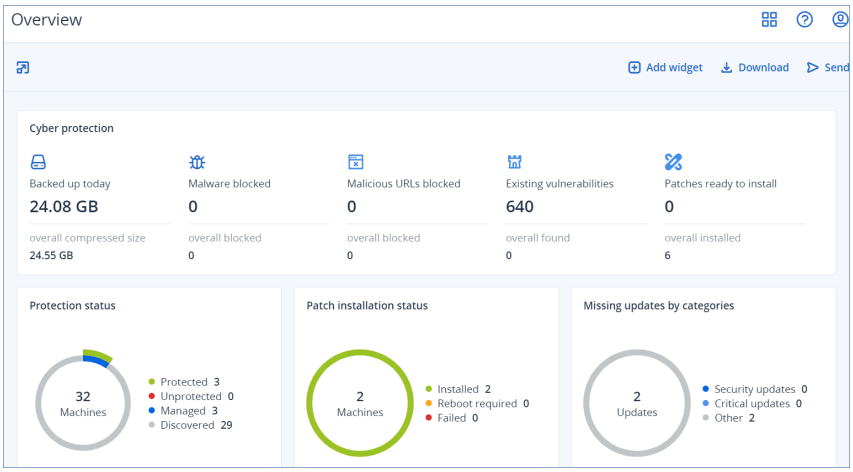
Los widgets se actualizan cada cinco minutos. Los widgets tienen elementos interactivos que le permiten investigar y solucionar problemas. Puede descargar el estado actual del panel de información o bien enviarlo por correo electrónico en formato .pdf y/o .xls.

Puede elegir entre una gran variedad de widgets, presentados como tablas, gráficos circulares, diagramas de barras, listas y estructuras de árbol. Puede agregar varios widgets del mismo tipo con diferentes filtros.

Los botones **Descargar** y **Enviar** de **Supervisión** > **Información general** no están disponibles en las ediciones Estándar del servicio Cyber Protection.

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.

© Acronis International GmbH, 2003-2025



Pasos para reorganizar los widgets en el panel de información

Haga clic en los nombres de los widgets para arrastrarlos y soltarlos.

Pasos para editar un widget

Haga clic en el icono de lápiz situado al lado del nombre del widget. Al editar un widget, puede cambiarle el nombre, modificar el intervalo de tiempo, establecer filtros y agrupar filas.

Pasos para agregar un widget

Haga clic en **Añadir widget** y, luego, realice uno de los siguientes procedimientos:

- Haga clic en el widget que quiera añadir. El widget se añadirá con la configuración predeterminada.
- Para editar el widget antes de añadirlo, haga clic en Personalizar cuando el widget esté seleccionado. Después de editar el widget, haga clic en **Listo**.

Pasos para eliminar un widget

Haga clic en el signo de X situado al lado del nombre del widget.

Panel de control Actividades

El panel de control de **Actividades** proporciona una visión general de las actividades actuales y pasadas en cargas de trabajo protegidas. De forma predeterminada, el período de retención es de hasta 90 días, pero puede acortarse si el número de actividades es demasiado grande o debido al mantenimiento del centro de datos. Consulte este artículo de la base de conocimiento para obtener la información más reciente sobre el mantenimiento del centro de datos.

Para personalizar la vista del panel de control **Actividades**, haga clic en el icono del engranaje y, a continuación, seleccione las columnas que desea ver.

Para ver el progreso de la actividad en tiempo real, seleccione la casilla de verificación **Actualizar automáticamente**. No obstante, la actualización frecuente de varias actividades merma el rendimiento del servidor de gestión.

Puede buscar las actividades enumeradas a través de los siguientes criterios:

© Acronis International GmbH, 2003-2025

- **Nombre de dispositivo**
  El equipo en el que se lleva a cabo la actividad.
- **Iniciado por**
  La cuenta que inició la actividad.

También puede filtrar las actividades por las siguientes propiedades:

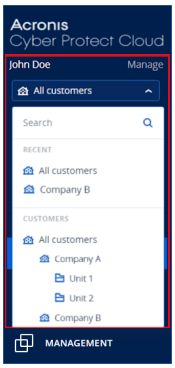
- **Estado**
  Por ejemplo, completada, con errores, en progreso o cancelada.
- **Tipo**
  Por ejemplo, aplicar plan, eliminar copias de seguridad o instalar actualizaciones de software.
- **Período**
  Por ejemplo, las actividades más recientes, las actividades de las últimas 24 horas, o las actividades durante un plazo específico de tiempo dentro del período de retención predeterminado.

Para ver más detalles sobre una actividad, selecciónala en la lista y, a continuación, en el panel **Detalles de actividad**, haz clic en **Todas las propiedades**. Para obtener más información sobre las propiedades disponibles, consulte las referencias API de Actividad y Tarea en el Portal de la red de desarrolladores.

Panel de control de Alertas

El panel de control **Supervisión** > **Alertas** muestra las alertas actuales de los inquilinos que gestiona. Las alertas se muestran para todos los inquilinos del cliente o un inquilino del cliente específico, según el nivel seleccionado en la lista desplegable del menú de navegación.

La lista desplegable no está disponible si gestiona un único inquilino.



Cada alerta contiene información general sobre su causa o consejos para la resolución de problemas. Para obtener más ayuda en la resolución del problema subyacente, haga clic en **Obtener asistencia técnica** en cada alerta. Según su rol y los servicios que estén habilitados en su inquilino, puede buscar una solución en la base de conocimientos o enviar un ticket de soporte.

© Acronis International GmbH, 2003-2025

Personalización del panel de control Alertas

El panel de control **Alertas** admite la vista simple y la vista de tabla. La vista simple muestra una lista desplazable de las alertas actuales, mientras que la vista de tabla muestra más alertas en una pantalla y la información adicional sobre estas alertas.

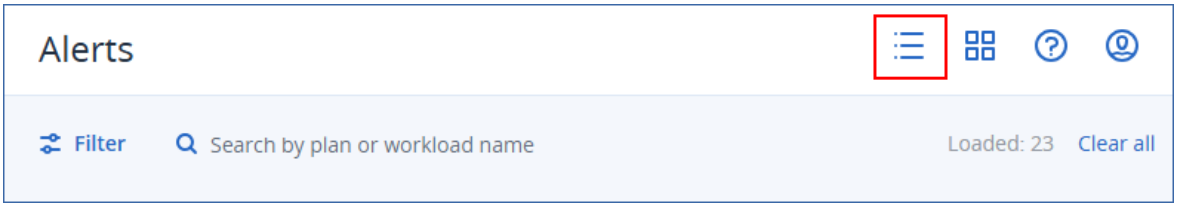
Al utilizar la vista de tabla, puede personalizar el panel de **Alertas** añadiendo o eliminando columnas.

Tanto en la vista simple como en la de tabla, puede ocultar la sección de filtro rápido.

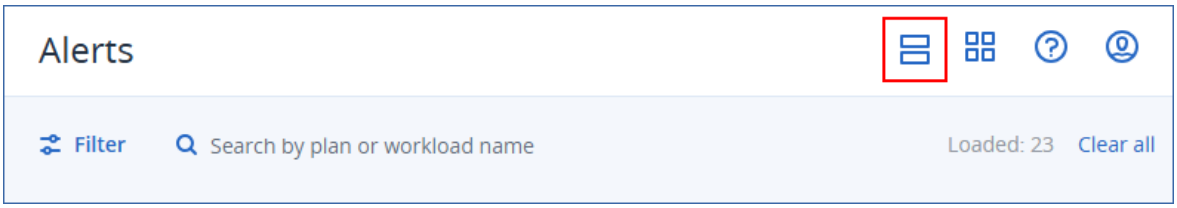
Cambiar entre vistas

Pasos para cambiar entre la vista simple y la de tabla

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. Para cambiar a la vista de tabla, haga clic en el icono de vista de tabla.



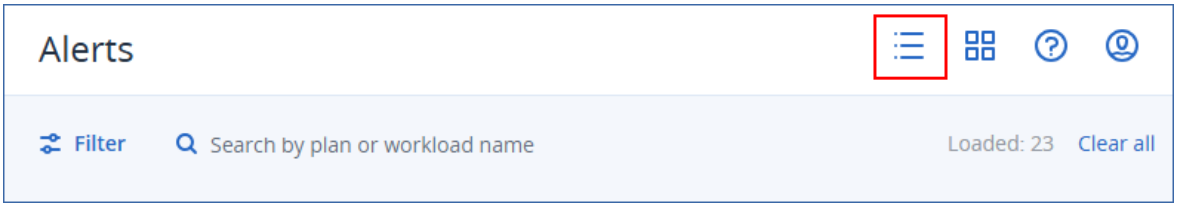
3. Para cambiar a la vista simple, haga clic en el icono de la vista simple.



Añadir o eliminar columnas

Pasos para añadir o eliminar columnas

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. [Si utiliza la vista simple] Haga clic en el icono de vista de tabla.



3. Haga clic en el icono de engranaje en la esquina superior derecha y seleccione las columnas que desea que sean visibles.
   Están disponibles las siguientes columnas:

© Acronis International GmbH, 2003-2025

Columna	Descripción
Gravedad (siempre disponible)	Nivel de importancia de la alerta. En nivel de gravedad puede ser uno de los siguientes: • Crítico • Error • Advertencia • Informativo
Tipo de alerta	Resumen de alerta. Para obtener más información, consulte "Tipos y categorías de alertas" (p. 295).
Mensaje (siempre disponible)	Detalles de la alerta
Tipo de supervisión	Tipo de supervisión: basada en umbrales o en anomalías. Para obtener más información, consulte "Supervisión del estado y el rendimiento de las cargas de trabajo" (p. 1507).
Carga de trabajo	Carga de trabajo para la que se genera la alerta
Fecha y hora	Fecha/hora de la alerta
Plan	Plan relacionado con la alerta (si corresponde)
Categoría de alertas	Grupo de alerta por área funcional. Para obtener más información, consulte "Tipos y categorías de alertas" (p. 295).
Origen	Origen de la alerta: sistema o aplicación de integración

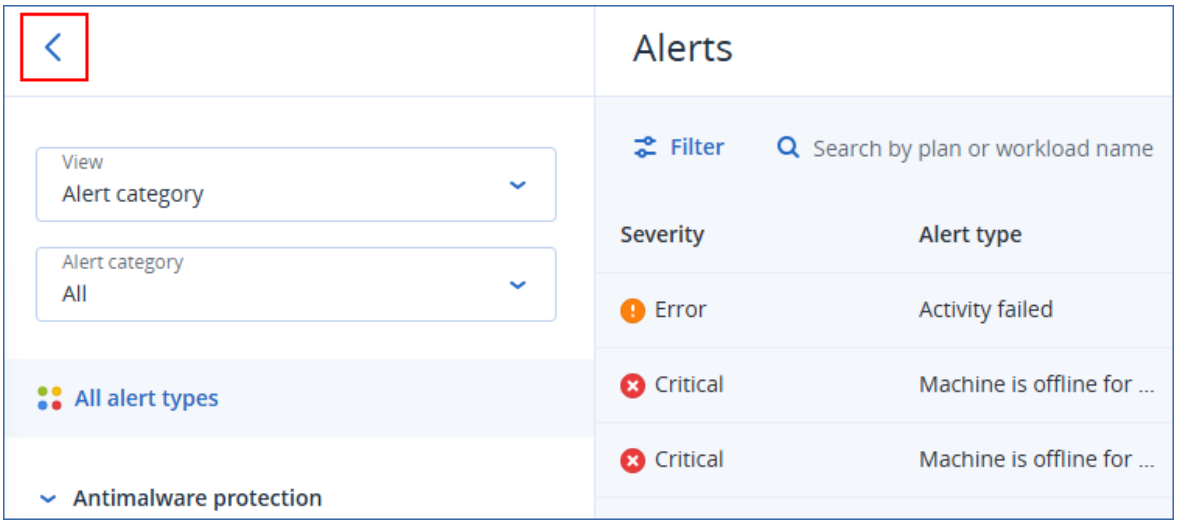
Nota
Si se seleccionan varias columnas, es posible que deba desplazar la pantalla horizontalmente para ver toda la información disponible.

Ocultar filtro rápido

Pasos para ocultar la sección de filtro rápido

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. Haga clic en el icono en la parte superior de la sección de filtro rápido.

© Acronis International GmbH, 2003-2025



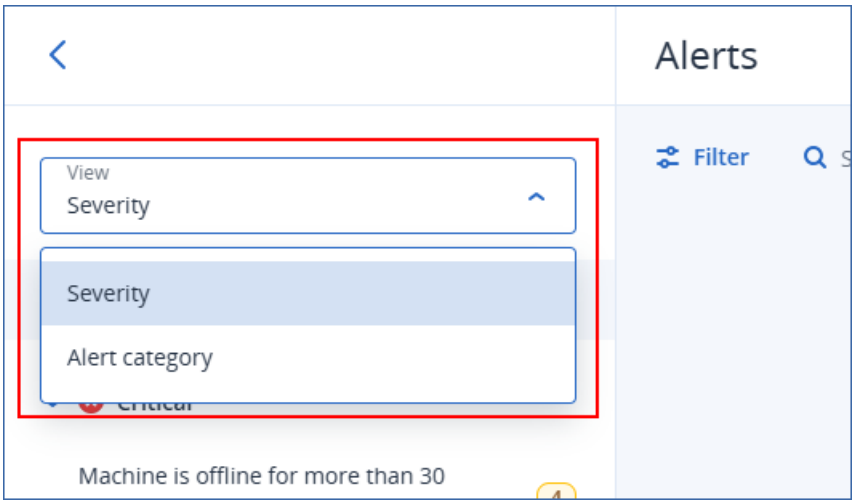
Alertas de filtrado

Puede utilizar el filtro rápido o el filtro principal.

Filtro rápido

Pasos para filtrar las alertas

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. En la lista desplegable **Vista**, seleccione los criterios del filtro.



3. [Opcional] [Si seleccionó **Categoría de alerta**] Seleccione una categoría de alerta específica.
4. [Opcional] Seleccione un tipo de alerta específico.

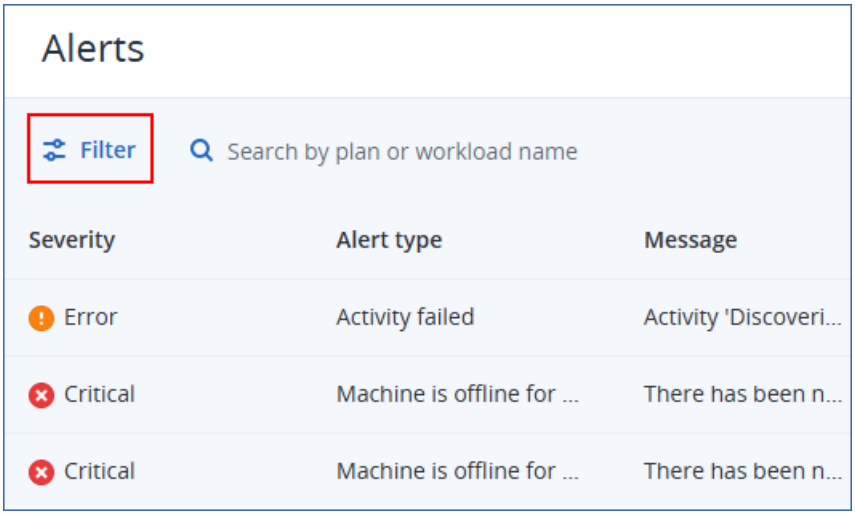
Como resultado, se enumeran las alertas que coinciden con los criterios del filtro.

Filtro principal

Pasos para filtrar las alertas

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. Haga clic en **Filtro**.



3. Configure los criterios del filtro y haga clic en **Aplicar**.

Nota
Los criterios del filtro disponibles dependen de la configuración del filtro rápido que ya puede haber configurado.

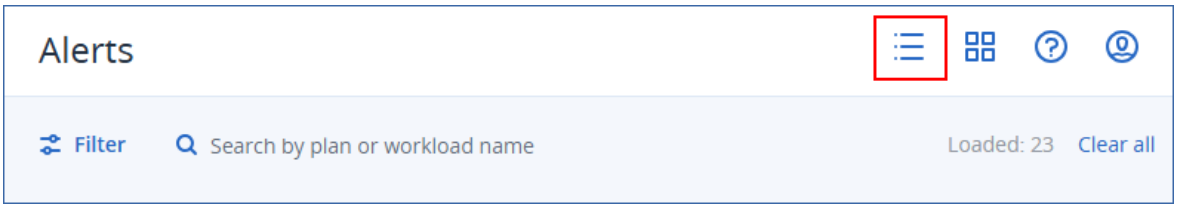
Como resultado, se enumeran las alertas que coinciden con los criterios del filtro.

Ordenación de alertas

Cuando utilice la vista de tabla, puede ordenar las alertas en orden descendente o ascendente.

Pasos para ordenar las alertas

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. [Si utiliza la vista simple] Haga clic en el icono de vista de tabla.



3. Haga clic en el nombre de la columna en la que desea ordenar las alertas.

Nota
No puede ordenar las alertas al hacer clic en la columna **Mensaje**.

Como resultado, las alertas se ordenan y se muestra una flecha junto al nombre de la columna seleccionada.

© Acronis International GmbH, 2003-2025

Creación de un ticket del centro de asistencia a partir de una alerta

Si el servicio PSA está habilitado para su cuenta, también puede crear un nuevo ticket del centro de asistencia directamente desde la alerta.

Pasos para crear un ticket del centro de asistencia

1. Haga clic en **Crear un nuevo ticket** en la alerta correspondiente.
   De manera alternativa, cuando trabaje en el modo de vista de tabla, seleccione una alerta y luego **Crear un nuevo ticket** en el panel derecho.
2. Defina lo siguiente:
   - En la sección del encabezado, seleccione la casilla de verificación **Facturable** si quiere que se facture al cliente el tiempo registrado en el ticket. Asimismo, seleccione la casilla de verificación **Enviar un correo electrónico al cliente** si desea enviar actualizaciones del ticket al cliente.
   - En la sección **Información general**, defina un título para el ticket. Este campo se completa automáticamente con un resumen de la alerta, pero puede editarse.
   - En la sección **Información del cliente**, los campos se completan automáticamente con la información correspondiente de la alerta.
   - En la sección **Elemento o servicio de configuración**, los campos se completan automáticamente con el dispositivo vinculado a la alerta. Puede reasignar un dispositivo, según sea necesario.
   - En la sección **Agente de soporte técnico**, los campos se completan automáticamente con el agente de soporte técnico, la categoría y el grupo de soporte técnico predeterminados. Puede reasignar un agente diferente, según sea necesario.
   - En la sección **Actualización del ticket**, los campos se completan automáticamente con la descripción y la información de la alerta. El campo **Estado** se establece como **Nuevo** de forma predeterminada y puede cambiarse.
   - En las secciones **Adjuntos**, **Elementos facturables** y **Notas internas**, añada los elementos correspondientes según sea necesario.
3. Haga clic en **Listo**.
   Cuando se cree el ticket, se añadirá un enlace al ticket en la alerta.
   Si se cierra una alerta, el ticket relacionado con ella se cerrará automáticamente.

Nota
Solo puede crear un ticket por alerta.

Tipos y categorías de alertas

Los tipos de alerta se agrupan en las siguientes categorías:

- Alertas de copia de seguridad
- Alertas de recuperación ante desastres

© Acronis International GmbH, 2003-2025

- Alertas de protección antimalware
- Alertas de filtrado de URL
- Alertas de licencias
- Alertas de EDR
- Alertas de control de dispositivos
- Alertas del sistema
- Alertas de conexión a nubes públicas
- Alertas de despliegue del software
- Gestión
- Búsqueda
- Supervisión

Alertas de copia de seguridad

Tipo de alerta	Descripción	Cómo resolver la alerta
Error al realizar copia de seguridad	La alerta se genera cuando una copia de seguridad falla con un error resoluble o se interrumpe debido al apagado del sistema.	Revise el registro de la operación de copia de seguridad. Haga clic en la carga de trabajo para seleccionarla y después en **Actividades** para encontrar la advertencia en el registro. El mensaje debería indicarle la causa raíz del problema.
Copia de seguridad completada con advertencias	La alerta se genera cuando se realiza una copia de seguridad correctamente pero con advertencias.	Revise el registro de la operación de copia de seguridad. Haga clic en la carga de trabajo para seleccionarla y después en **Actividades** para encontrar la advertencia en el registro. El mensaje debería indicarle la causa raíz del problema.
Se ha cancelado la copia de seguridad	La alerta se genera cada vez que un usuario cancela manualmente una copia de seguridad.	Puede iniciar la copia de seguridad manualmente haciendo clic en **Ejecutar ahora** o esperar hasta que se ejecute en el próximo horario programado.
Copia de seguridad cancelada debido al cierre de una ventana de copia de seguridad	La alerta se genera cuando se salta la actividad de copia de seguridad porque no quedaba tiempo en la ventana especificada en las opciones de copia de seguridad.	Reconfigure el horario o edite las opciones del plan de copia de seguridad en la ventana **Rendimiento y copia de seguridad**. Expanda la sección con su producto para obtener

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		instrucciones.
La copia de seguridad está en espera	La alerta se genera cuando hay un conflicto de programación y se inician dos tareas de copia de seguridad al mismo tiempo. En este caso, la segunda tarea de copia de seguridad se pone en cola hasta que la primera haya terminado o se haya detenido.	Asegúrese de que sus copias de seguridad se estén ejecutando en los intervalos de tiempo esperados y de acuerdo a su programación, y evite conflictos de programación.
La copia de seguridad no responde	La alerta se genera cuando una copia de seguridad no ha mostrado ningún progreso durante un tiempo, y podría estar congelada.	El problema podría ser causado por un bloqueo. Para obtener más información, consulte este artículo de la base de conocimientos.
La copia de seguridad no se ha iniciado	La alerta se genera cuando no se puede iniciar la copia de seguridad programada por un motivo desconocido.	Asegúrese de que está utilizando la última versión de su producto Acronis Backup. • Si el equipo del agente estaba disponible a la hora de inicio de la copia de seguridad: 1. Modifique la hora de inicio de la tarea de copia de seguridad. 2. Si vuelve a saltar la alerta, vuelva a crear la tarea de copia de seguridad. 3. Si la tarea de copia de seguridad recién creada también activa la alerta, contacte con el equipo de soporte para obtener asistencia. • Si el agente estaba offline: 1. No apague el equipo a la hora de la copia de seguridad. 2. Si la máquina no se apagó, asegúrese de que Acronis Managed Machine Service esté en funcionamiento: Inicio -> Buscar -> services.msc -> localizar Acronis Managed Machine Service. Si necesita ayuda, póngase en contacto con el equipo de soporte.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
Se desconoce el estado de la copia de seguridad	La alerta se genera cuando el agente de copia de seguridad estaba desconectado en el momento programado para la copia de seguridad. El estado de las copias de seguridad de los recursos será desconocido hasta que el agente de copia de seguridad se conecte.	1. Compruebe si estaba previsto que el agente estuviera offline (por ejemplo, en el caso de un cuaderno que está fuera de la red del servidor de administración). 2. Si el agente no debe estar desconectado, asegúrese de que el Acronis Managed Machine Service esté en funcionamiento: Inicio -> Buscar -> services.msc -> localice el Acronis Managed Machine Service y verifique su estado. Si el servicio está detenido, inícielo.
Falta la copia de seguridad	La alerta se genera cuando no se ha completado una copia de seguridad en más de [Días desde la última copia de seguridad] días, lo cual se define en la opción de Alertas de copia de seguridad.	Asegúrese de que el plan con la opción de **Alertas** de copia de seguridad habilitada esté programado y se ejecute al menos una vez dentro del período definido configurado para esta opción
La copia de seguridad está dañada	La alerta se genera cuando se completa la actividad de validación y muestra que la copia de seguridad está dañada.	Siga los pasos del artículo Solución de problemas con copias de seguridad corruptas. Si necesita ayuda para identificar la causa raíz de la corrupción del archivo, contacte con el equipo de soporte.
Ha fallado la protección continua de datos	La alerta se genera si ha fallado la protección continua de la copia de seguridad.	Compruebe las siguientes limitaciones: 1. La Protección continua de datos solo es compatible con el sistema de archivos NTFS y los siguientes sistemas operativos: • Escritorio: Windows 7 y posterior • Servidor: Windows Server 2008 R2 y posterior 2. CDP no admite **Acronis Secure Zone** como destino. 3. No se admiten las carpetas NFS

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		montadas en Windows. 4. No se admite la replicación continua: si hay dos ubicaciones en el plan de protección, las porciones de CDP solo se crean en el primer destino y los cambios se replican en el segundo durante la siguiente copia de seguridad. 5. Si se aplican cambios en una carpeta local protegida desde una fuente de red (por ejemplo, cuando los usuarios acceden a la carpeta desde la red), CDP no los detecta. 6. Si se está utilizando un archivo (por ejemplo, se están realizando algunos cambios en un archivo de Excel), CDP no detecta los cambios. Para que CDP detecte los cambios, guárdelos y luego cierre el archivo.
La validación ha fallado	La alerta se genera cuando el proceso de validación de la copia de seguridad no puede completarse.	Revise el registro de la operación fallida. Haga clic en la carga de trabajo para seleccionarla y después en **Actividades** para encontrar la advertencia en el registro. El mensaje debería indicarle la causa raíz del problema.
No se encuentra la contraseña de cifrado	La alerta se genera cuando falta la clave de cifrado de la base de datos o cuando es incorrecta o está dañada.	No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña. Debe establecer la contraseña de cifrado de forma local en el dispositivo protegido. No podrá establecer la contraseña de cifrado en el plan de protección. Para obtener más información, consulte Definición de la contraseña de cifrado.
La carga está pendiente	La alerta se genera si la comprobación programada descubre que el servicio de envío	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	físico al archivo en la nube para este plan de copias de seguridad no se ha cargado en el almacenamiento.	
Error en la recuperación de la copia de seguridad	La alerta se genera cuando falla la operación de recuperación al intentar recuperar copias de seguridad del sistema o de archivos.	Determina la fecha exacta del fallo de la copia de seguridad e intenta la recuperación con la última copia de seguridad correcta.

Alertas de recuperación ante desastres

Tipo de alerta	Descripción	Cómo resolver la alerta
Se ha alcanzado la cuota flexible para los servidores en la nube	La alerta se genera cuando se supera la cuota flexible para el almacenamiento de recuperación ante desastres.	Aumenta la cuota o elimina algunas copias de seguridad del almacenamiento en la nube.
Se ha alcanzado la cuota flexible	La alerta se genera cuando se supera la cuota flexible para las siguientes opciones: • Servidor en la nube. • Puntos de cálculo. • Direcciones IP públicas.	
Se ha superado la cuota de almacenamiento	La alerta se genera cuando se supera la cuota máxima para el almacenamiento de recuperación ante desastres. Este almacenamiento es utilizado por los servidores primarios y de recuperación. Si se alcanza el exceso de esta cuota, no será posible crear servidores primarios y de recuperación, o añadir o ampliar los discos de los servidores primarios existentes. Si se supera el exceso de esta cuota, no ser posible realizar una conmutación por error o simplemente iniciar un servidor detenido. Los servidores en	Póngase en contacto con su socio para aumentar la cuota asignada.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	funcionamiento continúan funcionando.	
Se ha superado la cuota estricta	La alerta se genera cuando se supera la cuota máxima para las siguientes opciones: • Servidores en la nube. • Puntos de cálculo. • Direcciones IP públicas.	Plantéese comprar cuotas adicionales o deshabilite las tareas de copia de seguridad en los dispositivos que ya no necesita proteger.
Error de conmutación por error	La alerta se genera cuando ocurre un problema del sistema después de que se inició una conmutación por error.	1. Seleccione el servidor de recuperación y luego haga clic en **Editar**. 2. Disminuya la CPU/RAM del servidor de recuperación. 3. Intente realizar una conmutación por error de nuevo.
Error en prueba de conmutación por error	La alerta se genera cuando ocurre un problema del sistema después del inicio de una conmutación por error de prueba.	1. Seleccione el servidor de recuperación y luego haga clic en **Editar**. 2. Disminuya la CPU/RAM del servidor de recuperación. 3. Intente realizar otra vez una conmutación por error de prueba. **Nota** Asegúrese de que la dirección IP de la red de producción sea la misma que la dirección IP que está configurada en el servidor DHCP.
Error de conmutación por recuperación	La alerta se genera cuando ocurre un problema del sistema después de que se inició una conmutación tras recuperación.	Puede ver la ubicación errónea en la lista de almacenamientos de copia de seguridad: tiene un número en lugar de un nombre (por lo general, el nombre de una ubicación coincide con uno de los nombres de usuario final existentes) y no la ha creado usted. Elimine la ubicación errónea: 1. En la consola de Cyber Protect, vaya a **Almacenamiento de la**

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		copia de seguridad. 2. Busque la ubicación y haga clic en el icono de cruz (x) para borrarla. 3. Haga clic en **Eliminar** para confirmar su elección. 4. Vuelva a intentar la conmutación por error.
Error de conmutación por recuperación: la copia de seguridad ha fallado	Esta alerta se genera cuando la copia de seguridad del servidor de recuperación durante el proceso de conmutación tras recuperación falla.	
Error de conmutación por recuperación: el cambio ha fallado.	Esta alerta se genera cuando el proceso de conmutación tras recuperación ha vuelto a la fase de transferencia de datos y la máquina virtual en la nube se ha iniciado.	Intente realizar el cambio nuevamente. Si falla, contacte con el equipo de soporte.
Se ha cancelado la conmutación por recuperación	La alerta se genera cuando un usuario cancela una conmutación tras recuperación.	Descarte manualmente la alerta de la consola.
Error de conexión VPN	La alerta se genera cuando se produce un fallo en la conexión VPN debido a razones que no están relacionadas con las acciones del usuario. El informe de estado del dispositivo VPN está obsoleto.	Si se encontró un problema al desplegar o conectar el dispositivo VPN Acronis, contacte con el equipo de soporte. Incluya la siguiente información en su correo electrónico: • Capturas de pantalla de los mensajes de error (si los hubiera) • Captura de pantalla de la interfaz CLI del dispositivo VPN Acronis • Su centro de datos de Acronis Backup Cloud y nombre de grupo.
(VPN no accesible) La puerta de enlace de conectividad no es accesible	La alerta se genera cuando el servicio de Disaster Recovery no puede alcanzar la puerta de enlace de conectividad. El	En caso de que haya tenido un problema al desplegar o conectar el dispositivo VPN Acronis, póngase en contacto con el equipo de soporte.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	informe de estado de la puerta de enlace de conectividad está obsoleto.	Incluya la siguiente información en su correo electrónico: • Capturas de pantalla de los mensajes de error (si los hubiera) • Captura de pantalla de la interfaz CLI del dispositivo VPN Acronis • Su centro de datos de Acronis Backup Cloud y nombre de grupo
Error de conexión de IPsec VPN	Esta alerta se genera cuando hay un error durante la negociación de la Fase 1 del IKE (Intercambio de Claves de Internet).	Compruebe la configuración de IPsec IKE (Intercambio de Claves de Internet) en el sitio local y en la nube.
Es necesario reasignar la IP de recuperación ante desastres	La alerta se genera cuando el dispositivo VPN detecta cambios en la red.	Reasigne la dirección IP. Para obtener más información, consulte "Reasignación de direcciones IP" (p. 1055)
Fallo de la puerta de enlace de conectividad	La alerta se genera cuando falla la implementación del servidor VPN en la nube.	Utilice la herramienta de verificación de la conexión y compruebe si hay errores en el resultado. Permita que el software Acronis pase a través del control de aplicaciones de sus cortafuegos y software antimalware.
Fallo al crear el servidor principal	La alerta se genera cuando el servidor principal no se creó debido a un error.	
Fallo al crear el servidor de recuperación	La alerta se genera cuando el servidor de recuperación no se creó debido a un error.	Asegúrese de que el servidor de recuperación cumpla con los requisitos de software. Para obtener más información, consulte "Requisitos de software para Disaster Recovery para Cyber Protect Cloud" (p. 1011).
Eliminar servidor principal	La alerta se genera cuando se elimina un servidor principal.	
Fallo de recuperación del servidor	La alerta se genera cuando el servidor principal o de	Encuentre los detalles. Si el mensaje

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	recuperación no logra recuperarse.	de error es genérico o poco claro (por ejemplo "Error interno") navegue a **Disaster Recovery → Servidores**, haga clic para seleccionar la máquina afectada, y luego en **Actividades**. Marque una actividad, mantenga pulsado CTRL y haga clic con el botón izquierdo en la actividad. Seleccione el icono de elipsis (...) de la actividad, y luego haga clic en **Información de actividad de tarea**.
Error al realizar copia de seguridad	La alerta se genera cuando falla una copia de seguridad del servidor en la nube (primario o servidor en el estado de conmutación por error de producción).	1. Verifique la conexión con la ubicación de la copia de seguridad. 2. Compruebe el dispositivo de almacenamiento de copia de seguridad (copias de seguridad locales).
Se ha excedido el límite de redes	La alerta se genera cuando se alcanza el número máximo de redes en la nube (5 redes).	Elimine o edite las redes de la nube para asegurarse de que coincidan con la configuración de la red local.
Error de runbook	La alerta se genera cuando falla la ejecución del runbook.	Esto no afecta a las funciones del producto, y se puede ignorar de manera segura. Para obtener más información, consulte "Creación de un runbook" (p. 1100).
Aviso de runbook	La alerta se genera cuando la ejecución del runbook se completa con advertencias.	Esto no afecta a las funciones del producto, y se puede ignorar de manera segura. Para obtener más información, consulte "Creación de un runbook" (p. 1100).
Se requiere la interacción del usuario en el runbook	La alerta se genera cuando el runbook está esperando una interacción del usuario.	Esto no afecta la funcionalidad del producto y se puede ignorar de manera segura. Alternativamente, puede realizar la acción que se describe en la sección **Acción del usuario**. Para más información, consulte "Creación de un runbook" (p. 1100).
Tráfico de Internet bloqueado	La alerta se genera cuando,	Comuníquese con el equipo de

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	debido a riesgos de seguridad, un administrador bloquea el tráfico de internet para una o más de las IP públicas en su cuenta.	soporte.
Tráfico de Internet desbloqueado	La alerta se genera cuando un administrador desbloquea el tráfico de internet para su cuenta.	
Superposición de redes locales	La alerta se genera cuando se detectan redes locales idénticas o superpuestas.	Compruebe la configuración del dispositivo VPN.
Cuota de servidores insuficiente para cambio de licencia	La alerta se genera cuando la cuota de servidores en la nube no es suficiente.	• Si la alerta se genera para un servidor físico, asegúrese de que el inquilino y el usuario tengan suficiente cuota para las opciones **Servidores de alojamiento web** o **Servidores**. • Si la alerta se genera para un servidor virtual, asegúrese de que el inquilino y el usuario tengan suficiente cuota para las opciones **Servidores de alojamiento web** o **Equipos virtuales**. Un servidor virtual no puede utilizar la cuota para la oferta de **Servidores**.
Artículo de oferta insuficiente para cambio de licencia	La alerta se genera cuando la opción **Almacenamiento de recuperación ante desastres** está desactivada.	
Error de cambio de licencia	La alerta se genera cuando la actualización de recuperación ante desastres encuentra un error.	Comuníquese con el equipo de soporte.
Puntos de cálculo insuficientes para cambio de licencia	La alerta se genera cuando no hay puntos de cálculo disponibles.	Aumenta la cuota estricta para la opción **Puntos de cálculo**.
Artículos de oferta de servidores insuficientes para	La alerta se genera cuando se desactiva la opción **Servidores**	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
cambio de licencia	**en la nube**.	
La directiva no ha podido crear el servidor de recuperación	La alerta se genera cuando ocurre un error al configurar la infraestructura de recuperación ante desastres.	Cree manualmente un servidor de recuperación, sin la propiedad de **Acceso a Internet**. Para obtener más información, consulte "Creación de un servidor de recuperación" (p. 1062).
Reprogramación de la conmutación por error de prueba automatizada del procesador de copias de seguridad	La alerta se genera cuando la conmutación por error de prueba automatizada se reprograma.	• Inicie manualmente una conmutación por error de prueba del servidor de recuperación. Para obtener más información, consulte "Ejecución de una prueba de conmutación por error" (p. 1078). • Espere la próxima fecha programada para la prueba automática de conmutación por error.
Tiempo de espera agotado en la conmutación por error de prueba automática del procesador de copias de seguridad	La alerta se genera cuando la conmutación por error de prueba automatizada expira. **Nota** Cada conmutación por error de prueba automatizada consume puntos de cálculo.	• Aumente el valor de tiempo de espera para la prueba automática de conmutación por error. • Espere la próxima fecha programada para la prueba automática de conmutación por error. • Inicie manualmente una conmutación por error de prueba del servidor de recuperación. Para obtener más información, consulte "Ejecución de una prueba de conmutación por error" (p. 1078).
Fallo general de la conmutación por error de prueba automatizada del procesador de copias de seguridad	La alerta se genera cuando falla la última conmutación por error de prueba automatizada programada del servidor de recuperación.	• Inicie manualmente una conmutación por error de prueba del servidor de recuperación. Para obtener más información, consulte "Ejecución de una prueba de conmutación por error" (p. 1078). • Espere a la siguiente fecha programada para la ejecución de

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		la conmutación por error de prueba automatizada.
Advertencia de conmutación por error de prueba automatizada	Esta alerta se genera cuando la copia de seguridad está cifrada.	Introduzca la contraseña de cifrado en la configuración del servidor de recuperación.
Error en la prueba automatizada de conmutación por error	Esta alerta se genera cuando una conmutación por error de prueba automatizada falla.	Introduzca la contraseña de cifrado para la copia de seguridad en la configuración del servidor de recuperación. La operación se iniciará de nuevo.
La conmutación por error de prueba automática ha fallado: se ha superado la cuota del artículo de oferta	Esta alerta se genera cuando la prueba automática de conmutación por error falla. El servidor de recuperación ya no tiene licencia debido a que se excedió la cuota estricta para uno de los siguientes artículos de oferta: • **DR y copia de seguridad directa en Azure** • **DR a Acronis o nube híbrida** • **Estaciones de trabajo** • **Equipos virtuales** • **Servidores**	Póngase en contacto con su socio para aumentar la cuota asignada.
La conmutación por error de prueba automática ha fallado: artículo de oferta deshabilitado	Esta alerta se genera cuando la prueba de conmutación por error automática falla. El servidor de recuperación ya no tiene licencia porque uno de los siguientes artículos de oferta fue deshabilitado: • **Estaciones de trabajo** • **Equipos virtuales** • **Servidores**	Póngase en contacto con su socio para aumentar la cuota asignada.
Se desactivó la protección de Disaster Recovery para una carga de trabajo	Esta alerta se genera cuando la protección de Disaster Recovery fue deshabilitada para una carga de trabajo porque se excedió la cuota estricta para uno de los siguientes artículos de oferta:	Póngase en contacto con su socio para aumentar la cuota asignada.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	• **DR y copia de seguridad directa en Azure** • **DR a Acronis o nube híbrida**	
El servidor de recuperación no tiene licencia	Esta alerta se genera cuando el servidor de recuperación ya no tiene licencia porque se excedió la cuota estricta para uno de los siguientes artículos de oferta: • **DR y copia de seguridad directa en Azure** • **DR a Acronis o nube híbrida**	Póngase en contacto con su socio para aumentar la cuota asignada.
El servidor principal no tiene licencia	Esta alerta se genera cuando el servidor primario ya no tiene licencia porque: • se superó la cuota estricta para el artículo de oferta **Servidores primarios**. • se deshabilitó el artículo de oferta **Servidores primarios**.	Póngase en contacto con su socio para aumentar la cuota asignada.
El servidor de recuperación no tiene licencia: se ha excedido la cuota del artículo de oferta	Esta alerta se genera cuando el servidor de recuperación ya no tiene licencia debido a que se excedió la cuota estricta para uno de los siguientes artículos de oferta: • **Estaciones de trabajo** • **Equipos virtuales** • **Servidores** Las operaciones de recuperación ante desastres podrían estar limitadas o no ser compatibles.	Póngase en contacto con su socio para aumentar la cuota asignada.
El servidor de recuperación no tiene licencia: artículo de oferta deshabilitado	Esta alerta se genera cuando el servidor de recuperación ya no tiene licencia porque uno de los siguientes artículos de oferta fue deshabilitado: • **Estaciones de trabajo** • **Equipos virtuales** • **Servidores**	Póngase en contacto con su socio para aumentar la cuota asignada.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	Las operaciones de recuperación ante desastres podrían estar limitadas o no ser compatibles.	
Error de transferencia de datos durante la conmutación tras recuperación	La alerta se genera cuando falla la fase de transferencia de datos de la conmutación tras recuperación.	Reintente la operación. Si vuelve a fallar, póngase en contacto con el equipo de soporte.
Fallo de conmutación tras recuperación	La alerta se genera cuando hay un error en la conmutación tras recuperación.	Puede ver la ubicación errónea en la lista de almacenamientos de copia de seguridad: tiene un número en lugar de un nombre (por lo general, el nombre de una ubicación coincide con uno de los nombres de usuario final existentes) y no la ha creado usted. Elimine la ubicación errónea: 1. En Cyber Protection, vaya a **Almacenamiento de la copia de seguridad**. 2. Encuentre la ubicación y luego haga clic en el icono de la cruz (x) para eliminarla. 3. Haga clic en **Eliminar** para confirmar su elección. 4. Inicie la conmutación por error de nuevo.
Fallo al confirmar la conmutación tras recuperación	La alerta se genera cuando la confirmación de la conmutación tras recuperación falla.	Reintente la operación. Si vuelve a fallar, póngase en contacto con el equipo de soporte.
El equipo de conmutación tras recuperación está listo para el cambio	La alerta se genera cuando el equipo está listo para el cambio. Más del 90 % de los datos se han transferido al sitio local.	
Cambio de conmutación tras recuperación finalizado	La alerta se genera cuando el cambio termina correctamente. La máquina virtual se restaura en el sitio local.	Descarte manualmente la alerta de la consola.
Agente de destino de la conmutación tras recuperación offline	La alerta se genera cuando el agente que se utiliza en el proceso de conmutación tras recuperación está offline.	Asegúrese de que el agente tenga acceso a Internet. Si es necesario, reinicie el agente.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
client_id de WebCP duplicado	Esta alerta se genera cuando hay un client_id duplicado para un recurso.	
Despliegue de Azure restaurado de la papelera de reciclaje	Esta alerta se genera cuando se restaura la infraestructura de recuperación ante desastres desde la papelera de reciclaje. Se detuvieron los servidores de recuperación en la conmutación por error de producción.	
Despliegue restaurado de la papelera de reciclaje	Esta alerta se genera cuando se restaura la infraestructura de recuperación ante desastres desde la papelera de reciclaje. Se detuvieron los servidores primario y de recuperación en la conmutación por error de producción.	
Se omitió la eliminación del grupo de recursos de Azure	Esta alerta se genera cuando un grupo de recursos de Azure no se pudo eliminar debido a un problema de conexión con la nube.	

Alertas de protección antimalware

Tipo de alerta	Descripción	Cómo resolver la alerta
Se ha evitado el intento de desinstalación o actualización del agente	La alerta se genera en cada intento de actualizar o desinstalar manualmente un agente de protección fuera del período de mantenimiento especificado, cuando la opción **Protección de desinstalación del agente** está habilitada para el agente.	Descarte manualmente la alerta de la consola. Consulte "Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada" (p. 213).
Se ha detectado una actividad de conexión remota sospechosa	La alerta se genera cuando se detecta un ransomware proveniente de una conexión remota.	Descarte manualmente la alerta de la consola.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
Actividad sospechosa detectada	La alerta se genera cuando se detecta un ransomware en la carga de trabajo.	Descarte manualmente la alerta de la consola. para desactivar la alerta. Según la opción que haya especificado en el plan de Active Protection, se detendrá el proceso malicioso, se revertirán los cambios realizados en el proceso o no se hará nada y tendrá que resolver el problema manualmente. Lea los detalles de la alerta para comprobar qué proceso está cifrando archivos y qué archivos están afectados. Si decide que el proceso que cifra los archivos está sancionado (alerta por falso positivo), añada este proceso a los procesos de confianza: 1. Abra el plan de Active Protection. 2. Haga clic en **Editar** para modificar la configuración. 3. En **Procesos de confianza**, especifique los procesos de confianza que nunca se considerarán ransomware. Especifique la ruta completa al ejecutable del proceso, comenzando con la letra de unidad. Por ejemplo: `C:\Windows\Temp\er76s7sdkh.exe`
Actividad de criptominería detectada	La alerta se genera cuando se detectan criptomineros ilícitos en la carga de trabajo.	Descarte manualmente la alerta de la consola.
Defensa de MBR: Actividad sospechosa detectada y suspendida	La alerta se genera cuando se detecta ransomware en la carga de trabajo (específicamente si el ransomware modifica la partición del MBR/GPT).	Descarte manualmente la alerta de la consola.
Se ha especificado una ruta de red no compatible	La alerta se genera cuando la ruta de recuperación que ha proporcionado el administrador no es una ruta de carpeta local.	Especifique la ruta local para la protección de la carpeta de red (ruta de recuperación). Descarte manualmente la alerta de la consola.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
El proceso crítico se añade como dañino en el plan de Active Protection	La alerta se genera cuando se añade un proceso crítico como un proceso bloqueado a la lista de exclusiones de protección.	Contacte al administrador para eliminar el proceso crítico de la lista de Exclusiones.
No se ha podido aplicar la directiva Active Protection	La alerta se genera cuando falla la aplicación de la política de Active Protection.	Compruebe el mensaje de error para ver por qué no se puede aplicar la directiva de Active Protection.
Secure Zone: Se ha detectado y bloqueado una operación no autorizada	La alerta se genera cuando se detecta ransomware en la carga de trabajo (específicamente si el ransomware modifica la partición de ASZ).	Descarte manualmente la alerta de la consola.
No se está ejecutando el servicio Active Protection	La alerta se genera cuando el servicio Active Protection se bloquea o no se está ejecutando.	Compruebe el mensaje de error para ver por qué no se está ejecutando el servicio Active Protection.
El servicio Active Protection no está disponible	La alerta se genera cuando el servicio Active Protection no está disponible porque falta un controlador o este no es compatible.	Compruebe en los registros de eventos de Windows si se ha bloqueado el servicio Acronis Active Protection (acronis_ protection_service.exe).
Conflicto con otra solución de seguridad	Se genera una alerta si Active Protection no está disponible para el equipo " {{resourceName}}" porque se ha detectado un conflicto con otra solución de seguridad. Para habilitar Active Protection, deshabilite o desinstale la solución de seguridad en conflicto.	**Solución 1**: si quiere usar protección en tiempo real Acronis, desinstale el software antivirus de terceros de la carga de trabajo. **Solución 2**: Si quiere usar el antivirus de terceros, en el plan de protección que se aplica a la carga de trabajo, desactive la protección en tiempo real de Acronis, el filtrado de URL y el antivirus de Windows Defender.
La acción de cuarentena ha fallado	La alerta se genera cuando el antimalware no logra poner en cuarentena un malware detectado.	Compruebe el mensaje de error para ver por qué no se ha podido poner en cuarentena.
Se ha detectado un proceso malicioso	La alerta se genera cuando el motor de comportamiento detecta un malware (tipo de proceso). Se pone en	Descarte manualmente la alerta de la consola.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	cuarentena el malware detectado.	
Se ha detectado un proceso malicioso, pero no se ha puesto en cuarentena	La alerta se genera cuando el motor de comportamiento detecta un malware (tipo de proceso). No se pone en cuarentena el malware detectado.	Descarte manualmente la alerta de la consola.
Se ha detectado y bloqueado malware (ODS)	La alerta se genera cuando el análisis programado detecta un malware. Se pone en cuarentena el malware detectado.	Descarte manualmente la alerta de la consola.
Se ha detectado y bloqueado malware (RTP)	La alerta se genera cuando la protección en tiempo real detecta un malware. Se pone en cuarentena el malware detectado.	Descarte manualmente la alerta de la consola.
Se ha detectado malware en una copia de seguridad	La alerta se genera cuando se detecta un malware durante el escaneo de la copia de seguridad.	Descarte manualmente la alerta de la consola.
Conflicto detectado entre la protección antimalware en tiempo real y el producto de seguridad	La alerta se genera cuando el antimalware no logra registrarse en el centro de seguridad de Windows.	**Solución 1**: si quiere usar protección en tiempo real Acronis, desinstale el software antivirus de terceros de la carga de trabajo. **Solución 2**: Si quiere usar el antivirus de terceros, en el plan de protección que se aplica a la carga de trabajo, desactive la protección en tiempo real de Acronis, el filtrado de URL y el antivirus de Windows Defender.
No se ha podido ejecutar el módulo Microsoft Security Essentials	La alerta se genera cuando se produce un error en la ejecución del módulo de Microsoft Security Essentials.	Compruebe el mensaje de error para ver por qué no se ha podido ejecutar el módulo de Microsoft Security Essentials.
La protección en tiempo real no está disponible porque hay instalado un software antivirus de terceros	La alerta se genera cuando la protección en tiempo real no se pudo activar porque el antivirus de terceros tiene habilitada la protección en tiempo real.	Deshabilite o desinstale el producto de seguridad de terceros, o deshabilite la protección antimalware en tiempo real del plan de protección.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
La protección en tiempo real no está disponible porque falta un controlador o este no es compatible	La alerta se genera cuando la protección en tiempo real no está disponible debido a un controlador incompatible o que falta.	Consulte el mensaje de error para ver por qué falló la instalación del controlador en la carga de trabajo.
El servicio Cyber Protection (o Active Protection) no responde	La alerta se genera cuando el servicio de ciberprotección responde a un ping de comprobación de estado desde la consola.	
No se ha podido actualizar la definición de seguridad	La alerta se genera cuando falla una actualización de la definición de seguridad.	Consulte el mensaje de error para ver por qué falló la actualización de la definición de seguridad.
La Protección contra alteraciones está habilitada	La alerta se genera cuando no se pueden cambiar la configuración de Microsoft Defender porque la protección contra alteraciones está habilitada.	Deshabilite la configuración de la Protección contra alteraciones en la carga de trabajo de Windows.
No se ha podido ejecutar el módulo de Windows Defender	La alerta se genera cuando falla la ejecución del módulo de Windows Defender.	Consulte el mensaje de error para ver por qué el módulo de Windows Defender no pudo ejecutarse.
Windows Defender está bloqueado por el software antivirus de un tercero	La alerta se genera cuando Windows Defender está bloqueado porque se ha instalado un software antivirus de terceros en la máquina.	Desactive o desinstale el producto de seguridad de terceros.
Conflicto de directiva de grupo	La alerta se genera cuando no se puede cambiar la configuración de Microsoft Defender porque está controlada por una directiva de grupo.	Desactive la configuración de la directiva de grupo en la carga de trabajo de Windows.
Microsoft Security Essentials ha tomado medidas para proteger este equipo de malware	La alerta se genera cuando Microsoft Security Essentials ha eliminado o puesto en cuarentena un malware.	Descarte manualmente la alerta de la consola.
Microsoft Security Essentials ha detectado	La alerta se genera cuando Microsoft Security Essentials	Descarte manualmente la alerta de la consola.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
malware	detecta malware u otro software potencialmente no deseado.	
Malware detectado en copia de seguridad de buzón de correo de M365	La alerta se genera cuando se detecta un malware durante el escaneo de la copia de seguridad.	Descarte manualmente la alerta de la consola.
El motor de comportamiento no está disponible	Esta alerta se genera cuando el motor de Comportamiento no está disponible en una carga de trabajo porque un controlador es incompatible o falta.	Asegúrese de que el controlador esté instalado correctamente en la carga de trabajo.
Se ha detectado una aplicación potencialmente no deseada	Esta alerta se genera cuando se detecta una aplicación potencialmente no deseada.	Descarte manualmente la alerta de la consola.
El análisis de la copia de seguridad en busca de malware no se ha iniciado	Esta alerta se genera cuando el escaneo de copia de seguridad no se ejecuta según la planificación.	Verifique el mensaje de error, por qué el escaneo de copia de seguridad no se inició.

Alertas de filtrado de URL

Tipo de alerta	Descripción	Cómo resolver la alerta
Se ha bloqueado una URL maliciosa	La alerta se genera cuando una URL maliciosa es bloqueada por el filtrado de URL.	Verifique la configuración del filtrado de URL. Está bloqueando páginas que se supone deben estar bloqueadas de acuerdo con la configuración del filtrado de URL. Para obtener más información, consulte "Filtrado de URL" (p. 1192).
Se ha ignorado una advertencia de URL maliciosa	La alerta se genera cuando decide continuar con la URL maliciosa que ha bloqueado el filtrado de URL.	Compruebe la configuración del filtrado de URL.
Conflicto detectado entre el filtrado de URL y un producto de seguridad	La alerta se genera cuando no se puede habilitar el filtrado de URL debido a un conflicto con otro producto de seguridad.	Compruebe la configuración del filtrado de URL.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
La URL del sitio web está bloqueada	La alerta se genera cuando una URL cumple todos los criterios especificados en la categoría bloqueada del filtrado de URL.	Compruebe la configuración del filtrado de URL.
Se ha detectado una URL maliciosa en un correo electrónico	Esta alerta se genera cuando el filtrado de URL detectó una URL maliciosa en una copia de seguridad de buzón de correo de M365. La acción al detectar mediante el filtrado de URL está configurada para Solo notificar.	Compruebe la configuración del filtrado de URL.
Se ha detectado una URL maliciosa	Esta alerta se genera cuando el filtrado de URL detectó una URL maliciosa. La acción al detectar mediante el filtrado de URL está configurada para Solo notificar.	Compruebe la configuración del filtrado de URL.

Alertas de licencias

Tipo de alerta	Descripción	Cómo resolver la alerta
Casi se ha alcanzado la cuota de almacenamiento	La alerta se genera cuando el uso está por debajo del 80 % (después de una limpieza o una actualización de cuota).	Compre almacenamiento adicional o libere espacio de su almacenamiento en la nube.
Se ha superado la cuota de almacenamiento	La alerta se genera cuando se utiliza el 100% de la cuota de almacenamiento.	Compre más espacio de almacenamiento. Para obtener más información, consulte este artículo de la base de conocimientos.
Cuota de carga de trabajo alcanzada	La alerta se genera cuando el uso del artículo de oferta es superior a 0 y superior a la cuota, pero inferior o igual a la cuota más el exceso.	
Cuota de carga de trabajo superada	La alerta se genera cuando el uso del artículo de oferta es > cuota + exceso.	
La carga de trabajo no tiene ninguna cuota para aplicar un plan de copias de seguridad (el	La alerta se genera cuando: • La cuota se elimina manualmente: **Dispositivo** >	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
recurso no tiene cuotas de servicio)	**Detalles** > **Cuota de servicio**, haga clic en **Modificar** y seleccione la opción **Sin cuota**. • La opción **consola de administración** está desactivada. • El valor de cuota+exceso de la opción **Consola de administración** se ha reducido por debajo del uso actual.	
No se puede proteger una carga de trabajo con una cuota asignada	La alerta se genera cuando el artículo de oferta no es suficiente y necesita tener: • un grupo dinámico. • un plan de copias de seguridad asignado a dicho grupo. • Un recurso que se incluye en ese grupo dinámico, pero tiene algunas cualidades que prohíben aplicarle el mismo plan de copia de seguridad.	
La licencia de suscripción ha caducado	La alerta se genera cuando una licencia ha expirado.	Cuando una suscripción expira, toda la funcionalidad del producto, excepto la recuperación, se bloquea hasta que se renueva la suscripción. Los datos protegidos con copia de seguridad se mantienen accesibles para la recuperación. Compre una licencia nueva.

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		Nota Si recientemente ha comprado una nueva suscripción pero aún recibe el mensaje de que su suscripción ha caducado, importe la nueva suscripción desde la cuenta Acronis: en la consola de administración, vaya a **Configuración** -> **Licencias**, y luego en la esquina superior derecha, haga clic en **Sincronizar**. Las suscripciones se sincronizarán.
La licencia de suscripción caducará próximamente	La alerta se genera si una licencia va a caducar en menos de 30 días.	Compre una nueva suscripción.

Alertas de EDR

Tipo de alerta	Descripción	Cómo resolver la alerta
Incidente detectado	La alerta se genera cuando se crea un incidente o cuando se actualiza el estado de un incidente existente.	Esta alerta le informa sobre un nuevo incidente o un incidente antiguo que ha sido actualizado. Puede ver la alerta y cerrarla. Puede elegir abrir el incidente para una investigación más profunda.
Indicador de compromiso (IOC) detectado	La alerta se genera cuando se detecta un nuevo indicador de compromiso por el servicio de búsqueda de amenazas de IOC de EDR.	Esta alerta le informa de que se ha detectado un IOC en una o más cargas de trabajo. Cuando abra la alerta, podrá hacer clic en el enlace para ver los detalles del IOC.
Error al aislar la carga de trabajo de la red	La alerta se genera cuando el usuario activa la acción para aislar el equipo de la red y falla la acción de aislamiento.	Tome las medidas necesarias.
No se pudo volver a conectar la carga de trabajo a la red	La alerta se genera cuando el usuario activa la acción para volver a conectar el equipo a la red y falla la acción.	Tome las medidas necesarias.
Se han modificado los ajustes del	La alerta se genera cuando se	Esta alerta le informa de que se

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
cortafuegos de Windows Defender	modifica la configuración del cortafuegos en una máquina aislada.	han modificado los detalles del cortafuegos en el equipo aislado. Es una alerta meramente informativa y puede cerrarla cuando la haya visto.

Alertas de control de dispositivos

Tipo de alerta	Descripción	Cómo resolver la alerta
El control de dispositivos y la prevención de pérdida de datos se ejecutarán con una funcionalidad limitada (CPU incompatible detectada)	La alerta se genera cuando se inicia el agente DeviceLock en un equipo físico con CPU compatible con la tecnología CET.	Desactive la opción de las máquinas afectadas para evitar estas alertas.
La funcionalidad de control de dispositivos aún no es compatible con macOS Ventura	La alerta se genera cuando se inicia el agente DeviceLock en un equipo físico macOS Ventura y se aplica el plan de protección con el control de dispositivos al agente. Solo aplicable a versiones en las que hay un problema con el pánico de kernel debido al controlador de DeviceLock.	
Transferencia permitida de datos confidenciales	La alerta se genera si se permite la transferencia de contenido sensible.	
Transferencia justificada de datos confidenciales	La alerta se genera si se justifica la transferencia de contenido sensible.	
Transferencia denegada de datos confidenciales	La alerta se genera si se bloquea la transferencia de contenido sensible.	
Revisar los resultados del Modo de observación de la prevención de pérdida de datos	La alerta se genera cuando es hora de revisar los resultados de la observación: • No se ha aplicado la licencia del paquete Advanced DLP. • Ha pasado un mes desde que se habilitó el Modo de observación en cualquier plan de protección que se aplica a al menos una	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	carga de trabajo. • Ha pasado un mes desde que saltó una alerta similar y se ha detectado el uso de DLP en el Modo de observación.	
Se ha cambiado el identificador de seguridad del usuario	La alerta se genera cuando se actualiza un SID para un nombre de usuario conocido. Esto puede suceder cuando se reinstala el sistema operativo en una carga de trabajo que no pertenece a un dominio.	
El acceso al dispositivo periférico está bloqueado	La alerta se genera cuando se bloquean algunas acciones (operaciones de lectura/escritura) en dispositivos compatibles.	
No es posible conectar con un recurso SSL remoto.	La alerta se genera cuando el acceso a un recurso SSL remoto se bloquea debido a la prevención de negociación adicional utilizada en el recurso.	Añade el recurso a la lista de permitidos para hosts remotos.

Alertas del sistema

Tipo de alerta	Descripción	Cómo resolver la alerta
El agente está obsoleto	La alerta se genera cuando la versión del agente está obsoleta.	Vaya a la lista de agentes y actualice el agente.
Actualización automática fallida	La alerta se genera cuando la actualización automática del agente falla.	Intente realizar una actualización manual.
Debe reiniciar el dispositivo tras instalar un nuevo agente	La alerta se genera cuando se requiere un reinicio tras una correcta instalación remota.	Reinicie la carga de trabajo.
Debe reiniciar el dispositivo tras actualizar el agente	La alerta se genera cuando se requiere un reinicio tras una correcta instalación local.	Reinicie la carga de trabajo.
Fallo en la actividad	La alerta se genera cuando una actividad falla.	Reinicie todos los servicios de Acronis en la carga de trabajo.
La actividad se completó con	La alerta se genera cuando se	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
advertencias	completa una actividad, pero se generaron avisos.	
La actividad no responde	La alerta se genera cuando una actividad en progreso no está respondiendo.	
No se ha podido implementar el plan	La alerta se genera cuando falla la implementación del plan de protección.	
No se pudo convertir el nombre de usuario en SID	La alerta se genera cuando falla la conversión del SID de planificación.	
El equipo está sin conexión desde hace más de 20 días	Esta alerta se genera cuando no ha habido conexión a una carga de trabajo durante más de 20 días. Las copias de seguridad de la carga de trabajo se detendrán si la conexión no se restaura antes de que el estado offline alcance los 30 días.	
El equipo está sin conexión desde hace más de 30 días	Esta alerta se genera cuando no ha habido conexión a una carga de trabajo durante más de 30 días. Las copias de seguridad de la carga de trabajo se detienen. Para reanudar las copias de seguridad, restaure la conexión a la carga de trabajo.	
Se ha evitado la desinstalación o actualización del agente	Esta alerta se genera cuando el servicio de Active Protection detuvo un intento de desinstalación o actualización del agente de protección.	Haga clic en **Permitir durante 1 hora** para activar la operación.
Se ha detectado un conflicto relacionado con el plan de protección	Esta alerta se genera cuando hay un conflicto entre un plan de protección aplicado a una carga de trabajo y un plan de protección de un grupo dinámico.	
Se ha detectado un fallo de protección	Esta alerta se genera cuando algunos controladores en una carga de trabajo no están funcionando correctamente y el módulo de protección antivirus y antimalware está temporalmente	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	no disponible.	
No hay suficiente espacio en el disco	Esta alerta se genera cuando la instalación de un agente falló debido a espacio insuficiente en el disco de una carga de trabajo.	Libere algo de espacio en el disco y reinicie la instalación.
Se debe reiniciar para completar la instalación del agente	Esta alerta se genera cuando la instalación de un agente se completó con éxito y se requiere un reinicio para aplicar los cambios.	
No se puede iniciar la instalación del agente porque aún no se ha reiniciado el sistema operativo	Esta alerta se genera cuando la instalación de un agente no puede iniciarse porque la carga de trabajo está esperando un reinicio.	
La instalación del agente ha fallado porque aún no se ha reiniciado el sistema operativo	Esta alerta se genera cuando la instalación de un agente falló porque la carga de trabajo requiere un reinicio.	
Actualización automática fallida	Esta alerta se genera cuando una actualización automática del agente instalado en una carga de trabajo ha fallado y ahora está suspendida.	Actualice el agente manualmente.
Actualización automática interrumpida	Esta alerta se genera cuando la actualización automática a otra versión en una carga de trabajo ha fallado. El sistema intentará actualizar de nuevo automáticamente.	
El agente está fuera de línea	Esta alerta se genera cuando un plan programado no se ejecutó porque el agente estaba desconectado.	

Alertas de conexión a nubes públicas

Tipo de alerta	Descripción	Cómo resolver la alerta
Access to Azure subscription will expire soon	The alert is generated one month before the connection token for Azure subscription expires.	Vaya a **Infraestructura** > **Nubes públicas**,

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		seleccione la suscripción de Azure y luego haga clic en **Renovar acceso**.
Access to Azure subscription expired	La alerta se genera cuando el token de conexión para la suscripción de Azure expira.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego haga clic en **Renovar acceso**.
New version of agent for Azure is available	The alert is generated when there is a new version of Agent for Azure.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego haga clic en **Actualizar** para Agente para Azure.
The version of Agent for Azure will reach end of life soon	This alert is generated when a version of Agent for Azure will reach end of life after one release (monthly release).	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego haga clic en **Actualizar** para Agente para Azure.
The version of Agent for Azure has reached end of life	This alert is generated when a version of Agent for Azure has reached end of life.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego haga clic en **Actualizar** para Agente para Azure.
Agent for Azure configuration failed	This alert is generated when the Agent	Vaya a

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	for Azure configuration failed. Go to the **Activities** tab.	**Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego revise la pestaña **Actividades** para obtener detalles.
Agent for Azure is in status Failed	This alert is generated when the Agent for Azure is in status Failed. Check the status of the Azure virtual machine.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego revise la pestaña **Agente para Azure** para obtener detalles y el enlace al portal de Microsoft Azure para gestionar la máquina virtual.
Agent for Azure update failed	This alert is generated when the Agent for Azure update failed and the Agent for Azure version is reverted back to the previous version.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego revise la pestaña **Actividades** para obtener detalles.
Agent for Azure deletion failed	This alert is generated when the Agent for Azure was not deleted successfully.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y luego verifique la pestaña **Agente para Azure** para obtener detalles, para el enlace al portal de Microsoft Azure

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
		donde puede realizar la operación de eliminación de la máquina virtual, y para los grupos de recursos correspondientes.
Agent for Azure deallocation failed	Esta alerta se genera cuando un agente para Azure sin usar no fue eliminado.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la suscripción de Azure y verifique la pestaña **Agente para Azure** para obtener detalles, para un enlace al portal de Microsoft Azure donde puede realizar la operación de eliminación de la máquina virtual, y para los grupos de recursos correspondientes.
Access to S3 public cloud expiring	This alert is generated one month before the connection token for Amazon S3/Wasabi access expires.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la conexión de Amazon S3/Wasabi en la lista y luego haga clic en **Renovar acceso**.
Access to S3 public cloud expired	This alert is generated when the connection token for Amazon S3/Wasabi access expires.	Vaya a **Infraestructura** > **Nubes públicas**, seleccione la conexión de Amazon S3/Wasabi en la lista y luego haga clic en **Renovar acceso**.

© Acronis International GmbH, 2003-2025

Alertas de despliegue del software

Tipo de alerta	Descripción
Se ha detectado una incompatibilidad de paquetes de software	Esta es una alerta crítica que se genera cuando un paquete de software no se puede instalar porque no es compatible con el sistema operativo del recurso informático de destino.
Intentar instalar el software que falta	Esta es una alerta crítica que se genera cuando un plan de despliegue de software intenta instalar un paquete de software que no se encuentra en el repositorio.
Intentar desinstalar el software que falta	Esta es una alerta crítica que se genera cuando un plan de despliegue de software intenta desinstalar un paquete de software que no se encuentra en el repositorio.
Es necesario reiniciar el equipo después de la instalación del software	Esta es una alerta de aviso que se genera cuando la instalación del paquete de software requiere un reinicio del sistema operativo del recurso informático de destino.
Es necesario reiniciar el equipo después de la desinstalación del software	Esta es una alerta de aviso que se genera cuando la desinstalación del paquete de software requiere un reinicio del sistema operativo del destino del recurso informático.

Gestión

Tipo de alerta	Descripción
Reinicio pendiente	Esta alerta se genera cuando un dispositivo no se ha reiniciado durante 7 días después de un despliegue correcto del software.
El análisis de vulnerabilidades ha fallado	Este es un aviso de alerta que se genera cuando una evaluación de vulnerabilidades ha fallado debido a un error.
La instalación del parche ha fallado	Este es un aviso de alerta que se genera cuando una instalación de gestión de parches ha fallado debido a un error.
Se requiere reinicio de PM	Este es un aviso de alerta que se genera cuando se requiere un reinicio del sistema para completar el proceso de instalación del parche.
Conexión a escritorio remoto fallida	Esta alerta se genera cuando no se puede establecer conexión con una carga de trabajo remota debido a un error.
Faltan credenciales	Este es un aviso de alerta que se genera cuando un script no puede ejecutarse en una carga de trabajo debido a que faltan las credenciales para el script.
Ejecución de script fallida	Esta es una alerta crítica que se genera cuando:

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción
	• un script no puede ejecutarse porque tiene el estado "Borrador". • un script no está en el repositorio de scripts. • un script no puede ejecutarse porque no se pueden descargar sus dependencias. • un script tarda demasiado en ejecutarse en una carga de trabajo. • un script no puede ejecutarse en una carga de trabajo porque el ejecutor del script se desconectó.
Preferencias de firewall	Esta es una alerta de aviso que se genera cuando: • se ha modificado la configuración de Microsoft Defender. • la configuración de Microsoft Defender está bloqueada y no se puede cambiar debido a un error interno.
Reglas locales de firewall deshabilitadas	Esta es una alerta de aviso que se genera cuando las reglas locales para la gestión del firewall están deshabilitadas.
Paquete incompatible	Esta es una alerta crítica que se genera cuando un paquete de software no se puede instalar porque no es compatible con el sistema operativo de la carga de trabajo de destino.
Falta paquete de instalación	Esta es una alerta crítica que se genera cuando no se puede instalar el software porque este no se encuentra.
Falta paquete de desinstalación	Esta es una alerta crítica que se genera cuando no se puede desinstalar el software porque este no se encuentra.
Reinicio requerido para la instalación del paquete	Esta es una alerta de aviso que se genera cuando se requiere un reinicio para completar la instalación del software.
Reinicio requerido para la desinstalación del paquete	Esta es una alerta de aviso que se genera cuando se requiere un reinicio para completar la desinstalación del software.

Buscar

Tipo de alerta	Descripción	Cómo resolver la alerta
Falló la indexación de búsqueda	Esta alerta se genera cuando el índice no se pudo crear para el archivado de correo electrónico de Microsoft 365.	Intente actualizar o reconstruir el índice.
Fallo en la eliminación de elemento de búsqueda	Esta alerta se genera cuando un elemento no se pudo eliminar del archivo comprimido de correo	

© Acronis International GmbH, 2003-2025

Tipo de alerta	Descripción	Cómo resolver la alerta
	electrónico de Microsoft 365 debido a un error en las reglas de retención.	

Supervisión

Tipo de alerta	Descripción
Es posible que falle el disco	Esta es una alerta de aviso que se genera cuando es probable que un disco en una carga de trabajo falle en el futuro.
El fallo del disco es inminente	Esta es una alerta crítica que se genera cuando un disco en una carga de trabajo está en estado crítico y fallará pronto.
Error al recopilar los datos	Esta alerta se genera cuando el monitor no pudo recopilar datos para una carga de trabajo debido a un error.

Widgets de alertas

En los widgets de alertas, puede ver la siguiente información de alertas relacionada con su carga de trabajo:

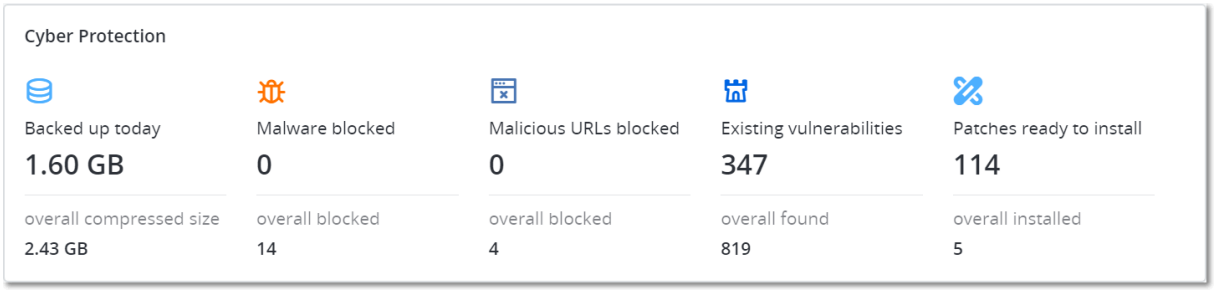
© Acronis International GmbH, 2003-2025

Campo	Descripción
widget de 5 últimas alertas	Una lista de las cinco últimas alertas.
Resumen de alertas histórico	Un widget gráfico que muestra las alertas por gravedad, tipo e intervalo de tiempo.
Resumen de alertas activas	Un widget gráfico que muestra las alertas activas por gravedad y tipo, así como la suma de alertas activas.
Historial de alertas	Una vista de tabla del historial de alertas.
Detalles de las alertas activas	Una vista de tabla de las alertas activas.

Cyber Protection

Este widget muestra información general sobre el tamaño de las copias de seguridad, el malware y las URL bloqueadas, las vulnerabilidades encontradas y los parches instalados.

Importante
Los valores del uso de almacenamiento que se muestran en la interfaz de usuario del producto están en unidades de bytes binarios: mebibyte (MiB), gibibyte (GiB) y tebibyte (TiB), aunque las etiquetas muestren MB, GB y TB, respectivamente. Por ejemplo, si el uso real es de 3105886629888 bytes, el valor que aparece en la interfaz de usuario se muestra correctamente como 2,82, pero se etiqueta con TB en lugar de TiB.



En la fila superior se muestran las estadísticas actuales:

- **Copia de seguridad realizada hoy**: la suma del tamaño de los puntos de recuperación de las últimas 24 horas.
- **Malware bloqueado**: el número de alertas activas actualmente relacionadas con malware bloqueado.
- **URL bloqueadas**: el número de alertas activas actualmente relacionadas con URL bloqueadas.
- **Vulnerabilidades existentes**: el número de vulnerabilidades que existen actualmente.
- **Parches listos para instalarse**: el número de parches disponibles actualmente para instalarse.

En la fila inferior se muestran las estadísticas globales:

© Acronis International GmbH, 2003-2025

- El tamaño comprimido de todas las copias de seguridad
- El número acumulado de elementos de malware bloqueados en todos los equipos
- El número acumulado de URL bloqueadas en todos los equipos
- El número acumulado de vulnerabilidades detectadas en todos los equipos
- El número acumulado de parches o actualizaciones instalados en todos los equipos

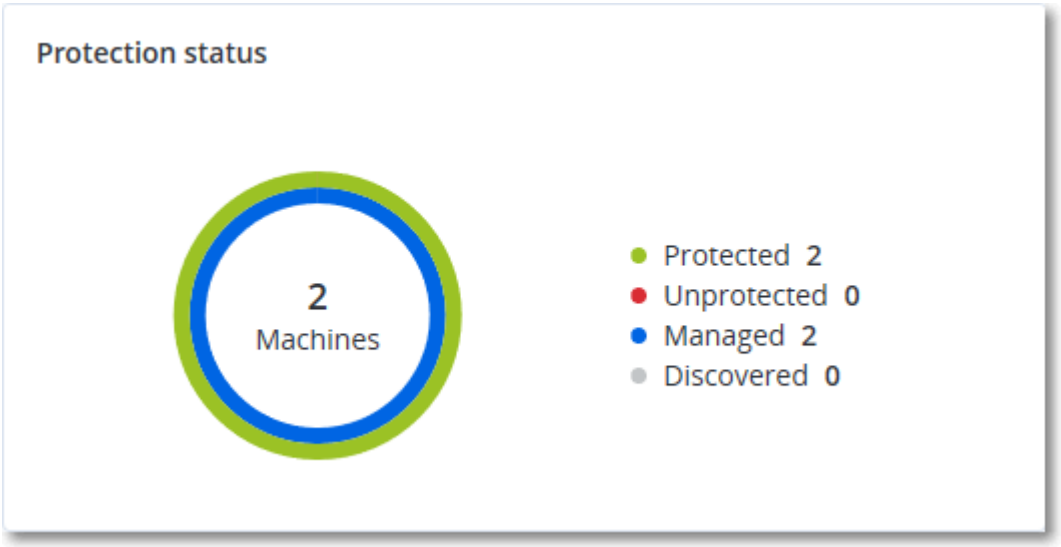
Estado de la protección

Este widget muestra el estado de protección actual de todos los equipos.

Un equipo puede encontrarse en uno de los siguientes estados:

- **Protegido**: equipos con un plan de protección aplicado.
- **Sin protección**: equipos sin un plan de protección aplicado. Incluyen tanto a los equipos detectados como a los gestionados en los que no hay ningún plan de protección aplicado.
- **Gestionado**: equipos en los que está instalado un agente de protección.
- **Detectado**: equipos en los que no está instalado un agente de protección.

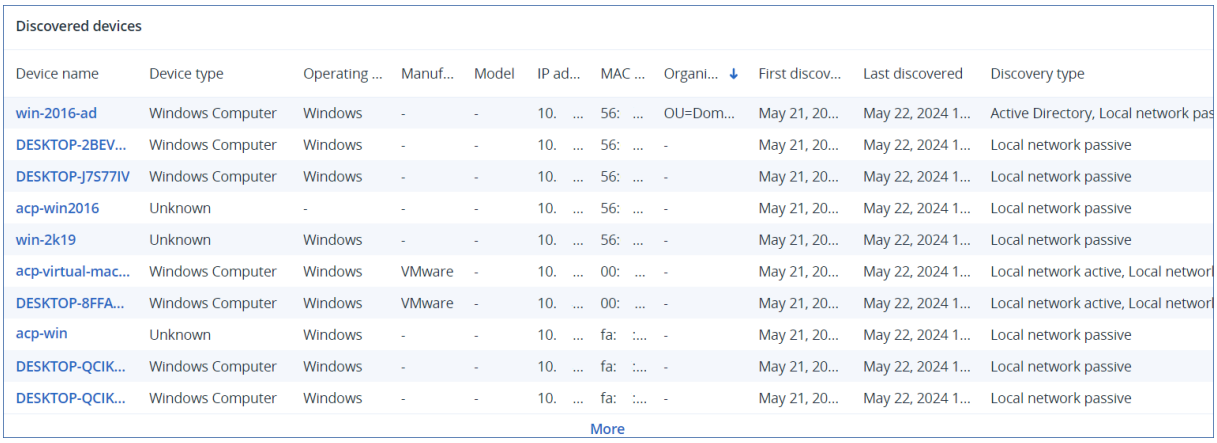
Si hace clic en el estado del equipo, se le redirigirá a la lista de equipos con este estado para que obtenga más información.



Dispositivos detectados

Este widget muestra información detallada acerca de los dispositivos que se detectaron en las redes de la organización.

© Acronis International GmbH, 2003-2025



Widgets de Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) incluye siete widgets a los que se puede acceder desde el panel de control **Información general**; tres de ellos también se muestran de forma predeterminada en la funcionalidad de EDR (consulte "Revisar incidentes" (p. 1258)).

Los siete widgets disponibles son los siguientes:

- Distribución de los principales incidentes por carga de trabajo
- Estado de la amenaza (mostrado en EDR)
- Historial de gravedad del incidente (mostrado en EDR)
- Tiempo medio de reparación de incidentes de seguridad
- Gráfico de quemado de incidentes de seguridad
- Detección por tácticas (mostrada en EDR)
- Estado de la red de las cargas de trabajo

Distribución de los principales incidentes por carga de trabajo

Este widget muestra las cinco cargas de trabajo con más incidentes (haga clic en **Mostrar todo** para volver a la lista de incidentes, que se filtra según los ajustes del widget).

Mantenga el ratón encima de la fila de una carga de trabajo para ver un desglose del estado actual de la investigación de los incidentes; los estados de la investigación son **Sin iniciar**, **Investigando**, **Cerrada** y **Falso positivo**. A continuación, haga clic en la carga de trabajo que desea analizar en profundidad. La lista de incidentes se actualiza según los ajustes del widget.

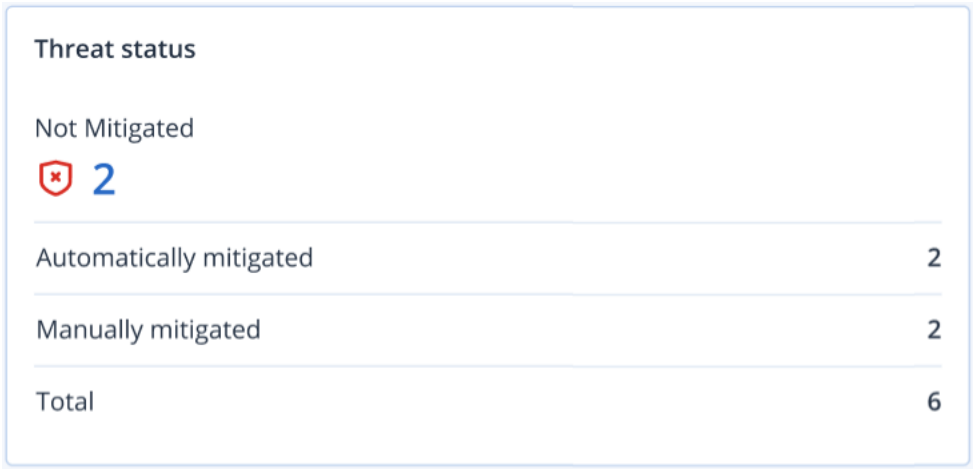
© Acronis International GmbH, 2003-2025



Estado de la amenaza

Este widget muestra el estado actual de la amenaza para todas las cargas de trabajo y destaca el número de incidentes que no se han mitigado y deben investigarse. El widget también indica el número de incidentes mitigados (de forma manual o automáticamente por el sistema).

Haga clic en el número **No mitigado** para filtrar la lista de incidentes de manera que se muestren aquellos que no se han mitigado.

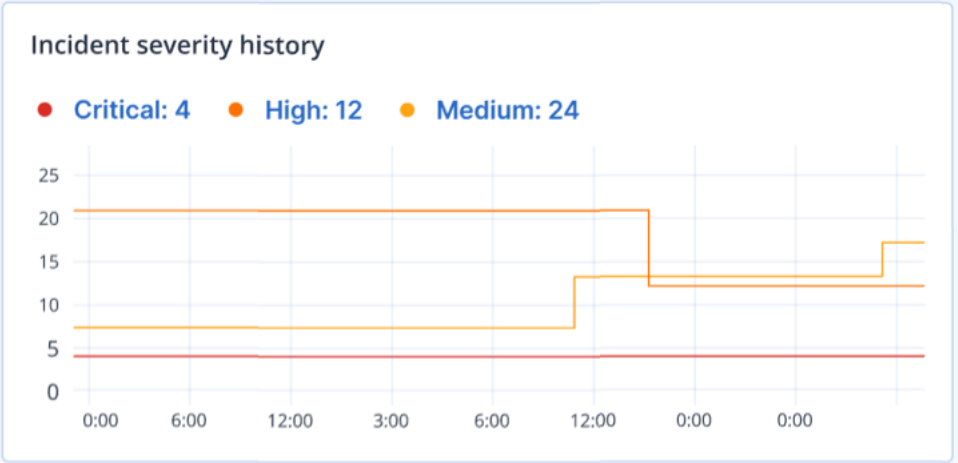


Historial de actividad del incidente

Este widget muestra la evolución de los ataques por gravedad y puede ayudarle a indicar las campañas de ataques. Cuando los picos son visibles, esto indica que la organización está siendo atacada.

Mantenga el ratón sobre el gráfico para ver un desglose del historial del incidente en un punto específico en las 24 horas previas (el periodo predeterminado). Haga clic en el nivel de gravedad (**Crítica**, **Alta** o **Media**) si desea ver una lista de incidentes relacionados; se le redirigirá a la lista de incidentes prefiltrada con los incidentes que coincidan con el nivel de gravedad seleccionado.

© Acronis International GmbH, 2003-2025



Tiempo medio de reparación de incidentes de seguridad

Este widget muestra el tiempo medio de reparación de incidentes de seguridad. Indica la rapidez con la que se investigan y reparan los incidentes.

Haga clic en una columna para ver un desglose de incidentes según la gravedad (**Crítica**, **Alta** y **Media**) y una indicación sobre cuánto tardan en repararse los distintos niveles de gravedad. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.

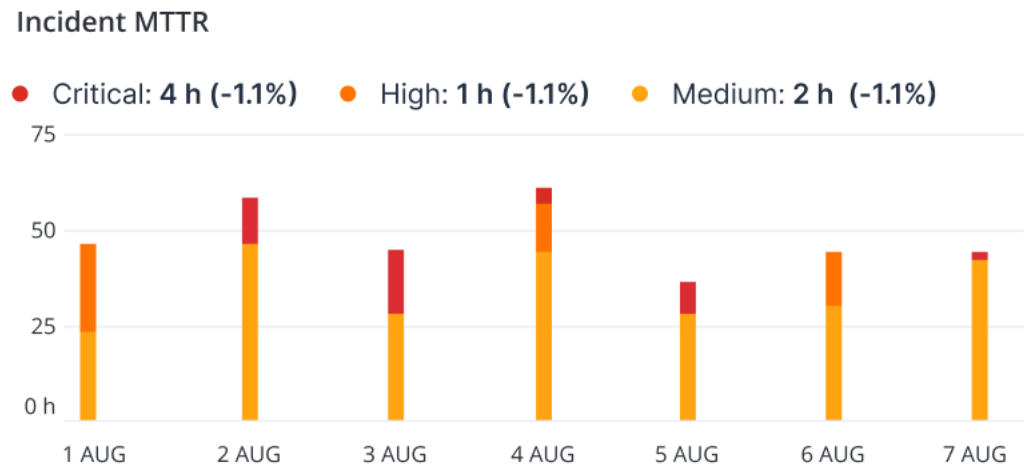


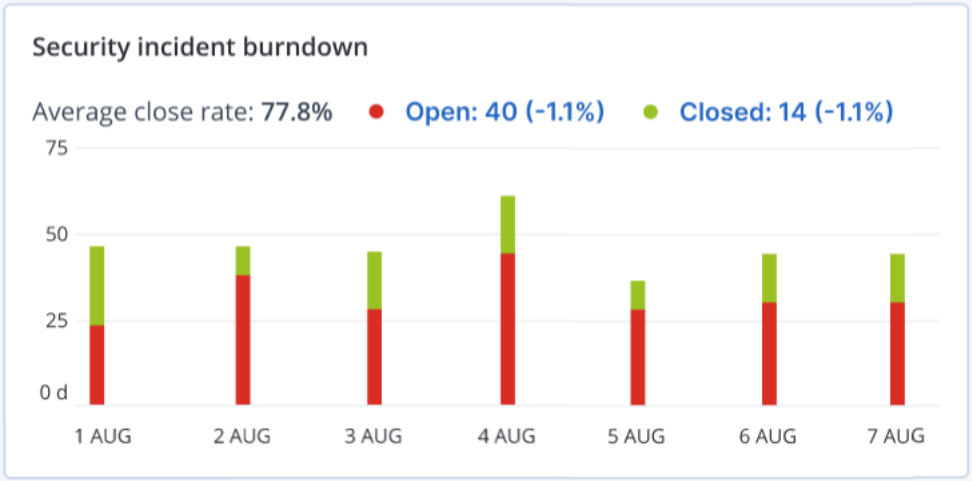
Gráfico de quemado de incidentes de seguridad

Este widget muestra la tasa de eficiencia de incidentes cerrados; el número de incidentes abiertos se mide comparado con el número de incidentes cerrados en un periodo de tiempo.

Mantenga el ratón encima de una columna para ver un desglose de los incidentes cerrados y abiertos del día seleccionado. Si hace clic en el valor Abierto, aparece una lista de incidentes filtrada para mostrar los incidentes abiertos actualmente (en los estados **Investigando** o **Sin iniciar**). Si hace clic en el valor Cerrado, se muestra la lista de incidentes filtrada para mostrar los incidentes que ya no están abiertos (en los estados **Cerrado** o **Falso positivo**).

© Acronis International GmbH, 2003-2025

El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.



Detección por tácticas

Este widget muestra el número de técnicas de ataque específicas que se han encontrado en los incidentes durante el periodo seleccionado.

Los valores en verde y rojo indican si el periodo de tiempo anterior ha aumentado o disminuido. En el siguiente ejemplo, los ataques de elevación de privilegios y comando y control han aumentado con respecto al periodo de tiempo anterior; esto podría indicar que sus necesidades de gestión de credenciales deben analizarse y la seguridad debe mejorar.



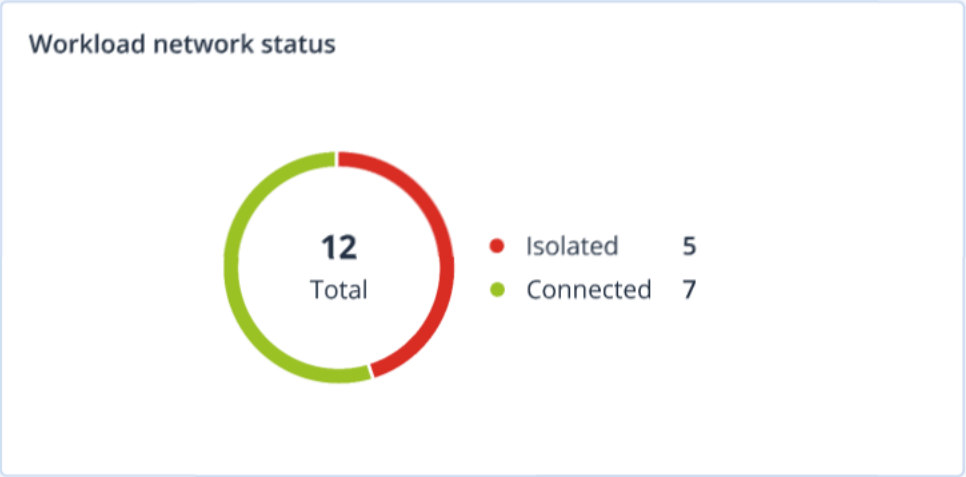
Estado de la red de las cargas de trabajo

Este widget muestra el estado de red actual de sus cargas de trabajo e indica cuántas están aisladas y cuántas conectadas.

Haga clic en el valor Aislada para ver la lista Cargas de trabajo con agentes (en el menú **Cargas de trabajo** de la consola de Cyber Protect), que está filtrada para mostrar las cargas de trabajo

© Acronis International GmbH, 2003-2025

aisladas. Haga clic en el valor Conectada para ver la Carga de trabajo con la lista de agentes filtrada para mostrar las cargas de trabajo conectadas.



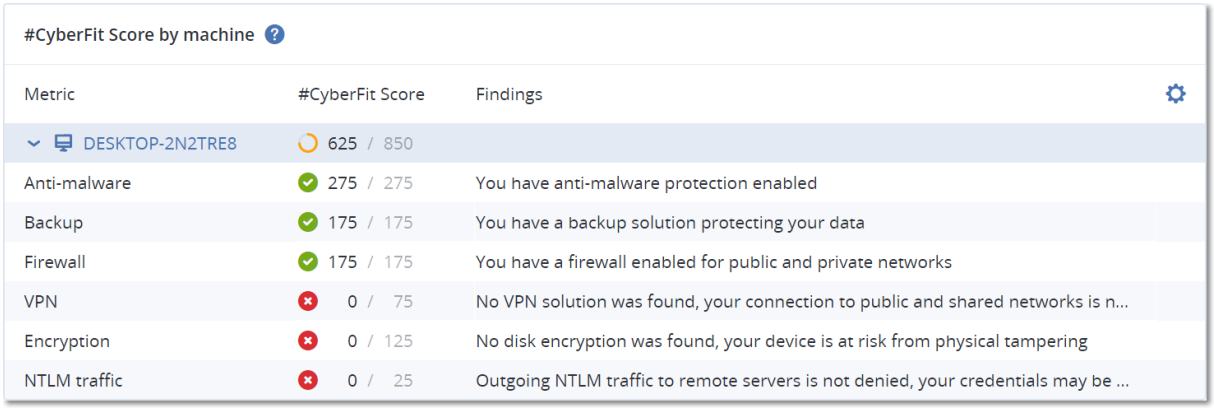
#CyberFit Score por equipo

Este widget muestra para cada equipo el #CyberFit Score total, las puntuaciones que lo componen e información sobre cada uno de los parámetros evaluados:

- Antimalware
- Copia de seguridad
- Cortafuegos
- VPN
- Cifrado
- Tráfico NTLM

Para mejorar la puntuación de cada parámetro, puede consultar las recomendaciones disponibles en el informe.

Para obtener más información sobre #CyberFit Score, consulte "#CyberFit Score para equipos".



© Acronis International GmbH, 2003-2025

Supervisión del estado del disco

La supervisión del estado del disco proporciona información sobre el estado actual del disco y una previsión para que pueda evitar una pérdida de datos que pueda estar relacionada con un fallo del disco. Son compatibles tanto los discos duros como los SSD.

Limitaciones

- La previsión del estado del disco solo se puede realizar en equipos Windows.
- Únicamente se supervisan los discos de equipos físicos. Los discos de máquinas virtuales no se pueden supervisar ni aparecen en los widgets sobre el estado del disco.
- No se admiten configuraciones RAID. Los widgets de estado del disco no incluyen ninguna información sobre los equipos con implementación RAID.
- Las unidades SSD NVMe no son compatibles.
- No se admiten los dispositivos de almacenamiento externos.

El estado del disco puede ser uno de los siguientes:

- **OK**:
  El estado del disco se encuentra entre el 70 y el 100 %.
- **Advertencia**:
  El estado del disco se encuentra entre el 30 y el 70 %.
- **Crítico**:
  El estado del disco se encuentra entre el 0 y el 30 %.
- **Calculando datos del disco**:
  Se están calculando tanto el estado del disco actual como su previsión.

Cómo funciona

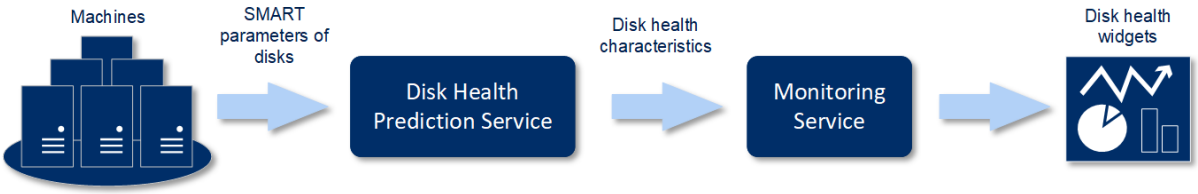
El servicio de predicción de estado del disco utiliza un modelo de predicción basado en la inteligencia artificial.

1. El agente de protección recopila los parámetros SMART de los discos y envía estos datos al servicio de predicción de estado del disco:
   - SMART 5: Número de sectores reasignados.
   - SMART 9: Horas durante las que está encendido.
   - SMART 187: Errores incorregibles de los que se ha informado.
   - SMART 188: Comando de tiempo de espera.
   - SMART 197: Número de sectores pendientes actuales.
   - SMART 198: Número de sectores incorregibles fuera de línea.
   - SMART 200: Tasa de error de escritura.

© Acronis International GmbH, 2003-2025

2. El servicio de previsión de estado de disco procesa los parámetros SMART recibidos, realiza predicciones y proporciona las siguientes características del estado del disco:
   - Estado actual del disco: OK, Advertencia, Crítico.
   - Previsión del estado del disco: negativa, estable, positiva.
   - Probabilidad de la previsión del estado del disco en porcentaje.

   El periodo de predicción es de un mes.
3. El servicio de supervisión recibe estas características y muestra la información relevante en los widgets del estado del disco en la consola de Cyber Protect.



Widgets sobre el estado del disco

Los resultados de la supervisión del estado del disco se muestran en los siguientes widgets que están disponibles en la consola de Cyber Protect.

- **Resumen del estado del disco**: Es un widget en estructura de árbol con dos niveles de datos que se pueden cambiar al desplazarse.
  - Nivel de equipo:
    Muestra información resumida sobre el estado del disco de los equipos de los clientes seleccionados. Solo se muestra el estado del disco más crítico. El resto de los estados aparecen en la información sobre herramientas cuando se pasa el ratón por encima de un bloque concreto. El tamaño del bloque del equipo depende del tamaño total de todos los discos del equipo. El color del bloque del equipo depende del estado del disco más crítico encontrado.

© Acronis International GmbH, 2003-2025



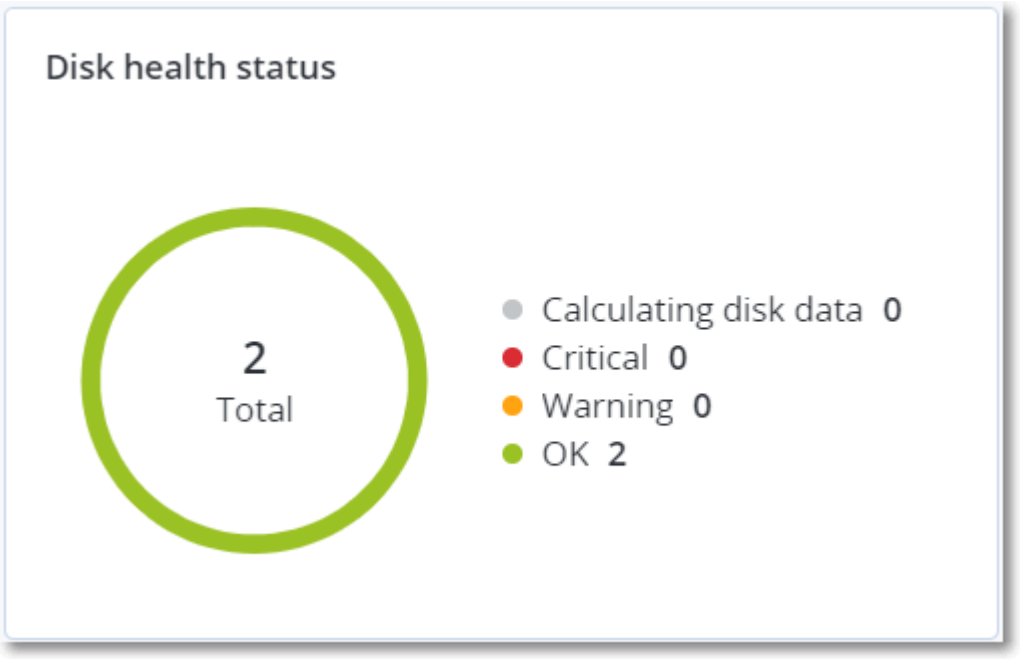
- Nivel de disco:
  Muestra el estado actual de todos los discos para el equipo seleccionado. Cada bloque de discos muestra el porcentaje de una de las siguientes previsiones del estado del disco y su probabilidad:
  - Se degradará
  - Permanecerá estable

© Acronis International GmbH, 2003-2025

- Mejorará



- **Estado del disco**: Es un widget con gráfico circular en el que se muestra el número de discos de cada estado.



© Acronis International GmbH, 2003-2025

Alertas sobre el estado del disco

La comprobación del estado del disco se ejecuta cada 30 minutos, pero la alerta correspondiente se genera una vez al día. Cuando el estado del disco cambia de **Advertencia** a **Crítico**, se genera siempre una alerta.

Nombre de la alerta	Gravedad	Estado del disco	Descripción
Es posible que falle el disco	Advertencia	(30 – 70)	Es probable que el disco <disk name> en este equipo falle en el futuro. Ejecute lo antes posible una copia de seguridad de imágenes completa de este disco, reemplácelo y, a continuación, recupere la imagen en el nuevo disco.
El fallo del disco es inminente	Crítico	(0 – 30)	El disco <disk name> en este equipo está en estado crítico y es muy probable que falle pronto. En este punto, no le recomendamos realizar una copia de seguridad de imágenes de este disco, ya que la carga añadida podría hacer que el disco falle. Realice inmediatamente una copia de seguridad de los archivos más importantes de este disco y reemplácelo.

Mapa de protección de datos

Nota
Esta función está disponible con el paquete Advanced Backup.

Gracias a la función del mapa de protección de datos, puede descubrir todos los datos que sean importantes para usted y obtener información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes en una vista escalable representada con una estructura de árbol.

El tamaño de cada bloque depende del tamaño o el número total de archivos importantes que pertenecen a un cliente o un equipo.

Los archivos pueden tener uno de los siguientes estados de protección:

- **Crítico**: hay entre un 51 y un 100 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Bajo**: hay entre un 21 y un 50 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la

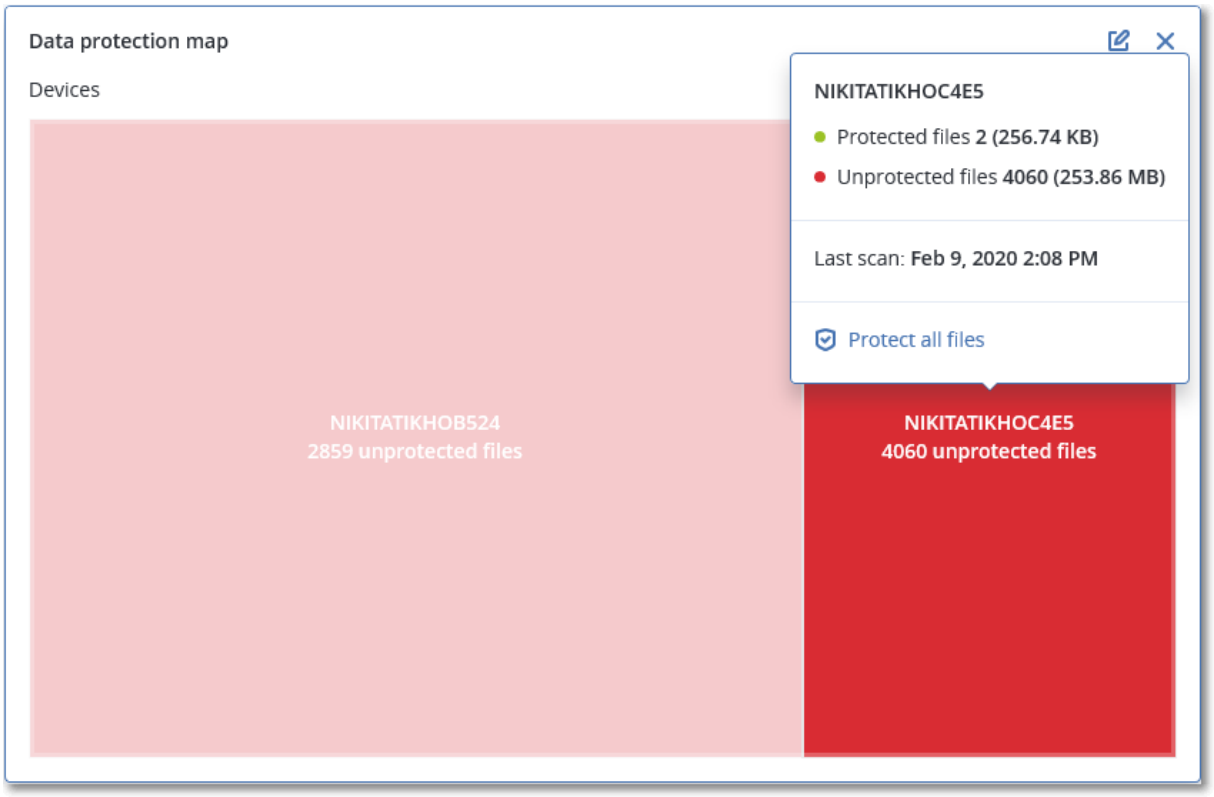
© Acronis International GmbH, 2003-2025

configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.

- **Medio**: hay entre un 1 y un 20 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Alto**: todos los archivos con las extensiones que ha especificado están protegidos (se ha realizado una copia de seguridad de ellos) para la ubicación o el equipo seleccionado.

Los resultados de la evaluación de la protección de datos se encuentran en el panel de control de supervisión en el widget del mapa de protección de datos, un widget en estructura de árbol en el que se muestra información sobre el nivel de un equipo.

- Nivel de equipo: muestra información sobre el estado de protección de archivos importantes según los equipos del cliente seleccionado.



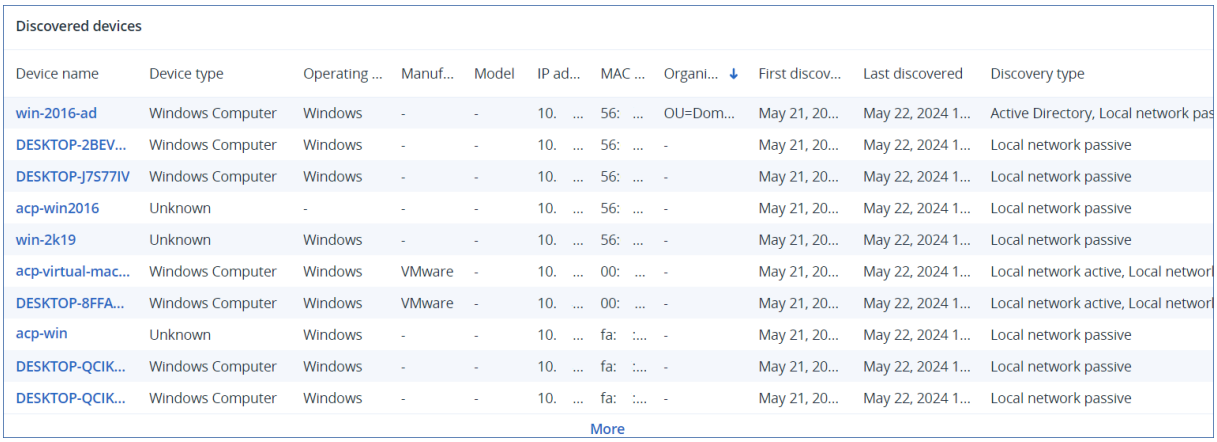
Para proteger los archivos que no estén protegidos, pase el ratón por encima del bloque y haga clic en **Proteger todos los archivos**. En la ventana de diálogo encontrará información sobre el número de archivos que no están protegidos y su ubicación. Para protegerlos, haga clic en **Proteger todos los archivos**.

También puede descargar un informe detallado en formato CSV.

© Acronis International GmbH, 2003-2025

Widget de dispositivos detectados

El widget de tabla **Dispositivos detectados** muestra información detallada acerca de los dispositivos de las redes de la organización que se detectaron mediante el análisis activo y pasivo. La información del dispositivo incluye el tipo de dispositivo, el fabricante, el sistema operativo, la dirección IP, la dirección MAC, la fecha de detección, etc.


Discovered devices

Device name	Device type	Operating ...	Manuf...	Model	IP ad...	MAC ...	Organi...	First discov...	Last discovered	Discovery type
win-2016-ad	Windows Computer	Windows	-	-	10. ...	56: ...	OU=Dom...	May 21, 20...	May 22, 2024 1...	Active Directory, Local network pas
DESKTOP-2BEV...	Windows Computer	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-J7S77IV	Windows Computer	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
acp-win2016	Unknown	-	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
win-2k19	Unknown	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
acp-virtual-mac...	Windows Computer	Windows	VMware	-	10. ...	00: ...	-	May 21, 20...	May 22, 2024 1...	Local network active, Local networ
DESKTOP-8FFA...	Windows Computer	Windows	VMware	-	10. ...	00: ...	-	May 21, 20...	May 22, 2024 1...	Local network active, Local networ
acp-win	Unknown	Windows	-	-	10. ...	fa: :...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-QCIK...	Windows Computer	Windows	-	-	10. ...	fa: :...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-QCIK...	Windows Computer	Windows	-	-	10. ...	fa: :...	-	May 21, 20...	May 22, 2024 1...	Local network passive

More

Widgets de evaluación de vulnerabilidades

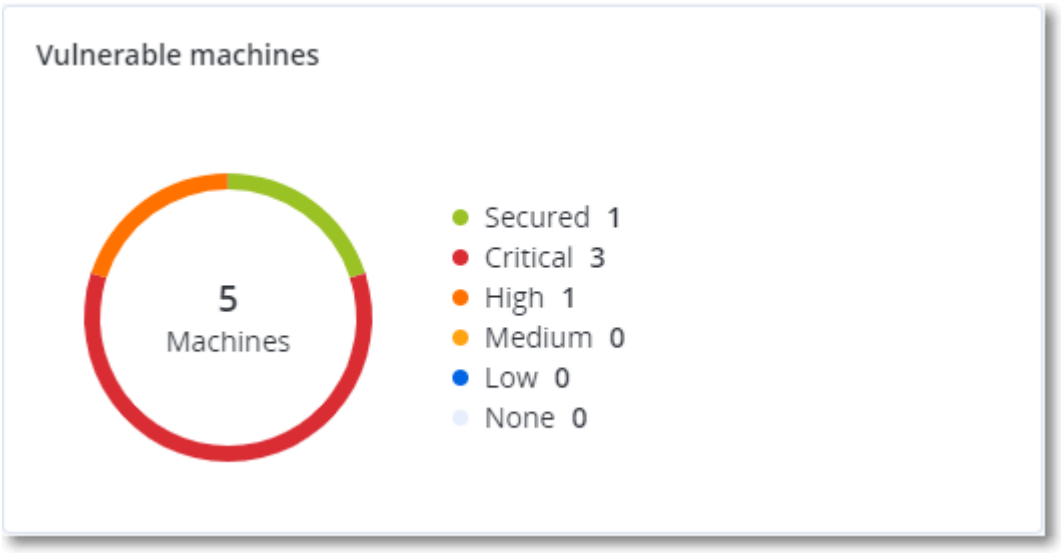
Equipos vulnerables

Este widget muestra los equipos vulnerables por gravedad de la vulnerabilidad.

La vulnerabilidad encontrada tendrá uno de los siguientes niveles de gravedad de acuerdo con el sistema Common Vulnerability Scoring System (CVSS) v3.0:

- Protegido: no se ha encontrado ninguna vulnerabilidad
- Crítico: 9,0-10,0 CVSS
- Alto: 7,0-8,9 CVSS
- Medio: 4,0-6,9 CVSS
- Bajo: 0,1-3,9 CVSS
- Ninguno: 0,0 CVSS

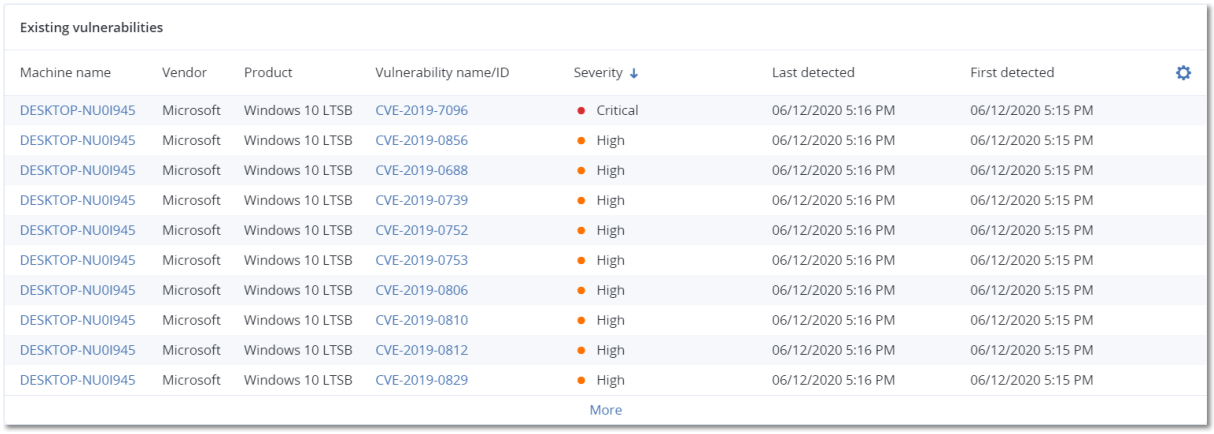
© Acronis International GmbH, 2003-2025



Vulnerabilidades existentes

Este widget muestra las vulnerabilidades que existen actualmente en los equipos. En el widget **Vulnerabilidades existentes**, hay dos columnas en las que se muestran determinadas marcas de hora y fecha:

- **Primera detección**: fecha y hora en que se detectó por primera vez una vulnerabilidad en el equipo.
- **Última detección**: fecha y hora en que se detectó por última vez una vulnerabilidad en el equipo.



Widgets de instalación de parches

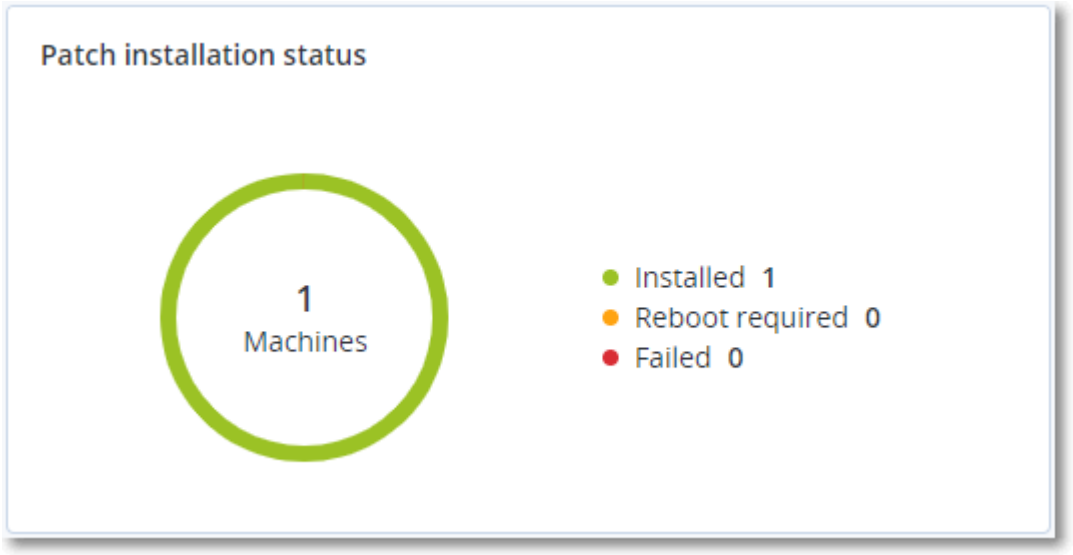
Hay cuatro widgets relacionados con la funcionalidad de gestión de parches.

Estado de instalación del parche

Este widget muestra el número de equipos agrupados por estado de instalación de parches.

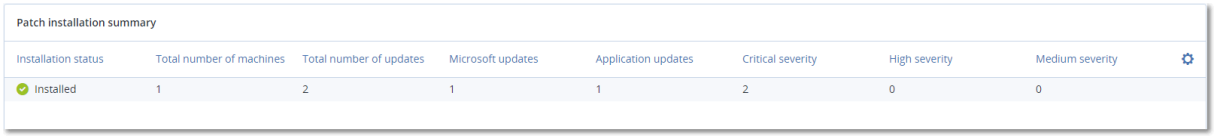
© Acronis International GmbH, 2003-2025

- **Instalado**: todos los parches disponibles están instalados en el equipo.
- **Reinicio necesario**: después de la instalación de un parche, es necesario reiniciar el equipo.
- **Fallida**: la instalación del parche ha fallado en el equipo.



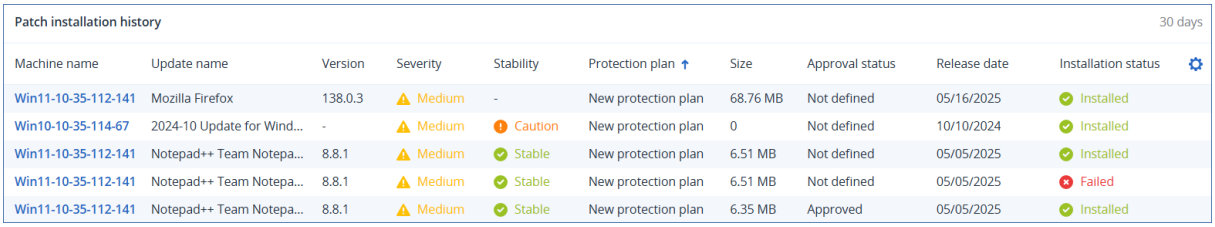
Resumen de la instalación del parche

Este widget muestra el resumen de parches que hay en los equipos por estado de instalación de parches.



Historial de instalación de parches

Este widget muestra información detallada sobre los parches que hay en los equipos.



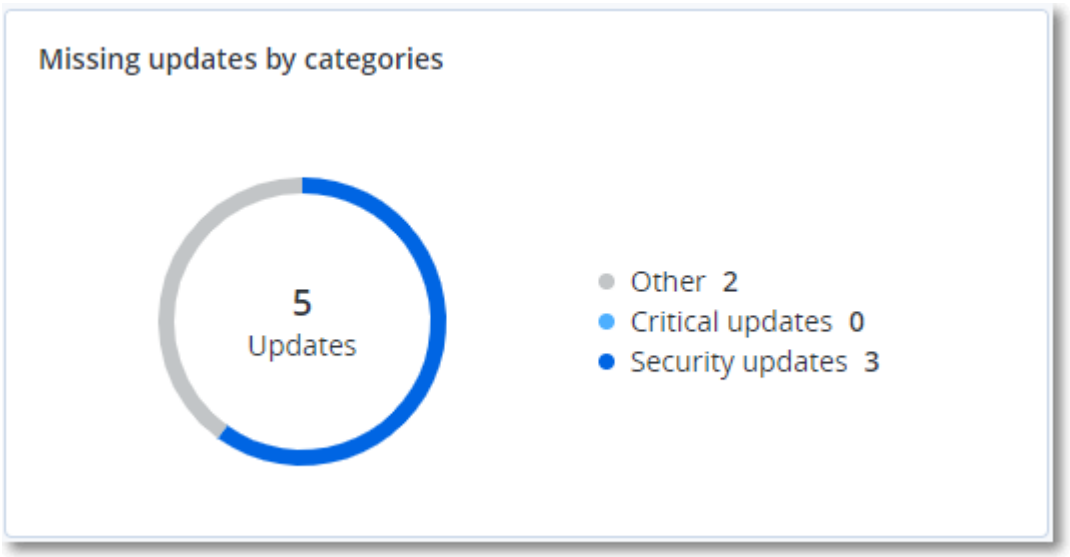
Actualizaciones que faltan por categoría

Este widget muestra el número de actualizaciones que faltan por categoría. Se muestran las siguientes categorías:

- Actualizaciones de seguridad
- Actualizaciones críticas

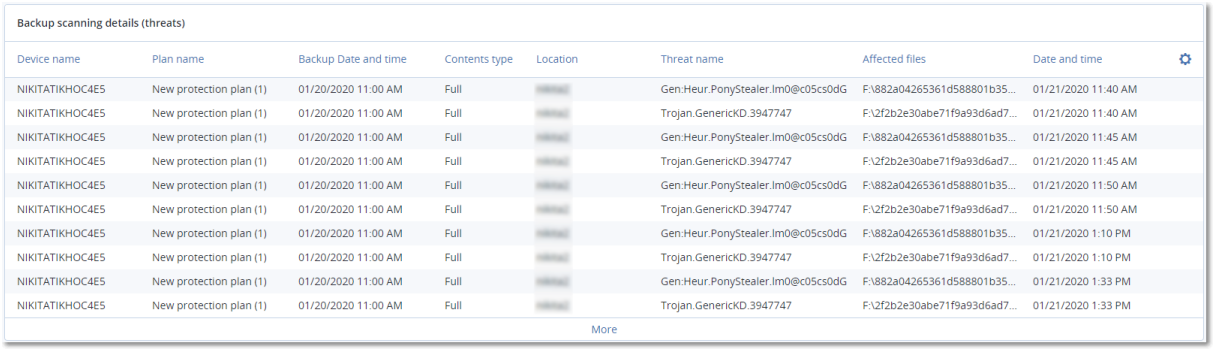
© Acronis International GmbH, 2003-2025

- Otros



Detalles del análisis de copias de seguridad

Este widget muestra información detallada sobre las amenazas detectadas en las copias de seguridad.


Backup scanning details (threats)

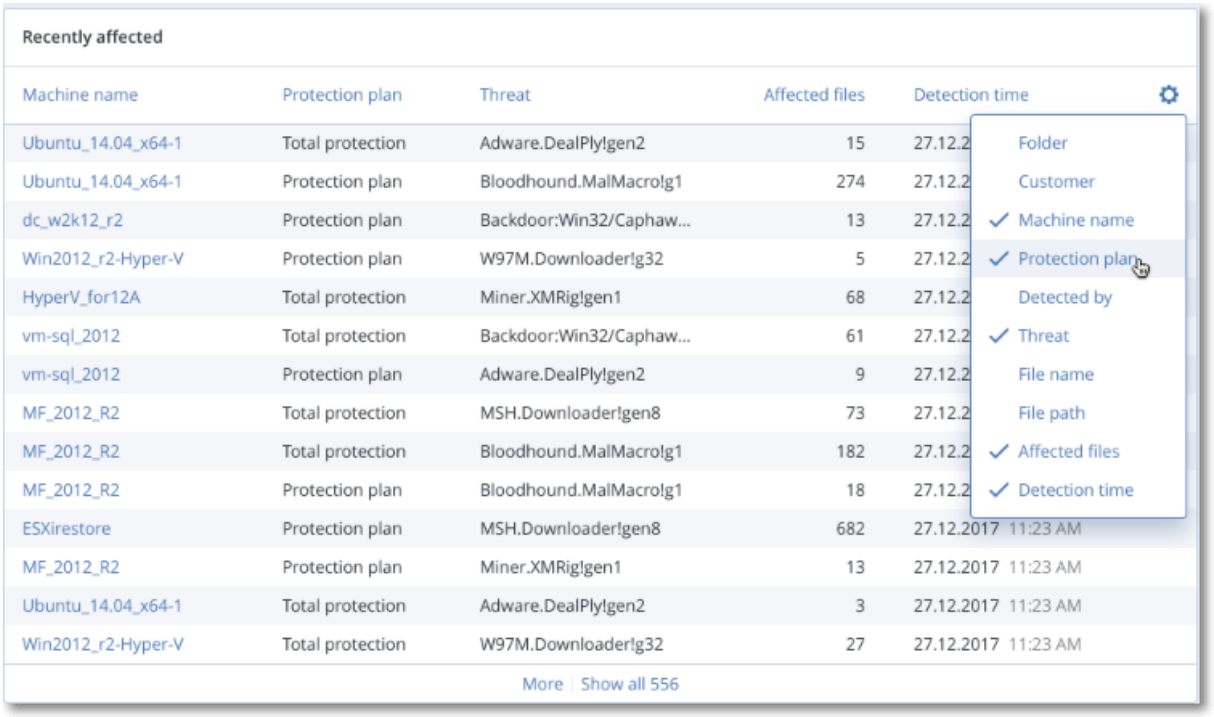
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

Elementos afectados recientemente

Este widget muestra información detallada sobre las cargas de trabajo que se han visto afectadas por amenazas como virus, malware y ransomware. Puede encontrar información sobre las amenazas detectadas, la hora a la que se detectaron y el número de archivos que se vieron afectados.

© Acronis International GmbH, 2003-2025



Descargar datos de cargas de trabajo afectadas recientemente

Puede descargar los datos de las cargas de trabajo que se han visto afectadas, generar un archivo CSV y enviarlo a los destinatarios que especifique.

Para descargar los datos de las cargas de trabajo que se han visto afectadas, siga los siguientes pasos:

1. En el widget **Elementos afectados recientemente**, haga clic en **Descargar datos**.
2. En el campo **Período**, introduzca el número de días de los cuales desee descargar datos. Solo puede indicar 200 días como máximo.
3. En el campo **Destinatarios**, introduzca las direcciones de correo electrónico de todas las personas que recibirán un mensaje con un enlace para descargar el archivo CSV.
4. Haga clic en **Descargar**.

   El sistema empezará a generar el archivo CSV con los datos de las cargas de trabajo que se han visto afectadas en el período de tiempo que ha especificado. Cuando el archivo CSV se haya creado, el sistema enviará un correo electrónico a los destinatarios. Entonces, cada destinatario podrá descargar el archivo CSV.

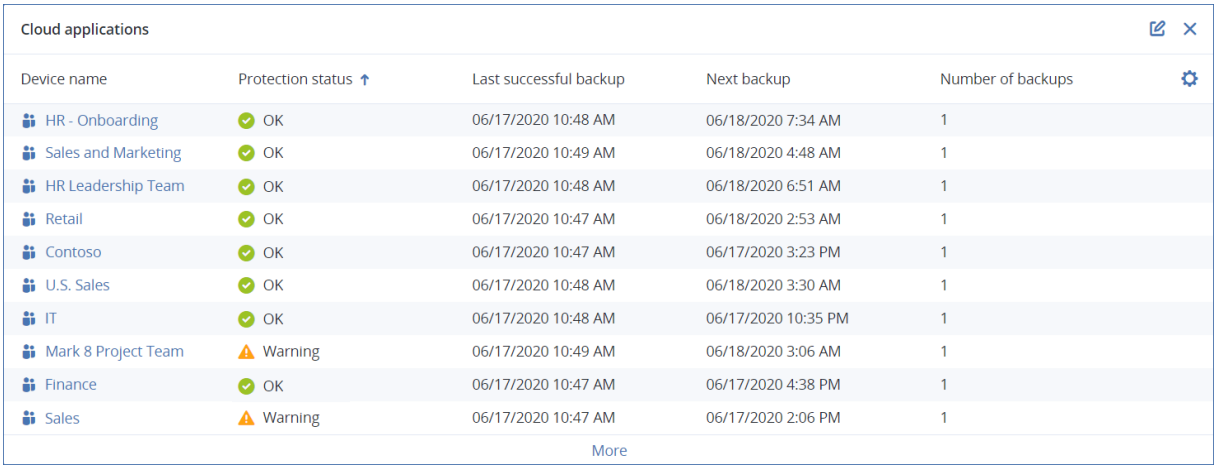
Aplicaciones de Cloud

Este widget muestra información detallada sobre los recursos nube a nube:

- Usuarios de Microsoft 365 (buzón de correo, OneDrive)
- Grupos de Microsoft 365 (buzón de correo, sitio del grupo)
- Carpetas públicas de Microsoft 365

© Acronis International GmbH, 2003-2025

- Colecciones de sitios de Microsoft 365
- Equipos de Microsoft 365
- Usuarios de Google Workspace (Gmail, Google Drive)
- Unidades compartidas de Google Workspace



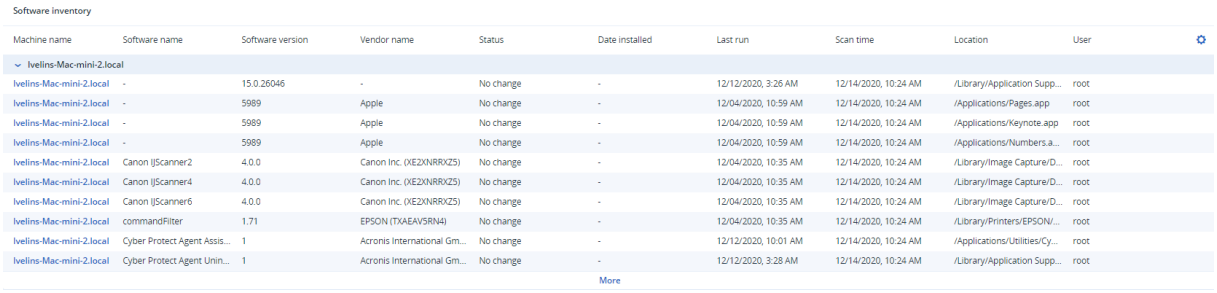
También hay información adicional acerca de los recursos nube a nube en los siguientes widgets:

- Actividades
- Lista de actividades
- 5 últimas alertas
- Historial de alertas
- Resumen de alertas histórico
- Resumen del historial de alertas
- Detalles de las alertas activas
- Resumen de ubicaciones

Widgets de software

Widgets de inventario de software

El widget de tabla de **Inventario de software** muestra información detallada sobre todo el software que se ha instalado en dispositivos de Windows y macOS de su organización.

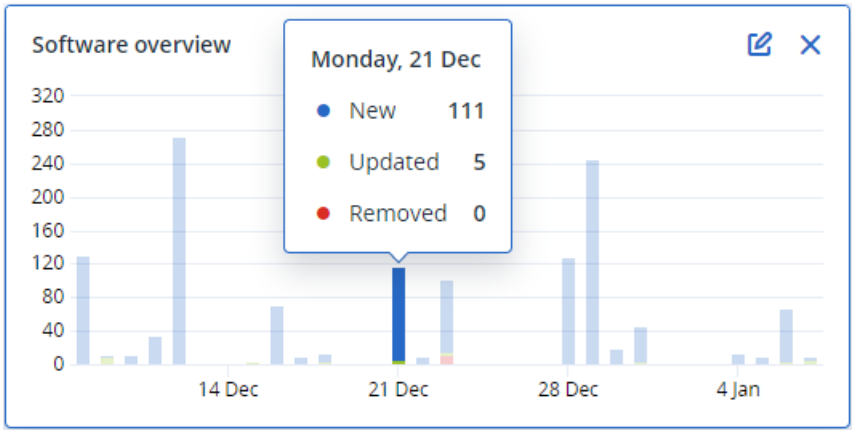


© Acronis International GmbH, 2003-2025

Puede filtrar la información en el widget por nombre de máquina, nombre de software, nombre de proveedor y estado.

Nota
En los filtros **Nombre de la máquina**, **Nombre del software** y **Nombre del proveedor**, puede seleccionar hasta 20 valores.

El widget de **información general del software** muestra el número de aplicaciones nuevas, actualizadas y eliminadas en dispositivos de Windows y macOS en su organización durante un período específico de tiempo (7 días, 30 días o el mes en curso).



Cuando pase el ratón sobre determinada barra del gráfico, aparecerá la siguiente información sobre la herramienta:

Nuevas: el número de aplicaciones instaladas recientemente.

Actualizadas: el número de aplicaciones actualizadas.

Eliminadas: el número de aplicaciones eliminadas.

Cuando haga clic en la parte de la barra correspondiente a determinado estado, se le redirigirá a la página **Gestión del software** -> **Inventario del software**. La información que aparece en esa página está filtrada de acuerdo con la fecha y el estado correspondientes.

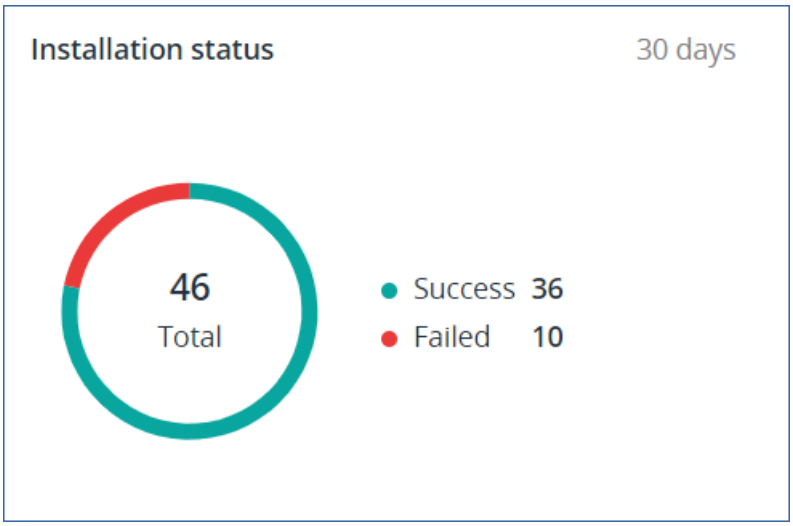
Puede filtrar la información en el widget por nombre de dispositivo.

Nota
En el filtro **Nombre del dispositivo**, puede seleccionar hasta 20 valores.

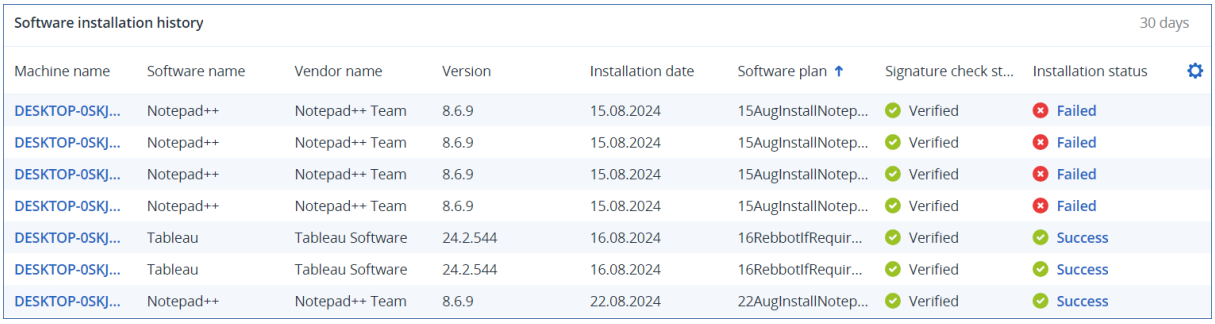
Widgets de instalación de software

El widget **Estado de la instalación** muestra el número total de actividades de instalación, agrupadas por estado. Al hacer clic en un segmento del gráfico circular, se redirige a la página **Actividades**, donde solo se muestran las actividades con el estado correspondiente, ordenadas cronológicamente.

© Acronis International GmbH, 2003-2025



El widget **Historial de instalación de software** proporciona información detallada sobre el estado de las instalaciones remotas de software en sus dispositivos gestionados. Al hacer clic en un estado en la columna **Estado de la instalación**, se redirige a la página **Actividades**, donde se muestran las actividades con el estado correspondiente en orden cronológico.

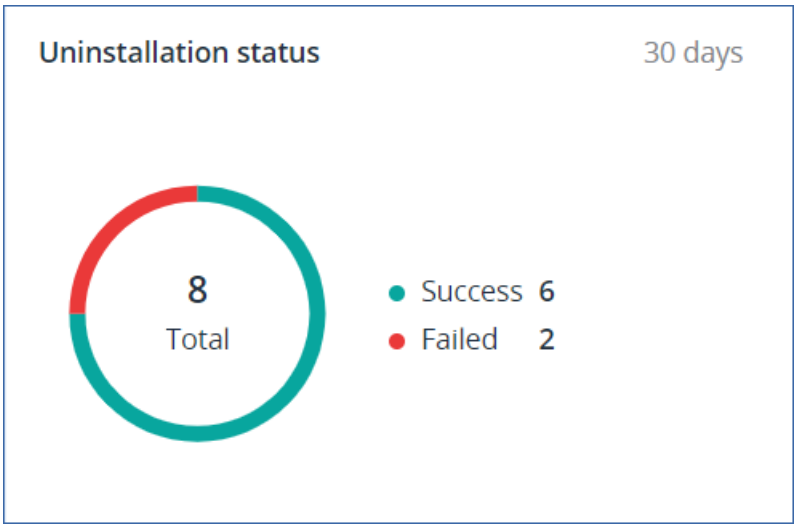

Software installation history — 30 days

Machine name	Software name	Vendor name	Version	Installation date	Software plan	Signature check st...	Installation status
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Tableau	Tableau Software	24.2.544	16.08.2024	16RebbotIfRequir...	Verified	Success
DESKTOP-0SKJ...	Tableau	Tableau Software	24.2.544	16.08.2024	16RebbotIfRequir...	Verified	Success
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	22.08.2024	22AugInstallNotep...	Verified	Success

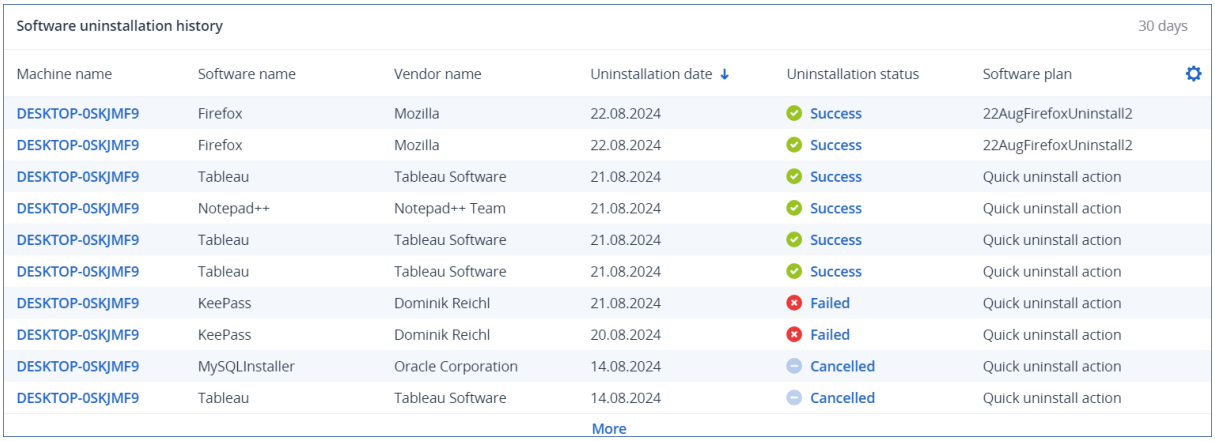
Widgets de desinstalación de software

El widget **Estado de la desinstalación** muestra el número total de actividades de desinstalación, agrupadas por estado. Al hacer clic en un segmento del gráfico circular, se redirige a la página **Actividades**, donde solo se muestran las actividades con el estado correspondiente, ordenadas cronológicamente.

© Acronis International GmbH, 2003-2025



El widget **Historial de desinstalación de software** proporciona información detallada del estado de las desinstalaciones de software remotas en sus dispositivos gestionados. Al hacer clic en un estado en la columna **Estado de desinstalación**, se redirige a la página **Actividades**, donde se muestran las actividades con el estado correspondiente en orden cronológico.


Software uninstallation history — 30 days

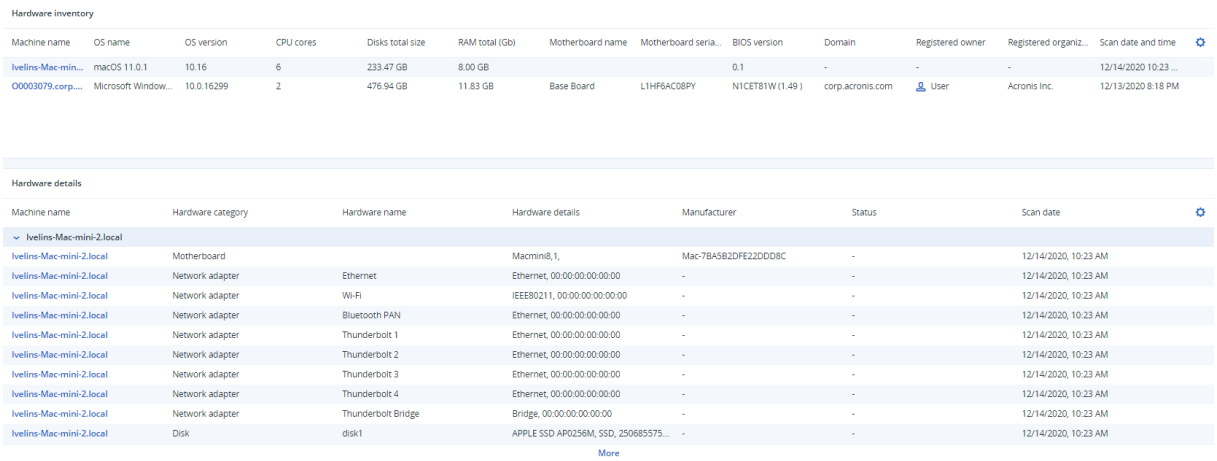
Machine name	Software name	Vendor name	Uninstallation date ↓	Uninstallation status	Software plan
DESKTOP-0SKJMF9	Firefox	Mozilla	22.08.2024	Success	22AugFirefoxUninstall2
DESKTOP-0SKJMF9	Firefox	Mozilla	22.08.2024	Success	22AugFirefoxUninstall2
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Notepad++	Notepad++ Team	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	KeePass	Dominik Reichl	21.08.2024	Failed	Quick uninstall action
DESKTOP-0SKJMF9	KeePass	Dominik Reichl	20.08.2024	Failed	Quick uninstall action
DESKTOP-0SKJMF9	MySQLInstaller	Oracle Corporation	14.08.2024	Cancelled	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	14.08.2024	Cancelled	Quick uninstall action

More

Widgets de inventario de hardware

Los widgets de tablas de **inventario de hardware** y de **detalles de hardware** muestran información sobre todo el hardware instalado en dispositivos físicos y virtuales de Windows y macOS en su organización.

© Acronis International GmbH, 2003-2025



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

El widget de tabla de **cambios de hardware** muestra información sobre el hardware que se ha añadido, eliminado y cambiado en dispositivos físicos y virtuales de Windows y macOS en su organización durante un período específico de tiempo (7 días, 30 días o el mes en curso).



Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Puede filtrar los resultados que se muestran en los widgets de inventario de hardware.

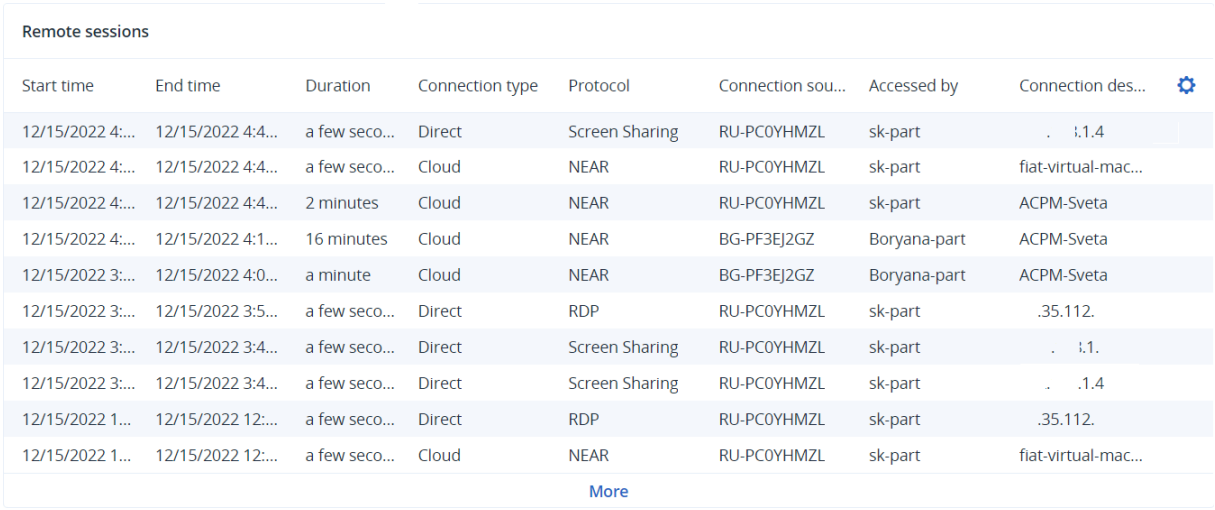
Nota

En el filtro **Nombre de la máquina**, puede seleccionar hasta 20 valores.

Widget de sesiones remotas

Este widget muestra la información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos.

© Acronis International GmbH, 2003-2025


Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

Protección inteligente

Fuente de amenazas

El centro de operaciones de ciberprotección (CPOC) de Acronis genera alertas de seguridad que se envían únicamente a las regiones geográficas relacionadas. Estas alertas de seguridad proporcionan información sobre malware, vulnerabilidades, desastres naturales, salud pública y otros tipos de acontecimientos globales que puedan afectar a la protección de sus datos. El registro de amenazas le informa sobre todas las posibles amenazas para que pueda evitarlas.

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Algunas alertas de seguridad se pueden resolver con las acciones específicas que indican los expertos en seguridad. Otras alertas de seguridad solo le informan sobre las próximas amenazas, pero no hay acciones recomendadas disponibles.

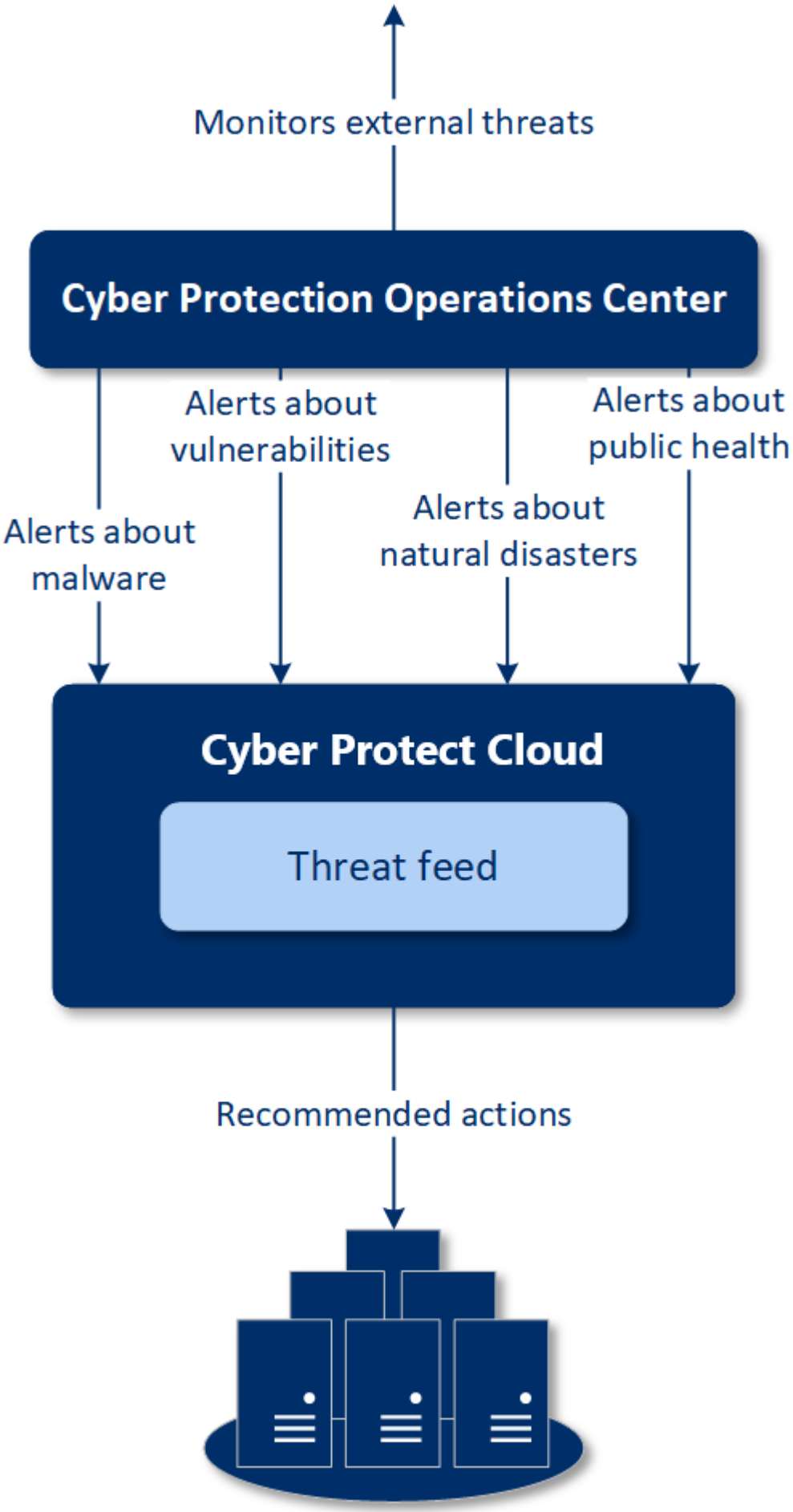
Nota
Las alertas de malware se generan solo en los equipos que tienen instalado el agente para la protección antimalware y el filtrado de URL.

Cómo funciona

El centro de operaciones de ciberprotección (CPOC) de Acronis supervisa las amenazas externas y genera alertas sobre amenazas relacionadas con malware, vulnerabilidades, desastres naturales y salud pública. Podrá ver todas estas alertas en la consola de Cyber Protect, en la sección **Fuente de amenazas**. Puede realizar las acciones recomendadas respectivas en función del tipo de alerta.

El principal flujo de trabajo de la fuente de amenazas está representado en el siguiente diagrama.

© Acronis International GmbH, 2003-2025



© Acronis International GmbH, 2003-2025

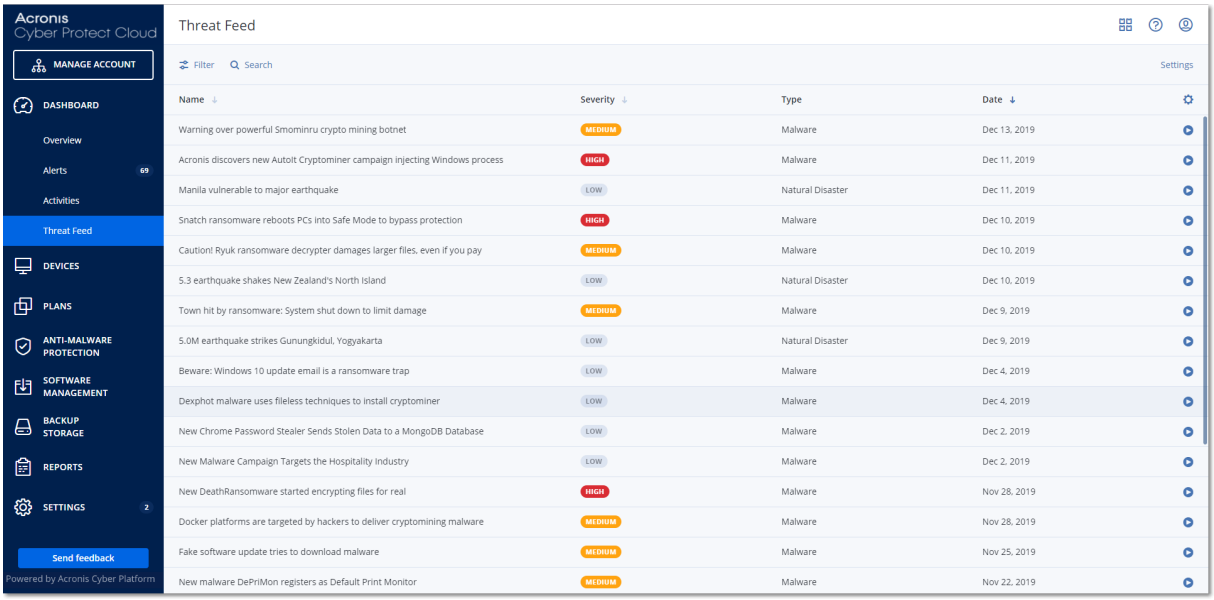
Para ejecutar las acciones de solución de amenazas recomendadas según las alertas recibidas del centro de operaciones de ciberprotección de Acronis, lleve a cabo las siguientes acciones:

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Fuente de información sobre amenazas** para comprobar si hay alguna alerta de seguridad existente.
2. Seleccione una alerta de la lista y revise la información proporcionada.
3. Haga clic en **Iniciar** para iniciar el asistente.
4. Habilite las acciones que quiera llevar a cabo y los equipos en los que se deben aplicar. Es posible que se sugieran las siguientes opciones:
   - **Evaluación de vulnerabilidades**: su función es analizar los equipos de búsqueda de vulnerabilidades.
   - **Gestión de parches**: sirve para instalar parches en los equipos seleccionados.
   - **Protección antimalware**: su función es ejecutar un análisis completo de los equipos seleccionados.

     Nota
     Esta acción está disponible solo en las máquinas que tienen instalado el agente para la protección antimalware.

   - **Copia de seguridad de equipos protegidos o no protegidos**: sirve para realizar copias de seguridad de cargas de trabajo protegidas o no protegidas.
     Si todavía no hay copias de seguridad para la carga de trabajo (en todas las ubicaciones accesibles, en sitios locales y en la nube) o las copias de seguridad existentes están cifradas, el sistema crea una copia de seguridad completa con el siguiente formato de nombre:
     `%workload_name%-Remediation`
     El destino predeterminado de la copia de seguridad es el almacenamiento Cyber Protect Cloud, pero puede configurar otra ubicación antes de empezar la operación.
     Si ya existe una copia de seguridad no cifrada, el sistema creará una copia de seguridad incremental en el archivo comprimido existente.
5. Haga clic en **Iniciar**.
6. En la página **Actividades**, verifique que la actividad se haya realizado correctamente.

© Acronis International GmbH, 2003-2025



Eliminación de todas las alertas

La limpieza automática del registro de amenazas se lleva a cabo cuando transcurren los siguientes periodos:

- Desastre natural: 1 semana
- Vulnerabilidad: 1 mes
- Malware: 1 mes
- Salud pública: 1 semana

Mapa de protección de datos

Con el mapa de protección de datos puede:

- Recibir información detallada sobre los datos almacenados (clasificación, ubicaciones, estado de protección y otro tipo de información adicional) en sus cargas de trabajo.
- Comprobar si los datos están protegidos. Se considera que los datos están protegidos si se aplica un plan de protección con el módulo de copia de seguridad habilitado a la carga de trabajo.
- Llevar a cabo acciones para proteger los datos.

Cómo funciona

1. Primero, cree un plan de protección con el módulo Mapa de protección de datos habilitado.
2. A continuación, cuando se haya ejecutado el plan y sus datos se hayan detectado y analizado, obtendrá la representación visual de la protección de datos en el widget Mapa de protección de datos.
3. Otra opción es que vaya a **Dispositivos** > **Mapa de protección de datos** y busque allí información sobre los archivos que no estén protegidos por dispositivo.

© Acronis International GmbH, 2003-2025

4. Puede realizar acciones para proteger los archivos detectados como no protegidos en los dispositivos.

Gestión de los archivos detectados que no tienen protección

Para proteger los archivos importantes detectados como no protegidos, lleve a cabo las siguientes acciones:

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Mapa de protección de datos**.
   En la lista de dispositivos, puede encontrar información general sobre el número de archivos sin protección, el tamaño de los archivos por dispositivo y la última detección de datos.
   Para proteger los archivos de un equipo en concreto, haga clic en el icono de puntos suspensivos y luego en **Proteger todos los archivos**. Se le dirigirá a la lista de planes en la que puede crear un plan de protección con el módulo de copia de seguridad habilitado.
   Para eliminar el dispositivo concreto en el que se encuentran los archivos sin protección de la lista, haga clic en **Ocultar hasta la próxima detección de datos**.
2. Para obtener información más detallada sobre los archivos sin protección de un dispositivo concreto, haga clic en el nombre del dispositivo.
   Verá el número de archivos sin protección por extensión y ubicación. Defina las extensiones en el campo de búsqueda para las que quiera tener información sobre los archivos sin protección.
3. Para proteger todos los archivos que no estén protegidos, haga clic en **Proteger todos los archivos**. Se le dirigirá a la lista de planes en la que puede crear un plan de protección con el módulo de copia de seguridad habilitado.

Para obtener un informe con información sobre los archivos que no están protegidos, haga clic en **Descargar informe detallado en CSV**.

Ajustes del mapa de protección de datos

Para obtener más información sobre cómo crear un plan de protección con el módulo Mapa de protección de datos, consulte "Creación de un plan de protección".

Para el módulo Mapa de protección de datos se pueden especificar los siguientes ajustes:

Planificación

Puede definir diferentes configuraciones para crear la planificación en función de la tarea que se vaya a realizar para el mapa de protección de datos.

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma

© Acronis International GmbH, 2003-2025

Campo	Descripción
	predeterminada, la tarea se iniciará cuando cualquier usuario inicie sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario cierre sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación. • **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes: • **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.

© Acronis International GmbH, 2003-2025

Campo	Descripción
Especifique una cuenta de usuario que al cerrar sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo** • **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.

Extensiones y reglas de excepción

En la pestaña **Extensiones**, puede definir la lista de extensiones de archivo que se considerarán importantes durante la detección de datos y comprobar si están protegidas. Para definir extensiones, utilice el siguiente formato:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

En la pestaña **Reglas de excepción**, puede seleccionar qué archivos y carpetas no hay que comprobar en el estado de protección durante la detección de datos.

© Acronis International GmbH, 2003-2025

- **Archivos y carpetas ocultos**: si esta opción está seleccionada, los archivos y carpetas ocultos se omitirán durante el análisis de los datos.
- **Archivos y carpetas del sistema**: si esta opción está seleccionada, los archivos y carpetas del sistema se omitirán durante el análisis de los datos.

La pestaña Actividades

La pestaña **Actividades** proporciona información general de las actividades de los últimos 90 días.

Pasos para filtrar actividades en el panel de control

1. En el campo **Nombre de dispositivo**, especifique el equipo en el que se lleva a cabo la actividad.
2. En la lista desplegable **Estado**, seleccione el estado. Por ejemplo, completada, con errores, en progreso o cancelada.
3. En la lista desplegable **Acciones remotas**, seleccione la acción. Por ejemplo, aplicar plan, eliminar copias de seguridad o instalar actualizaciones de software.
4. En el campo **Más reciente**, establezca el periodo de actividades. Por ejemplo, las actividades más recientes, las actividades de las últimas 24 horas, o las actividades durante un periodo específico de tiempo dentro de los últimos 90 días.
5. Si accede a la pestaña **Actividades** como administrador de partner, podrá filtrar las actividades para un cliente específico que gestione.

Para personalizar la vista de la pestaña **Actividades**, haga clic en el icono de engranaje y seleccione las columnas que desea ver. Para ver el progreso de la actividad en tiempo real, seleccione la casilla de verificación **Actualizar automáticamente**.

Para cancelar la ejecución de una actividad, haga clic en el nombre y, a continuación, en la pantalla **Detalles**, haga clic en **Cancelar**.

Puede buscar las actividades enumeradas a través de los siguientes criterios:

- Nombre de dispositivo
  El equipo en el que se lleva a cabo la actividad.
- Iniciado por
  La cuenta que inició la actividad.

Las actividades del escritorio remoto se pueden filtrar por las siguientes propiedades:

- Crear plan
- Aplicando plan
- Revocando plan
- Plan de eliminación
- Conexión remota
  - Conexión a escritorio remoto de la nube a través de RDP
  - Conexión a escritorio remoto de la nube a través de NEAR

© Acronis International GmbH, 2003-2025

  - Conexión a escritorio remoto de la nube a través del Uso compartido de pantalla de Apple
  - Conexión a escritorio remoto a través del cliente web
  - Conexión a escritorio remoto a través de Asistencia rápida
  - Conexión a escritorio remoto directa a través de RDP
  - Conexión a escritorio remoto directa a través del Uso compartido de pantalla de Apple
  - Transferencia de archivos
  - Transferencia de archivos a través de Asistencia rápida
- Acción remota
  - Apagar una carga de trabajo
  - Reiniciar una carga de trabajo
  - Cerrar sesión del usuario remoto en la carga de trabajo
  - Vaciar la papelera de reciclaje para el usuario en la carga de trabajo
  - Suspender una carga de trabajo

Cyber Protect Monitor

Puede instalar Cyber Protect Monitor como un componente adicional que selecciona durante la instalación del Agente para Windows o Agente para Mac. Cyber Protect Monitor muestra información sobre el estado de protección del equipo en el que está instalado el Agente para Windows o Agente para Mac.

Puede usar Cyber Protect Monitor para configurar el cifrado de las copias de seguridad y la configuración del servidor proxy, así como para chatear con técnicos.

Cyber Protect Monitor es compatible con los siguientes sistemas operativos.

- Con Agente para Windows
  - Windows 10 versión 1809 y posteriores
  - Windows Server 2019 y versiones posteriores
- Con el agente para Windows (heredado)
  - Windows 7 y posterior
  - Windows Server 2008 R2 y posterior
- Con Agente para Mac
  - Todas las versiones de macOS compatibles con Agent for Mac, excepto macOS 10.x.

Cuando el agente para File Sync & Share está instalado en el equipo, Cyber Protect Monitor proporciona acceso al servicio de File Sync & Share. La funcionalidad de File Sync & Share es accesible después de un proceso de integración obligatorio durante el cual los usuarios inician sesión en su propia cuenta de File Sync & Share y seleccionan una carpeta de sincronización

© Acronis International GmbH, 2003-2025

personal. Para obtener más información sobre el agente para File Sync & Share, consulte la guía de usuario Cyber Files Cloud.

Importante
Cyber Protect Monitor está accesible para los usuarios que podrían no tener derechos administrativos para el servicio Cyber Protection o File Sync & Share.

La tabla siguiente resume las operaciones que están disponibles para los usuarios sin derechos administrativos.

Agentes instalados	Los usuarios pueden	Los usuarios no pueden
Agente para Windows o agente para Mac	• Aplique el plan de protección predeterminado a sus equipos • Comprobar el estado de protección de sus equipos • Reciba notificaciones de Active Protection • Pausar temporalmente las copias de seguridad de sus equipos • Configure los ajustes del servidor proxy • Cambie la configuración de cifrado de la copia de seguridad **Advertencia.** Al cambiar la configuración de cifrado en Cyber Protect Monitor, se sobrescribe la configuración en el plan de protección y afecta a todas las copias de seguridad del equipo. Esta operación puede hacer que algunos planes de protección fallen. Para obtener más información, consulte "Cifrado" (p. 583). No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña. • Chatear con un técnico	• Aplique planes de protección personalizados • Gestione planes de protección que ya están aplicados
Agente para Windows (heredado)	• Aplique el plan de protección predeterminado a sus equipos • Comprobar el estado de protección de sus equipos • Reciba notificaciones de Active	• Aplique planes de protección personalizados • Gestione planes de protección que ya están aplicados

© Acronis International GmbH, 2003-2025

Agentes instalados	Los usuarios pueden	Los usuarios no pueden
	Protection • Pausar temporalmente las copias de seguridad de sus equipos • Configure los ajustes del servidor proxy • Cambie la configuración de cifrado de la copia de seguridad **Advertencia.** Al cambiar la configuración de cifrado en Cyber Protect Monitor, se sobrescribe la configuración en el plan de protección y afecta a todas las copias de seguridad del equipo. Esta operación puede hacer que algunos planes de protección fallen. Para obtener más información, consulte "Cifrado" (p. 583). No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.	
Agente para Windows y agente para Sync and Share Agente para Mac y agente para Sync and Share	• Sincronizar contenido entre su carpeta de sincronización local y su cuenta de File Sync & Share • Pause las operaciones de sincronización • Cambie la carpeta de sincronización • Verifique los tipos de archivos que no se pueden sincronizar • Chatear con un técnico	• Edite los tipos de archivos que no se pueden sincronizar

Configuración del servidor proxy en Cyber Protect Monitor

Puede configurar el servidor proxy en Cyber Protect Monitor. La configuración afectará a todos los agentes que están instalados en el equipo.

Pasos para configurar el servidor proxy

1. Abra Cyber Protect Monitor y, a continuación, haga clic en el icono de engranaje de la esquina superior derecha.
2. Haga clic en **Configuración** y después en **Proxy**.
3. Habilite el conmutador **Utilizar servidor proxy** y, a continuación, escriba la dirección y el puerto del servidor proxy.

© Acronis International GmbH, 2003-2025

4. [Si el acceso al servidor proxy está protegido con contraseña] Habilite el conmutador **Se necesita la contraseña** y, a continuación, escriba el nombre de usuario y la contraseña para acceder al servidor proxy.
   La contraseña puede incluir caracteres alfanuméricos en minúsculas y mayúsculas, y los siguientes caracteres especiales:
   ```
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` } | { ~
   ```
5. Haga clic en **Guardar**.
   La configuración del servidor proxy se guarda en el archivo `http-proxy.yaml`.

Chats en el Monitor

Desde su dispositivo, puede chatear con técnicos o administradores en la consola de Cyber Protect. De esta forma, puede recibir asistencia en tiempo real con los problemas.

Iniciar un chat en Cyber Protect Monitor

Puede utilizar Cyber Protect Monitor para chatear con técnicos del inquilino en el que está registrado su carga de trabajo en la consola de Cyber Protect. Puede iniciar una nueva sesión de chat o puede responder en sesiones de chat que se hayan iniciado en la consola. El Monitor muestra notificaciones de escritorio cuando tiene nuevos mensajes en el chat.

Para iniciar una nueva sesión de chat desde el Monitor

1. Abra Cyber Protect Monitor.
2. Haga clic en el icono de chat.
   Se abre una ventana de chat.
3. En el campo de texto, escriba su mensaje.
4. Para enviar el mensaje, haga clic en el icono de flecha o pulse Intro.
   Su mensaje se envía a la consola de Cyber Protect. La sesión del chat se asignará a un técnico o administrador que le ayudará.

Nota
Las sesiones de chat se cierran automáticamente si un usuario está inactivo durante 15 minutos.

Acciones adicionales con chats en Cyber Protect Monitor

Si tiene una sesión de chat activa en Cyber Protect Monitor, puede realizar las siguientes acciones: editar mensaje, eliminar mensaje, buscar una palabra clave o mensaje, o finalizar el chat.

Editar mensaje

Puede editar cualquier mensaje que haya enviado en la sesión de chat.

Para editar un mensaje en la sesión de chat

© Acronis International GmbH, 2003-2025

1. En el Monitor, en la ventana del chat, localice el mensaje que desea editar.
2. Pase el ratón sobre el mensaje y haga clic en el icono de lápiz que aparece.
3. Edite el mensaje y haga clic en **Guardar**.
   Los cambios se guardan. El mensaje se etiqueta como **Editado**.

Eliminar mensaje

Puede eliminar cualquier mensaje que haya enviado en el chat.

Para eliminar un mensaje en la sesión de chat

1. En el Monitor, en la ventana del chat, localice el mensaje que desea eliminar.
2. Pase el ratón sobre el mensaje y haga clic en el icono de la papelera que aparece.
3. Haga clic en **Eliminar** en la ventana de confirmación.

Buscar en el chat

Puede buscar ciertos mensajes o palabras clave en las sesiones de chat o ver el historial de chat de una fecha específica.

Para buscar en la sesión de chat

1. En el Monitor, en la ventana del chat, haga clic en el icono de bucle.
2. [Opcional] Para ver el historial de chat de una fecha específica, haga clic en el icono del calendario y, a continuación, seleccione la fecha.

   Nota
   Solo las fechas para las que hay un historial de chat disponible están habilitadas para su selección.

   El sistema muestra el historial de chat desde la fecha que seleccionó.
3. [Opcional] En el campo de búsqueda, escriba la palabra clave o el mensaje que desea encontrar.
   El sistema muestra el número de resultados que coinciden con la búsqueda. Puede utilizar las flechas para ir al siguiente o al anterior resultado.

Finalizar chat

Puede finalizar la sesión de chat en cualquier momento.

Para finalizar la sesión de chat

1. En el Monitor, abra la ventana del chat.
2. Haga clic en **Finalizar chat**.
3. En la ventana de confirmación, haga clic en **Finalizar**.
   La sesión de chat está cerrada.

© Acronis International GmbH, 2003-2025

Activar o desactivar las notificaciones de chat en Cyber Protect Monitor

Puede habilitar las notificaciones de chat y ver una notificación en el escritorio cuando reciba nuevos mensajes de chat. Al hacer clic en la notificación, se abrirá la ventana del chat directamente.

Alternativamente, si no desea ver las notificaciones de escritorio sobre nuevos mensajes de chat, puede desactivar las notificaciones de chat.

Activar notificaciones

Para habilitar notificaciones de chat

1. Abra Cyber Protect Monitor.
2. Haga clic en **Configuración**.
3. Haga clic en **Notificaciones de chat**.
4. Seleccione **Notificaciones de escritorio** y haga clic en **Guardar**.

Desactivar notificaciones

Para deshabilitar las notificaciones de chat

1. Abra Cyber Protect Monitor.
2. Haga clic en **Configuración**.
3. Haga clic en **Notificaciones de chat**.
4. Quite **Notificaciones de escritorio** y haga clic en **Guardar**.

Informes

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Un informe sobre operaciones puede incluir cualquier conjunto de widgets del panel de control. Todos los widgets muestran la información de resumen de toda la empresa.

Según el tipo de widget, el informe incluye datos para un intervalo de tiempo o para el momento de la navegación o generación de informes. Consulte "Datos informados según el tipo de widget" (p. 369).

Todos los widgets históricos muestran la información del mismo intervalo de tiempo. Puede cambiar este intervalo en la configuración de los informes.

Puede utilizar informes predeterminados o crear uno personalizado.

Puede descargar un informe o enviarlo por correo electrónico en formato XLSX (Excel) o PDF.

© Acronis International GmbH, 2003-2025

El conjunto de informes predeterminados depende de la edición del servicio Cyber Protection que tenga. Los informes predeterminados se indican a continuación:

Nombre del informe	Descripción
#CyberFit Score por equipo	Muestra el #CyberFit Score, basado en la evaluación de parámetros de seguridad y en la configuración de cada equipo, así como las recomendaciones para mejoras.
Alertas	Muestra las alertas que se producen durante un periodo especificado.
Detalles del análisis de copias de seguridad	Muestra información detallada sobre las amenazas detectadas en las copias de seguridad.
Actividades diarias	Muestra información resumida sobre las actividades realizadas durante un periodo especificado.
Mapa de protección de datos	Muestra información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes de los equipos.
Amenazas detectadas	Muestra información sobre los equipos afectados por número de amenazas bloqueadas, así como la de los equipos en buen estado y los vulnerables.
Equipos detectados	Enumera todos los equipos hallados en la red de la organización.
Predicción del estado del disco	Muestra predicciones de cuándo se deteriorará el disco duro/SSD y del estado actual del disco.
Vulnerabilidades existentes	Muestra las vulnerabilidades existentes en el sistema operativo de su organización. El informe también muestra información de los equipos afectados en su red respecto a cada producto enumerado.
Inventario de software	Muestra información sobre el software instalado en los dispositivos de su organización.
Inventario de hardware	Muestra información sobre el hardware disponible en los dispositivos de su organización.
Resumen de gestión de parches	Muestra el número de parches que faltan, los instalados y los aplicables. Puede desglosar los informes para obtener información sobre los parches que faltan y los instalados, así como detalles de todos los sistemas.
Resumen	Muestra la información resumida sobre los dispositivos protegidos durante un periodo especificado.
Actividades semanales	Muestra información resumida sobre las actividades realizadas durante un periodo especificado.
Sesiones remotas	Muestra la información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos.

© Acronis International GmbH, 2003-2025

Nota
Los datos de uso del almacenamiento local solo se comunican a nivel de unidad y de inquilino de cliente. Los usuarios no reciben información sobre el uso del almacenamiento local en los informes de resumen.

Acciones con informes

Añadir

Pasos para añadir un nuevo informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes disponibles, haga clic en **Añadir informe**.
3. [Para añadir un informe predefinido] Haga clic en el nombre del informe predefinido.
4. [Para añadir un informe personalizado] Haga clic en **Personalizar** y añada widgets al informe.
5. [Opcional] Arrastre y suelte los widgets para reorganizarlos.

Vista

Pasos para ver un informe

- Para ver un informe, haga clic en su nombre.

Editar

Pasos para editar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea editar.
3. En la esquina superior derecha de la pantalla, haga clic en **Configuración**.
4. Edite el informe y haga clic en **Guardar**.

Eliminar

Pasos para eliminar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea eliminar.
3. En la esquina superior derecha de la pantalla, haga clic en el icono de elipsis (...) y luego en **Eliminar informe**.
4. Haga clic en **Eliminar** en la ventana de confirmación.

Planificación

Para programar un informe

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea programar.
3. En la esquina superior derecha de la pantalla, haga clic en **Configuración**.
4. Junto a **Programado**, habilite el conmutador.
   - Especifique las direcciones de correo electrónico de los destinatarios.
   - Seleccione el formato del informe.

     - **Nota**
       Puede exportar hasta 1000 elementos en un archivo PDF y hasta 10 000 elementos en un archivo XLSX. La fecha y hora de los archivos PDF y XLSX utilizan la hora local de su equipo.

   - Seleccione el idioma del informe.
   - Configure la planificación.
5. Haga clic en **Guardar**.

Descargar

Pasos para descargar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. En la esquina superior derecha de la pantalla, haga clic en **Descargar**.
4. Seleccione el formato del informe.

Como resultado, se descarga un archivo en el formato seleccionado a su equipo.

Si ha seleccionado **Excel y PDF**, se descargará un archivo ZIP en su equipo.

Enviar

Pasos para enviar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. En la esquina superior derecha de la pantalla, haga clic en **Enviar**.
4. Especifique las direcciones de correo electrónico de los destinatarios.
5. Seleccione el formato del informe.
6. Haga clic en **Enviar**.

Estructura de exportación

Pasos para exportar la estructura del informe

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. En la esquina superior derecha de la pantalla, haga clic en el icono de elipsis (...) y luego en **Exportar**.

Como resultado, la estructura del informe se guarda en su equipo como un archivo JSON.

Volcar datos

Para volcar los datos del informe

Puede exportar todos los datos de un periodo personalizado, sin filtrarlos, a un archivo CSV y enviar el archivo CSV a un destinatario de correo electrónico. El archivo CSV solo contiene datos acerca de los widgets que se incluyen en el informe.

Nota
Puede exportar hasta 150 000 elementos en un archivo CSV. La fecha y hora del archivo CSV utilizan la Hora universal coordinada (UTC).

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe cuyos datos desea volcar.
3. En la esquina superior derecha de la pantalla, haga clic en el icono de elipsis (...) y luego en **Volcar datos**.
4. Especifique las direcciones de correo electrónico de los destinatarios.
5. En **Intervalo de tiempo**, especifique el periodo personalizado para el que desea volcar datos.

   Nota
   La preparación de archivos CSV para periodos más largos lleva más tiempo.

6. Haga clic en **Enviar**.

Datos informados según el tipo de widget

Según el rango de datos que muestran, hay dos tipos de widgets en el panel de control:

- Widgets que muestran los datos reales en el momento de la navegación o la generación de informes.
- Widgets que muestran datos históricos.

Cuando configure un rango de fechas en los ajustes del informe para volcar datos para un periodo determinado, el rango de tiempo seleccionado se aplicará solo a los widgets que muestran datos históricos. El parámetro del rango de tiempo no se aplica a los widgets que muestran los datos reales en el momento de la navegación.

La siguiente tabla enumera los widgets disponibles y sus rangos de datos.

© Acronis International GmbH, 2003-2025

Nombre del widget	Datos mostrados en el widget e informes
#CyberFit Score por equipo	Reales
5 últimas alertas	Reales
Detalles de las alertas activas	Reales
Resumen de alertas activas	Reales
Actividades	Históricos
Lista de actividades	Históricos
Historial de alertas	Históricos
Estadísticas de la estrategia de ataque	Históricos
Detalles del análisis de copias de seguridad (amenazas)	Históricos
Estado de la copia de seguridad	Históricos: en columnas **Ejecuciones totales** y **Número de ejecuciones correctas** Reales: en el resto de columnas
URL bloqueadas	Reales
Aplicaciones de Cloud	Reales
Cyber protection	Reales
Mapa de protección de datos	Históricos
Dispositivos	Reales
Dispositivos detectados	Reales
Resumen del estado del disco	Reales
Estado del disco por dispositivos físicos	Reales
Vulnerabilidades existentes	Históricos
Cambios del hardware	Históricos
Detalles del hardware	Reales
Inventario de hardware	Reales
Resumen de alertas histórico	Históricos
Historial de actividad del incidente	Históricos
Resumen de ubicaciones	Reales

© Acronis International GmbH, 2003-2025

Actualizaciones que faltan por categoría	Reales
Sin protección	Reales
Historial de instalación de parches	Históricos
Estado de instalación del parche	Históricos
Resumen de la instalación del parche	Históricos
Estado de la protección	Reales
Elementos afectados recientemente	Históricos
Sesiones remotas	Históricos
Gráfico de quemado de incidentes de seguridad	Históricos
Tiempo medio de reparación de incidentes de seguridad	Históricos
Inventario de software	Reales
Información general del software	Históricos
Estado de la amenaza	Reales
Equipos vulnerables	Reales
Estado de la red de las cargas de trabajo	Reales

© Acronis International GmbH, 2003-2025

Gestión de cargas de trabajo en la consola de Cyber Protect

En esta sección se describe cómo gestionar las cargas de trabajo en la consola de Cyber Protect.

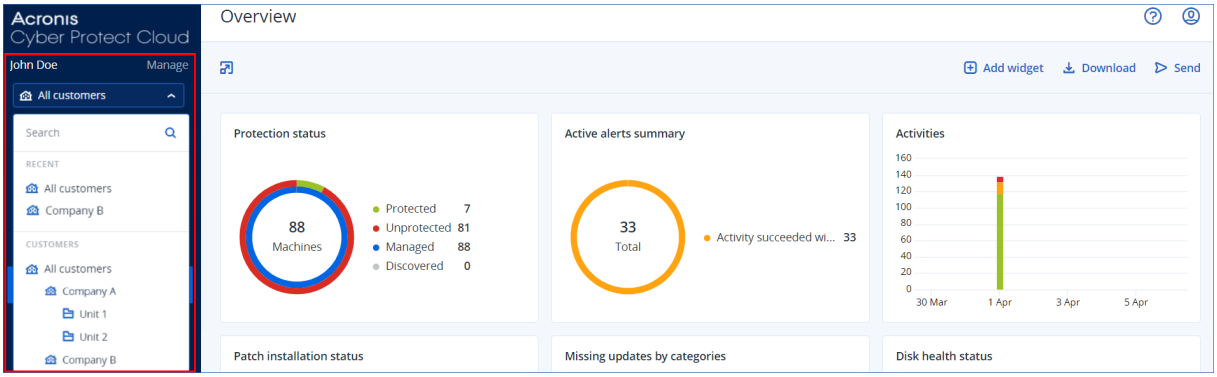
Consola de Cyber Protect

En la consola de Cyber Protect puede gestionar cargas de trabajo y planes, modificar la configuración de seguridad, configurar los informes y comprobar el almacenamiento de copias de seguridad.

La consola de Cyber Protect proporciona acceso a servicios o funciones adicionales, como File Sync & Share o protección antivirus y antimalware y filtrado de URL, gestión de parches, control de dispositivos y evaluación de vulnerabilidades. El tipo y el número de estos servicios y características varían según su licencia de Cyber Protection.

Para comprobar la información más importante acerca de su protección en el panel de control, vaya a **Supervisión** > **Información general**.

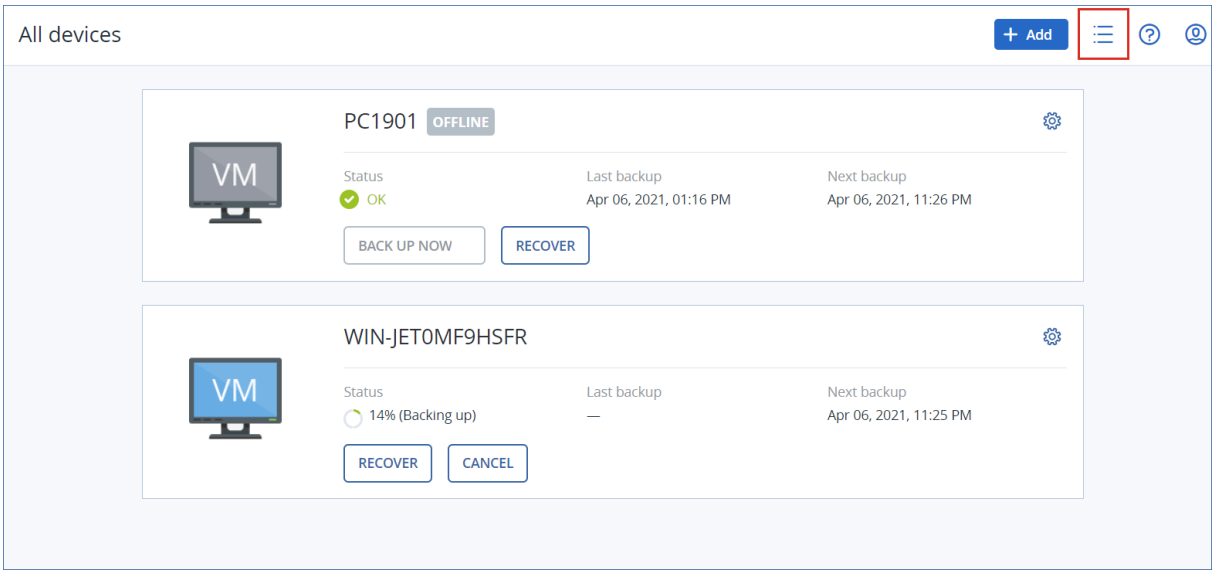
Según sus permisos de acceso, puede administrar la protección de uno o varios inquilinos o unidades de un inquilino. Para cambiar el nivel de jerarquía, utilice la lista desplegable del menú de navegación. Solo se muestran los niveles a los que tiene acceso. Para acceder al portal de administración, haga clic en **Gestionar**.



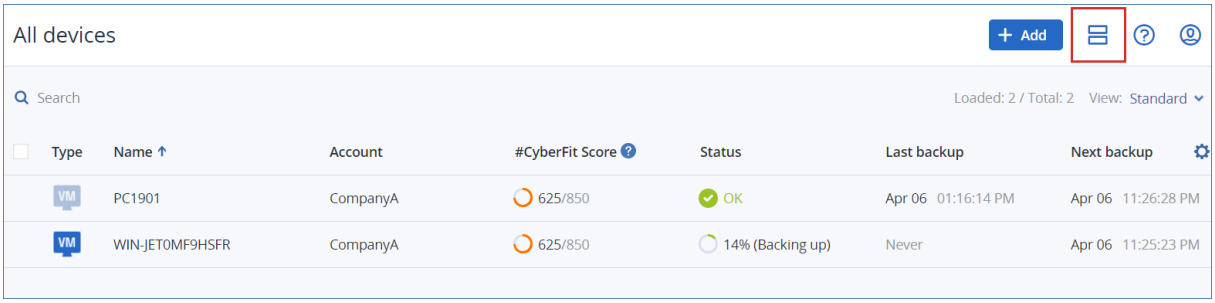
La sección **Dispositivos** está disponible en la vista sencilla y de tabla. Para cambiar entre ellas, haga clic en el icono correspondiente en la esquina superior derecha.

La vista sencilla muestra solo unas pocas cargas de trabajo.

© Acronis International GmbH, 2003-2025



La vista de tabla se habilita automáticamente si el número de cargas de trabajo aumenta.



Las dos vistas proporcionan acceso a las mismas operaciones y características. Este documento detalla el acceso a operaciones desde la vista de tabla.

Cuando una carga de trabajo se conecta o desconecta de la red, su estado tarda un tiempo en cambiar en la consola de Cyber Protect. Se verifica el estado de la carga de trabajo cada minuto. Si el agente instalado en el equipo correspondiente no transfiere datos y no hay respuesta tras cinco comprobaciones consecutivas, la carga de trabajo se mostrará como offline. Se mostrará que la carga de trabajo vuelve a estar en línea cuando responda a una comprobación de estado o cuando comience a transferir datos.

Novedades de la consola de Cyber Protect

Cuando haya nuevas funciones de Cyber Protect Cloud disponibles, verá una ventana emergente con una breve descripción de estas al iniciar sesión en la consola de Cyber Protect.

También puede ver la descripción de las nuevas funciones haciendo clic en el enlace **Novedades** situado en la esquina inferior izquierda de la pantalla principal de la consola de Cyber Protect.

Si no hay nuevas funciones, no se mostrará el enlace **Novedades**.

Niveles de administración en la consola de Cyber Protect

Cyber Protect Cloud admite la administración en los siguientes niveles:

© Acronis International GmbH, 2003-2025

- Nivel de partner (**Todos los clientes**)

  Este nivel solo está disponible para los administradores de partners que gestionan inquilinos de cliente.
- Nivel de cliente

  Este nivel está disponible para los administradores de clientes y administradores de partners que gestionan inquilinos de cliente.
- Nivel de unidad

  Este nivel está disponible para los administradores de unidad, los administradores de clientes del inquilino principal y los administradores de partners que gestionan el inquilino de clientes principal.

Los administradores pueden gestionar objetos, como planes o cargas de trabajo, en sus propios inquilinos y en sus inquilinos secundarios, con las siguientes limitaciones:

- Los inquilinos de clientes pueden restringir el acceso a los administradores de partners.
- Los administradores de clientes y los administradores de partners que gestionan el inquilino de clientes principal pueden acceder a las unidades en todo momento.

Los administradores no pueden ver ni acceder a objetos en un nivel superior al de su propio inquilino.

Por ejemplo, los administradores de clientes pueden gestionar planes de protección en el nivel de cliente y en el nivel de unidad. Los administradores de unidad solo pueden gestionar sus propios planes de protección en el nivel de unidad. No pueden gestionar planes de protección en el nivel de cliente ni los planes de protección creados por el administrador de clientes en el nivel de unidad. Para más información consulte "Planes en diferentes niveles de administración" (p. 246).

Selección de un nivel de administración

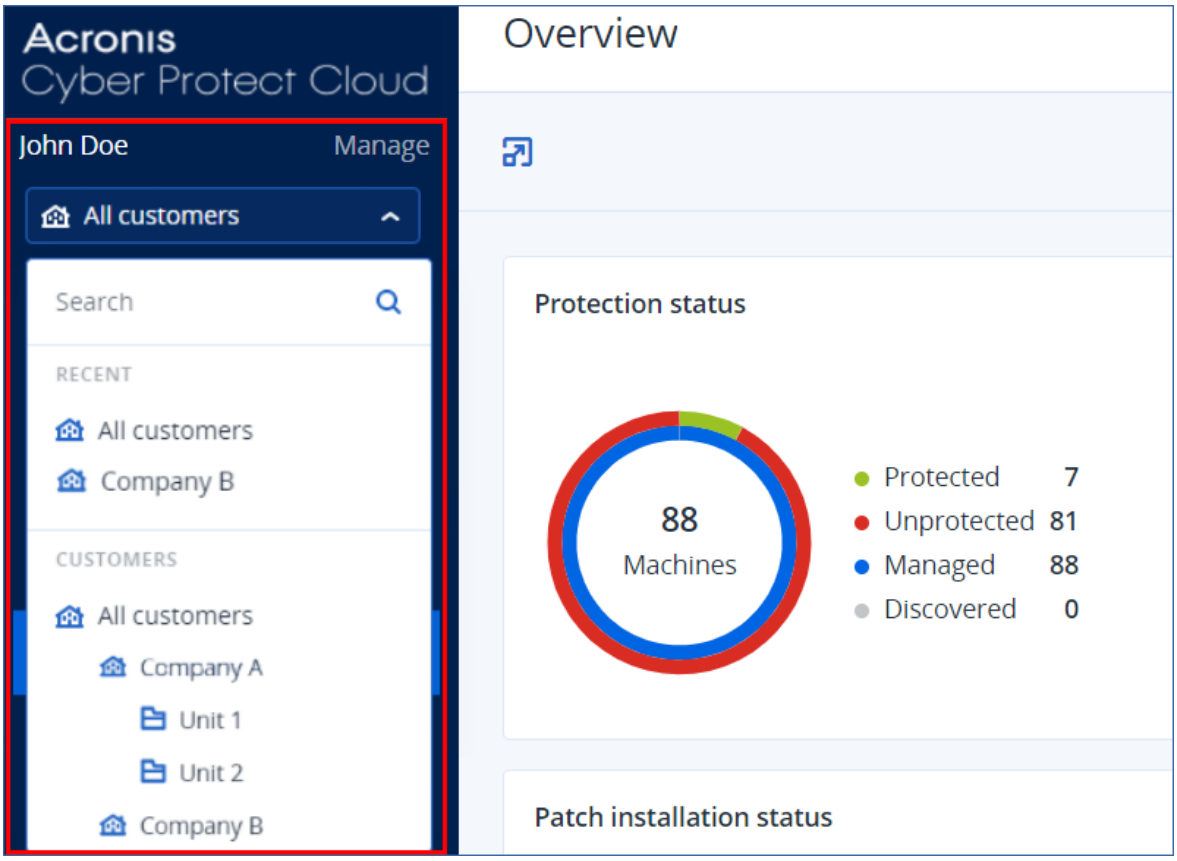
Los administradores que gestionan varios inquilinos y pueden acceder al portal de administración pueden seleccionar el nivel de administración en la consola de Cyber Protect.

Para seleccionar un nivel de administración

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. En el menú de navegación situado a la izquierda, haga clic en la flecha junto al nombre del inquilino.
3. Seleccione una de las siguientes opciones:
   - [Para administradores de partners] Para trabajar a nivel de partner, seleccione **Todos los clientes**.

© Acronis International GmbH, 2003-2025

- Para trabajar en el nivel de cliente o unidad, seleccione el nombre de un cliente o unidad.



Uso de la consola de Cyber Protect a nivel de **Todos los clientes**

Los administradores de partners pueden utilizar la consola de Cyber Protect a nivel de partner (**Todos los clientes**).

En este nivel, los administradores de partners pueden realizar acciones con cargas de trabajo de diferentes clientes. Por ejemplo, un administrador de partner puede aplicar el mismo plan a varias cargas de trabajo de diferentes clientes.

A nivel de partner (**Todos los clientes**), la consola de Cyber Protect ofrece una vista personalizada. Por ejemplo, las pestañas **Alertas** y **Actividades** proporcionan filtros adicionales relacionados con el partner, mientras que las pestañas **Dispositivos** y **Gestión** proporcionan acceso solo a las funciones u objetos que son accesibles para los administradores de partners.

Pestaña Alertas

Los administradores de partners pueden ver las alertas de todos los clientes que gestionan, buscarlas y filtrarlas según los siguientes criterios:

- Dispositivo
- Cliente
- Plan

Pestaña Actividades

© Acronis International GmbH, 2003-2025

Los administradores de partners pueden ver las actividades de todos los inquilinos gestionados o las actividades de un inquilino en concreto.

Las actividades se pueden filtrar por cliente, estado, hora y tipo.

Los siguientes tipos de actividades se preseleccionan automáticamente a nivel de partner:

- Aplicando plan
- Creación del plan de protección
- Plan de protección
- Revocando plan
- Programación

Pestaña Dispositivos

Los administradores de partners pueden ver las cargas de trabajo de todos los inquilinos gestionados, seleccionar cargas de trabajo de diferentes inquilinos y crear grupos de dispositivos.

Importante
En el nivel de partner (**Todos los clientes**), es posible que no pueda realizar todas las operaciones que están disponibles en el nivel de cliente. Para realizar una operación que no es compatible en el nivel de partner, vaya al nivel de cliente.

Pestaña Gestión

Los planes disponibles se agrupan por tipo.

En **Gestión** > **Planes de protección**, los administradores de partners pueden ver los planes que se utilizan en los inquilinos de clientes gestionados y filtrar estos planes por estado, cliente y fecha de creación. Los administradores de partners pueden crear nuevos planes a nivel de partner. Para obtener más información sobre los planes en diferentes niveles, consulte "Planes en diferentes niveles de administración" (p. 246).

Pestaña Gestión del software

Si el escaneo de inventario de software está habilitado para las cargas de trabajo del cliente, usted podrá ver los resultados del escaneo del software.

Visualizar las cargas de trabajo de clientes específicos

A nivel de partner, puede ver las cargas de trabajo con agentes que pertenecen a cada inquilino de cliente gestionado.

Para ver las cargas de trabajo de un cliente específico

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. En el árbol, haga clic en **Equipos con agentes** para ampliar la lista.
3. Haga clic en el nombre del cliente cuyas cargas de trabajo desea ver y gestionar.

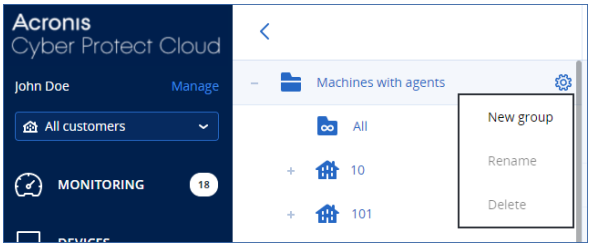
© Acronis International GmbH, 2003-2025

Crear grupos de dispositivos estáticos en el nivel de partner

Puede crear grupos de dispositivos estáticos en el nivel de partner (**Todos los dispositivos**).

Cómo crear grupos de dispositivos estáticos en el nivel de partner

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en el icono de engranaje situado junto a **Equipos con agentes** y, a continuación, haga clic en **Nuevo grupo**.



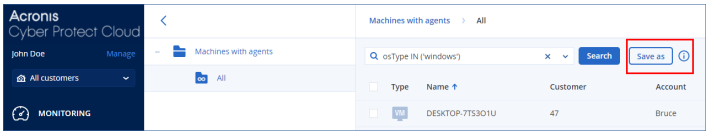
3. Especifique el nombre del grupo.
4. Agregue una descripción.
5. Haga clic en **Aceptar**.

Crear un grupo dinámico de dispositivos en el nivel de partner

Puede crear grupos dinámicos de dispositivos en el nivel de partner (**Todos los dispositivos**).

Pasos para crear un grupo dinámico de dispositivos en el nivel de partner

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. En el árbol, haga clic en **Equipos con agentes** para ampliar la lista.
3. Haga clic en **Todos**.
4. En el campo de búsqueda, especifique los criterios según los que desee crear un grupo de dispositivos dinámico y, a continuación, haga clic en **Buscar**.
   Para obtener más información sobre los criterios de búsqueda disponibles, consulte "Atributos de búsqueda para cargas de trabajo que no son de nube a nube" (p. 417) y "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 416).
5. Haga clic en **Guardar como** y especifique el nombre del grupo.



6. [Opcional] Agregue una descripción.
7. Haga clic en **Aceptar**.

Ejecutar autodetección de equipos en el nivel de partner

Puede ejecutar la autodetección de equipos en el nivel de partner (**Todos los clientes**).

© Acronis International GmbH, 2003-2025

Requisitos previos

Hay al menos una máquina con un agente de protección instalado en la red local de su cliente o en el dominio del directorio activo.

Importante
Solo los agentes que estén instalados en máquinas Windows pueden ser agentes de detección. Si no hay agentes de detección en los entornos de su cliente, no podrá utilizar la opción **Múltiples dispositivos** en el panel **Añadir dispositivos**.

La autodetección no permite añadir controladores de dominio debido a los permisos adicionales necesarios para que el servicio de agente se ejecute.

La instalación remota de agentes solo se admite en las máquinas que ejecuten Windows (Windows XP no es compatible). Para la instalación remota en una máquina que ejecute Windows Server 2012 R2, debe instalarse la actualización de Windows KB2999226.

Para ejecutar autodetección de máquinas en el nivel de inquilino partner

Buscar en Active Directory

Pasos para añadir varios dispositivos desde Active Directory

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Múltiples dispositivos**, haga clic en **Detectar dispositivos**.
   Se abre el asistente de detección.
4. Seleccione un inquilino de cliente y, a continuación, seleccione el agente de detección que realizará el escaneo para detectar máquinas.

   Nota
   Un agente de detección es un recurso informático en el que se instala un agente de protección.
   El agente de detección debe ser un miembro del dominio de Active Directory.
   Puede seleccionar un agente que esté asociado con el inquilino seleccionado.

5. Seleccione **Buscar en Active Directory** y haga clic en **Siguiente**.
6. En la ventana **Buscar en Active Directory**, seleccione cómo buscar los equipos y haga clic en **Aceptar**.

Opción	Descripción
En lista de unidades organizativas	Seleccione el grupo de equipos que se va a añadir.
Por consulta	Use la consulta en dialecto LDAP para seleccionar los equipos. La **base de**

© Acronis International GmbH, 2003-2025

Opción	Descripción
en dialecto LDAP.	**búsqueda** define dónde buscar, mientras que la opción **Filtro** le permite especificar el criterio de selección de los equipos.

7. En la lista de máquinas detectadas, seleccione los equipos que desee añadir y, a continuación, haga clic en **Siguiente**.

   Se abrirá la pestaña **Seleccionar opción de incorporación**. Las siguientes opciones de incorporación están disponibles.

Opción	Descripción
Incorporación automática completa a través de Active Directory	Esta opción utiliza un controlador de dominio en el que se ha instalado un agente de detección para incorporar dispositivos detectados desde Active Directory. No es necesario realizar una preconfiguración manual de los dispositivos.
Preconfiguración manual e incorporación automática	Esta opción requiere la preconfiguración manual de los dispositivos y utiliza un agente de detección para la incorporación de los dispositivos detectados.
Agregar como máquinas no administradas	Esta opción agrega los dispositivos detectados a la consola como dispositivos sin gestionar, sin instalar un agente de protección en ellos.

8. Dependiendo de la opción de incorporación que seleccione, haga lo siguiente:
   - Si ha seleccionado **Incorporación automática completa a través de Active Directory**, complete los pasos 4-13 del procedimiento correspondiente.
   - Si ha seleccionado **Preconfiguración manual e incorporación automática**, complete los pasos 4-11 del procedimiento correspondiente.
   - Si ha seleccionado **Agregar como equipos sin gestionar**, seleccione la cuenta de usuario en la que se registrarán los dispositivos y haga clic en **Agregar**.

Analizar red local

Para detectar varios dispositivos al analizar la red local

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Múltiples dispositivos**, haga clic en **Detectar dispositivos**.

   Se abre el asistente de detección.
4. Seleccione un inquilino de cliente y, a continuación, seleccione el agente de detección que realizará el escaneo para detectar máquinas.
5. Haga clic en **Analizar red local**.

© Acronis International GmbH, 2003-2025

Comienza el análisis detección activa de dispositivos. Se le redirige a la pantalla **Dispositivos detectados** > **Red de área local**. Una vez finalizado el análisis, se muestra una notificación en la que se indica la cantidad de dispositivos detectados e incluye un enlace a la lista de dispositivos donde puede ver detalles adicionales sobre ellos.

De forma manual o importando un archivo

Pasos para añadir varios dispositivos manualmente o importando un archivo

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Múltiples dispositivos**, haga clic en **Detectar dispositivos**.
   Se abre el asistente de detección.
4. Seleccione un inquilino de cliente y, a continuación, seleccione el agente de detección que realizará el escaneo para detectar máquinas.
5. Haga clic en **Especificar manualmente o importar desde un archivo**.
6. Añada equipos mediante una de las siguientes opciones.
   - Para añadir equipos manualmente:
     a. En el campo **Añadir equipo**, escriba la dirección IPv4 o el nombre de host del equipo.
     b. Repita el paso previo para cada equipo que quiera añadir.
   - Pasos para añadir equipos importando un archivo:
     a. Haga clic en **Importar lista de equipos desde archivo**.
     b. En la ventana **Importar lista de equipos desde archivo**, suelte el archivo de texto que contiene la lista de equipos o haga clic en **Examinar**, navegue hasta el archivo, selecciónelo y haga clic en **Abrir**.
     El archivo debe contener direcciones IP o nombres de host, uno por línea. A continuación se muestra un ejemplo del contenido del archivo:

     ```
     156.85.34.10
     156.85.53.32
     156.85.53.12
     EN-L00000100
     EN-L00000101
     ```

   Cuando ya se hayan añadido las direcciones de los equipos manualmente o se hayan importado de un archivo, el agente intentará anclar los equipos añadidos y comprobar su disponibilidad.
7. Haga clic en **Siguiente**.
   Se abrirá la pestaña **Seleccionar opción de incorporación**. Las siguientes opciones de incorporación están disponibles.

Opción	Descripción
Incorporación automática	Esta opción utiliza un controlador de dominio en el que se ha instalado un agente de detección para incorporar dispositivos

© Acronis International GmbH, 2003-2025

Opción	Descripción
completa a través de Active Directory	detectados desde Active Directory. No es necesario realizar una preconfiguración manual de los dispositivos.
Preconfiguración manual e incorporación automática	Esta opción requiere la preconfiguración manual de los dispositivos y utiliza un agente de detección para la incorporación de los dispositivos detectados.
Agregar como máquinas no administradas	Esta opción agrega los dispositivos detectados a la consola como dispositivos sin gestionar, sin instalar un agente de protección en ellos.

8. Dependiendo de la opción de incorporación que seleccione, haga lo siguiente:
   - Si ha seleccionado **Incorporación automática completa a través de Active Directory**, complete los pasos 4-13 del procedimiento correspondiente.
   - Si ha seleccionado **Preconfiguración manual e incorporación automática**, complete los pasos 4-11 del procedimiento correspondiente.
   - Si ha seleccionado **Agregar como equipos sin gestionar**, seleccione la cuenta de usuario en la que se registrarán los dispositivos y haga clic en **Agregar**.

Creación de un plan global de exclusiones de antivirus y antimalware

El plan global de exclusiones de antivirus y antimalware (exclusiones globales) le permite crear una lista de elementos de confianza a nivel de partner. Los administradores de partners pueden añadir archivos, carpetas, procesos o hashes a un único plan y aplicarlo a todas las cargas de trabajo de los clientes. El plan de exclusiones globales gestiona de forma eficiente las listas de elementos de confianza para los inquilinos de los clientes al eliminar la necesidad de editar manualmente cada plan de protección individual.

Cómo crear un plan global de exclusiones de antivirus y antimalware

1. En el portal de administración, vaya a **Supervisión** > **Uso**.
2. En **Cyber Protect**, seleccione **Protección** y haga clic en **Gestionar servicio**.
3. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
4. Haga clic en **Crear plan**.
   Se abrirá la plantilla del plan de protección.
5. Despliegue el módulo **Exclusiones globales de protección antivirus y antimalware**.
6. Seleccione la opción **Exclusiones**.
   Se abre la ventana **Exclusiones globales de antivirus y antimalware**.
7. En la sección **Elementos de confianza**, haga clic en **Agregar** para seleccionar entre las opciones disponibles:

© Acronis International GmbH, 2003-2025

- Para añadir archivos, carpetas o procesos a los elementos de confianza, seleccione la opción **Archivo/carpeta/proceso**. Se mostrará la ventana **Añadir archivo/carpeta/proceso**.
  - En el campo **Archivo/proceso/carpeta**, escriba la ruta para cada proceso, carpeta o archivo en una nueva línea.
  - Seleccione la casilla de verificación **Añadir como archivo/carpeta** para añadir el archivo o carpeta a los elementos de confianza.
    Ejemplos de descripciones de carpetas: `D:\folder\`, `/home/Folder/folder2`, `F:\`
  - Seleccione la casilla de verificación **Añadir como proceso** para añadir el proceso a los elementos de confianza. Los procesos seleccionados se excluirán de la supervisión.
    Puede especificar la ruta completa a un proceso o usar un comodín. Por ejemplo, para excluir todos los procesos en la carpeta `Temp`, puede introducir `C:\Windows\Temp\*.exe`.
    También se admiten rutas de red local. Por ejemplo, `\\localhost\folderpath\file.exe`
- Para añadir los hashes MD5 a la lista de elementos de confianza, seleccione la opción **Hash**. Se abrirá la ventana **Añadir hash**.
  - Aquí puede insertar los hash MD5 en líneas separadas para que se incluyan como de confianza en la lista de exclusiones de protección. En función de estos hash, Cyber Protection excluirá los procesos descritos por los hash MD5 de la supervisión.

8. En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos de confianza. Por ejemplo, motivos y propósitos de la exclusión, fecha/hora, etc.

   Nota
   Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

9. Haga clic en **Agregar** y luego en **Listo**.

Nota

- Puede crear tantos planes de exclusiones globales como necesite y aplicarlos a las cargas de trabajo de sus clientes directos.
- Los planes activos se aplican de forma acumulativa.
- Si el mismo elemento aparece en más de un plan, no se duplicará.
- Un elemento siempre será de confianza si existe en la lista de elementos de confianza bajo un plan de exclusiones globales y en la lista de elementos bloqueados bajo el módulo de exclusiones de protección.

Uso de comodines para definir exclusiones

Para definir exclusiones, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. El signo de pregunta (?) sustituye exactamente cero o un carácter. No pueden usarse variables de entorno, como `%AppData%`.

Puede usar un comodín (*) para añadir elementos a las listas de exclusión.

© Acronis International GmbH, 2003-2025

- Los comodines se pueden usar en medio o al final de la descripción.

Ejemplos de comodines aceptados en descripciones:

```
C:\*.pdf
```

```
D:\folders\file.*
```

```
C:\Users\*\AppData\Roaming
```

- No se pueden utilizar caracteres comodín al principio de la descripción.

Ejemplos de comodines no aceptables en descripciones:

```
*.docx
```

```
*:\folder\
```

Uso de variables para definir exclusiones

También puede usar variables para añadir elementos a las listas de exclusiones globales, con las siguientes limitaciones:

- Para Windows, solo se admiten las variables del SISTEMA. No se admiten las variables específicas del usuario, por ejemplo, `%USERNAME%` o `%APPDATA%`. No se admiten variables con `{username}`. Para obtener más información, consulte https://ss64.com/nt/syntax-variables.html.
- Para macOS, no se admiten las variables de entorno.
- Para Linux, no se admiten las variables de entorno.

Ejemplos de formatos compatibles:

- `%WINDIR%\Media`
- `%public%`
- `%CommonProgramFiles%\Acronis\`

Cargas de trabajo

Una carga de trabajo es cualquier tipo de recurso protegido, por ejemplo, un equipo físico, una máquina virtual, un buzón de correo o una instancia de la base de datos. En la consola de Cyber Protect la carga de trabajo se muestra como un objeto al que puede aplicar un plan (de protección, copia de seguridad o programación).

Algunas cargas de trabajo requieren la instalación de un agente de protección o el despliegue de un dispositivo virtual. Puede instalar agentes desde la interfaz gráfica de usuario o la interfaz de línea de comandos (instalación desatendida). Puede usar la instalación desatendida para automatizar el proceso de instalación. Para obtener más información sobre cómo instalar un agente de protección, consulte "Instalación e implementación de los agentes de Cyber Protection" (p. 38).

© Acronis International GmbH, 2003-2025

Un dispositivo virtual (VA) es una máquina virtual ya preparada que contiene un agente de protección. Con un dispositivo virtual puede hacer una copia de seguridad de otras máquinas virtuales en el mismo entorno sin instalar un agente de protección en ellas (copia de seguridad sin agente). Los dispositivos virtuales están disponibles en formatos específicos de hipervisor, como .ovf, .ova, o .qcow. Para obtener más información sobre qué plataformas de virtualización admiten la copia de seguridad sin agente, consulte "Plataformas de virtualización compatibles" (p. 511).

Importante
Los agentes deben estar en línea al menos una vez cada 30 días. De lo contrario, se revocarán sus planes y las cargas de trabajo quedarán desprotegidas.

La tabla siguiente resume los tipos de carga de trabajo y sus agentes respectivos.

Tipo de carga de trabajo	Agente	Ejemplos (lista parcial)
Equipos físicos	Se instala un agente de protección en todos los equipos protegidos.	Workstation Equipo portátil Servidor
Equipos virtuales	Según la plataforma de virtualización, puede que estén disponibles los siguientes métodos de copia de seguridad: • Copia de seguridad basada en agente: se instala un agente de protección en todos los equipos protegidos. • Copia de seguridad sin agente: se instala un agente de protección solo en el host del hipervisor, en una máquina virtual dedicada, o se despliega como un dispositivo virtual. Este agente realiza la copia de seguridad de todas las máquinas virtuales en el entorno.	Equipo virtual VMware Equipo virtual Hyper-V Máquina virtual basada en Kernel (KVM) gestionada por oVirt Máquinas virtuales de VMware Cloud Director (vCD)*
Cargas de trabajo de Microsoft 365 Business Cargas de trabajo de Google Workspace	Un agente de la nube realiza la copia de seguridad de estas cargas de trabajo, de modo que no es necesario instalar nada. Para usar el agente de la nube, debe añadir su organización de Microsoft 365 o Google Workspace a la consola de Cyber Protect. Además, hay disponible un Agente local para Office 365. Requiere instalación y solo se puede utilizar para realizar copias de seguridad de buzones de Exchange Online. Para obtener más información sobre las diferencias entre el agente local y el agente en la nube, consulte "Protección de los datos de Microsoft 365" (p. 833).	Buzón de correo de Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Sitio de SharePoint

© Acronis International GmbH, 2003-2025

Tipo de carga de trabajo	Agente	Ejemplos (lista parcial)
		Buzón de correo de Google Google Drive
Aplicaciones	La copia de seguridad de los datos de aplicaciones específicas la realizan agentes dedicados, como Agente para SQL, Agente para Exchange, Agente para MySQL/MariaDB o Agente para Active Directory.	Bases de datos de SQL Server Bases de datos de MySQL o MariaDB Bases de datos de Oracle Active Directory
Dispositivos móviles	Se instala una aplicación móvil en los dispositivos protegidos.	Dispositivos Android o iOS
Sitios web	Un agente de la nube realiza la copia de seguridad de los sitios web, de modo que no es necesario instalar nada.	Sitios web accedidos a través de los protocolos SFTP o SSH

Para obtener más información sobre qué agente necesita y dónde instalarlo, consulte "¿Qué Agente necesito?" (p. 42)

* Para obtener más información sobre la integración de VMware Cloud Director con Cyber Protect Cloud, consulte la Guía para administradores de partners.

Adición de cargas de trabajo a la consola de Cyber Protect

Para empezar a proteger sus cargas de trabajo, primero debe añadirlas a la consola de Cyber Protect.

Nota
Los tipos de carga de trabajo que puede añadir dependerán de las cuotas de servicio de su cuenta. Si falta un tipo de carga de trabajo específico, se muestra en gris en el panel **Añadir dispositivos**.

Un administrador de partners puede habilitar las cuotas de servicio necesarias en el portal de administración. Para obtener más información, consulte "Información para administradores de partners" (p. 390).

Pasos para añadir una carga de trabajo

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Dispositivos** > **Todos los dispositivos** y haga clic en **Agregar**.
   Se abrirá el panel **Añadir dispositivos** en la parte derecha.
3. Seleccione el canal de publicación.
4. Haga clic en el tipo de carga de trabajo que quiere añadir y siga las instrucciones de la carga de trabajo específica que ha seleccionado.

La tabla siguiente resume los tipos de carga de trabajo y las acciones necesarias.

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
Varios equipos Windows	Realice una autodetección en su entorno. Para llevar a cabo la autodetección, necesita al menos un equipo con un agente de protección instalado en su red local o en el dominio de Active Directory. Este agente se usa como agente de detección.	"Incorporación de varios dispositivos" (p. 189)
Estaciones de trabajo de Windows Servidores de Windows	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de agentes de protección en Windows" (p. 75)
Estaciones de trabajo de macOS	Instale el Agente para macOS.	"Instalación de agentes de protección en macOS" (p. 72) o "Instalación y desinstalación de agentes de protección en macOS" (p. 100)
Servidores de Linux	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93)
Dispositivos móviles (iOS y Android)	Instale la aplicación móvil.	"Protección de dispositivos móviles" (p. 828)

© Acronis International GmbH, 2003-2025

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
Cargas de trabajo de la nube a la nube		
Microsoft 365 Business	Añada su organización de Microsoft 365 a la consola de Cyber Protect y utilice el agente de la nube para proteger los buzones de correo de Exchange Online, los archivos de OneDrive, Microsoft Teams y los sitios de SharePoint. También puede instalar el agente local para Office 365. Solo proporciona copias de seguridad de buzones de correo de Exchange Online. Para obtener más información sobre las diferencias entre el agente local y el agente en la nube, consulte "Protección de los datos de Microsoft 365" (p. 833).	"Protección de los datos de Microsoft 365" (p. 833)
Google Workspace	Añada su organización de Google Workspace a la consola de Cyber Protect y utilice el agente de la nube para proteger los buzones de correo de Gmail y los archivos de Google Drive.	"Protección de los datos de Google Workspace" (p. 907)
Equipos virtuales		
VMware ESXi (Broadcom)	Despliegue el Agente para VMware (dispositivo virtual) en su entorno.	"Implementación de Agente para VMware (dispositivo virtual)" (p. 137)
	Instale el Agente para VMware (Windows).	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de agentes de protección en Windows" (p. 75)
Virtuozzo Hybrid Infrastructure	Despliegue el Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual) en su entorno.	"Implementación del Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual)" (p. 147)
Microsoft Hyper-V	Instale el Agente para Hyper-V.	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de

© Acronis International GmbH, 2003-2025

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
		agentes de protección en Windows" (p. 75)
Virtuozzo Hybrid Server	Instale el Agente para Virtuozzo.	"Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93)
KVM	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de agentes de protección en Windows" (p. 75)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93)
Red Hat Virtualization (oVirt)	Despliegue el Agente para oVirt (dispositivo virtual) en su entorno.	"Implementando Agent para oVirt (dispositivo virtual)" (p. 159)
Citrix Hypervisor/XenServer	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de agentes de protección en Windows" (p. 75)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93)
Nutanix AHV	Despliegue de Agente para Nutanix AHV.	"Despliegue de Agente para Nutanix AHV" (p. 171)

© Acronis International GmbH, 2003-2025

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
Oracle VM	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de agentes de protección en Windows" (p. 75)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93)
Oracle LVM (oVirt)	Despliegue el Agente para oVirt (dispositivo virtual) en su entorno.	"Implementando Agent para oVirt (dispositivo virtual)" (p. 159)
Scale Computing HyperCore	Despliegue el Agente para Scale Computing HC3 (dispositivo virtual) en su entorno.	"Implementación de Agent para Scale Computing HC3 (dispositivo virtual)" (p. 141)
Proxmox VE	Instalar Agente para Proxmox (incluido en el Agente para Linux, 64 bits)	"Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93)
Almacenamiento conectado a red		
Synology	Despliegue el Agente para Synology (dispositivo virtual) en su entorno.	"Implementar Agente para Synology" (p. 176)
Aplicaciones		
Microsoft SQL Server	Instale el Agente para SQL.	"Instalación de agentes de protección en Windows" (p. 65) o "Instalación y desinstalación de agentes de protección en Windows" (p. 75)
Microsoft Exchange Server	Instale el Agente para Exchange.	
Microsoft Active Directory	Instale el Agente para Active Directory.	
Base de datos de Oracle	Instale el Agente para Oracle.	"Protección de base de datos de Oracle" (p. 936)

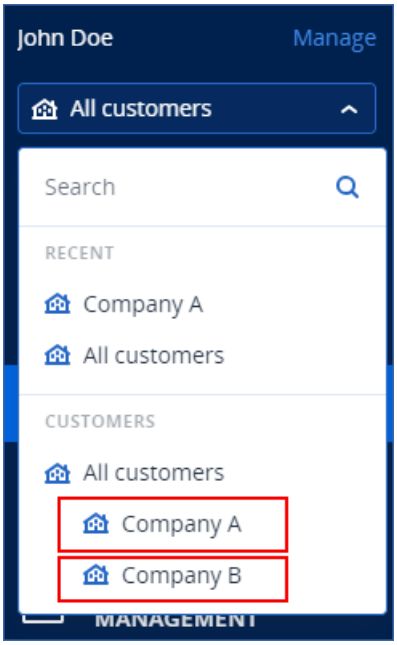
© Acronis International GmbH, 2003-2025

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
Sitio web	Configure la conexión con el sitio web.	"Protección de sitios web y servidores de alojamiento" (p. 946)

Para obtener más información sobre los agentes de protección disponibles y dónde instalarlos, consulte "¿Qué Agente necesito?" (p. 42)

Información para administradores de partners

- Es posible que falte un tipo de carga de trabajo en el panel **Añadir dispositivos** si no se habilita la cuota de servicio necesaria en el portal de administración. Para obtener más información sobre qué cuotas de servicio se necesitan para cada carga de trabajo, consulte Habilitar o deshabilitar elementos de oferta en la guía para administradores de partners.
- Como administrador de partners, no puede añadir cargas de trabajo en el nivel **Todos los clientes**. Para añadir una carga de trabajo, seleccione un inquilino de cliente individual.



Eliminación de cargas de trabajo de la consola de Cyber Protect

Puede eliminar de la consola de Cyber Protect las cargas de trabajo que ya no necesite proteger. Este procedimiento depende del tipo de carga de trabajo.

También puede desinstalar el agente de la carga de trabajo protegida. Al desinstalar un agente, se elimina automáticamente la carga de trabajo protegida de la consola de Cyber Protect.

© Acronis International GmbH, 2003-2025

Importante
Cuando se elimina una carga de trabajo de la consola de Cyber Protect, se revocan todos los planes que tenía aplicados. Al eliminar una carga de trabajo, no se eliminan los planes ni las copias de seguridad, ni se desinstala el agente de protección.

La tabla siguiente resume los tipos de carga de trabajo y las acciones necesarias.

Cargas de trabajo que se van a eliminar	Acciones necesarias	Procedimiento a seguir
Equipos físicos y virtuales		
Equipos físicos o máquinas virtuales en los que está instalado un agente de protección	1. Elimine la carga de trabajo de la consola de Cyber Protect. 2. [Opcional] Desinstale el agente de protección.	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Carga de trabajo con agente de protección)
Máquinas virtuales de las que se hace una copia de seguridad a nivel del hipervisor (copia de seguridad sin agente)	1. En la consola de Cyber Protect, elimine el equipo en el que está instalado el agente de protección. Todas las máquinas virtuales de las que este agente haga una copia de seguridad se eliminarán automáticamente de la consola. 2. [Opcional] Desinstale el agente de protección.	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Carga de trabajo sin un agente de protección)
Cargas de trabajo de la nube a la nube		
Cargas de trabajo de Microsoft 365	Elimine la organización de Microsoft 365 o Google Workspace de	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Carga de trabajo de la nube a la nube)

© Acronis International GmbH, 2003-2025

Cargas de trabajo que se van a eliminar	Acciones necesarias	Procedimiento a seguir
Business Cargas de trabajo de Google Workspace	la consola de Cyber Protect. Todos los recursos de esa organización se eliminarán automáticamente de la consola.	
Dispositivos móviles		
Dispositivos Android Dispositivos iOS	1. Elimine el dispositivo móvil de la consola de Cyber Protect. 2. [Opcional] Desinstale la aplicación del dispositivo móvil.	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Dispositivo móvil)
Almacenamiento conectado a red		
Synology	1. Elimine la carga de trabajo de la consola de Cyber Protect. 2. [Opcional] Desinstale el agente de protección.	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Carga de trabajo con un agente de protección)
Aplicaciones		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Base de datos de Oracle	1. En la consola de Cyber Protect, elimine el equipo en el que está instalado el agente de protección. Todos los objetos de los que este agente haga una copia de seguridad se eliminarán automáticamente	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Carga de trabajo sin un agente de protección)

© Acronis International GmbH, 2003-2025

Cargas de trabajo que se van a eliminar	Acciones necesarias	Procedimiento a seguir
	de la consola. 2. [Opcional] Desinstale el agente de protección.	
Sitios web	Elimine el sitio web de la consola de Cyber Protect.	"Pasos para eliminar una carga de trabajo de la consola de Cyber Protect" (p. 393) (Sitio web)

Pasos para eliminar una carga de trabajo de la consola de Cyber Protect

Carga de trabajo con un agente de protección

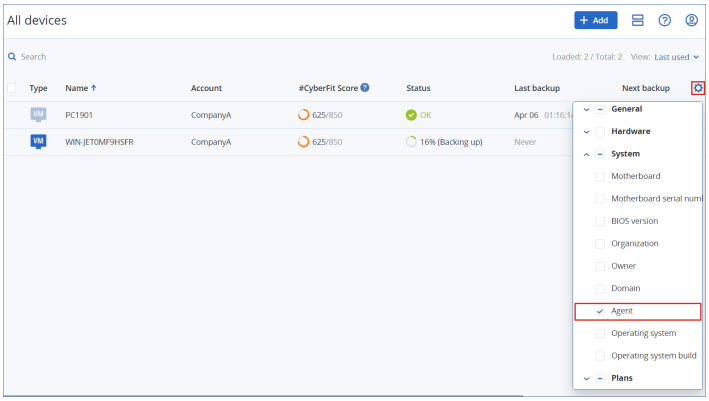
Puede eliminar este tipo de carga de trabajo directamente.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione la casilla de verificación de una o más cargas de trabajo que quiera eliminar.
3. En el panel **Acciones**, haga clic en **Eliminar**.
4. Haga clic en **Eliminar** para confirmar su elección.
5. [Opcional] Desinstale el agente tal como se describe en "Desinstalación de agentes" (p. 73).

Carga de trabajo sin un agente de protección

Para eliminar este tipo de carga de trabajo, debe eliminar el equipo en el que está instalado el agente de protección.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en el icono de engranaje en la esquina superior derecha y seleccione la casilla de verificación **Agente**.



Se mostrará la columna **Agente**.

© Acronis International GmbH, 2003-2025

3. En la columna **Agente**, compruebe el nombre del equipo donde está instalado el agente de protección.
4. En la consola de Cyber Protect, seleccione la casilla de verificación junto al equipo en el que está instalado el agente de protección.
5. En el panel **Acciones**, haga clic en **Eliminar**.
6. Haga clic en **Eliminar** para confirmar su elección.
7. [Opcional] Desinstale el agente tal como se describe en "Desinstalación de agentes" (p. 73).

Carga de trabajo de la nube a la nube

Para eliminar las cargas de trabajo de las que el agente de la nube haga copias de seguridad, elimine su organización de Microsoft 365 o Google Workspace de la consola de Cyber Protect.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Microsoft 365** o **Dispositivos** > **Google Workspace**.
2. Haga clic en el nombre de su organización de Microsoft 365 o Google Workspace.
3. En el panel **Acciones**, haga clic en **Eliminar grupo**.
4. Haga clic en **Eliminar** para confirmar la acción.

Dispositivo móvil

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione la casilla de verificación junto a la carga de trabajo que quiera eliminar.
3. En el panel **Acciones**, haga clic en **Eliminar**.
4. Haga clic en **Eliminar** para confirmar su elección.
5. [Opcional] Desinstale la aplicación del dispositivo móvil.

Sitio web

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione la casilla de verificación junto a la carga de trabajo que quiera eliminar.
3. En el panel **Acciones**, haga clic en **Eliminar**.
4. Haga clic en **Eliminar** para confirmar su elección.

Tipos de recurso

Tipos de recursos

Icono	Descripción
	Grupo de disponibilidad del agente

© Acronis International GmbH, 2003-2025

Icono	Descripción
	pool de AA
	Almacenamiento en Acronis Backup Gateway
	Acronis cloud
	Libreta de direcciones
	Todos los recursos
	Teléfono Android
	Buzón de correo de archivos comprimidos
	Acronis Storage Node
	Cinta de Acronis Storage Node
	Acronis Secure Zone
	Archivo de audio
	Plan de copias de seguridad
	Plan de réplica de copia de seguridad
	Calendario

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Plan de catalogación
	CD/DVD
	Limpieza de cintas
	Plan de limpieza
	Cloud
	Clúster
	Clúster de procesamiento
	CommuniGate
	Contactos
	Convertir a plan VM
	Cliente
	Centro de datos
	Clúster de base de datos
	Clúster de base de datos activo

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Linux de escritorio
	Windows de escritorio
	Disco
	Dispositivo
	Servidor de recuperación ante desastres
	Grupos dinámicos
	ECP Veil
	Unidad vacía
	Ranura de la unidad vacía
	Archivo cifrado
	Clúster ESX
	ESX temporal
	ESX desconocido
	Evento

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Archivo de Excel
	Clúster de Microsoft Exchange
	Archivo
	Carpeta
	Clientes de carpeta
	Seguidores
	Siguiendo
	Grupo libre
	FTP
	Google
	Google drive
	Grupo
	Clúster Hyper-V
	Hyper-V desconocido

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Archivo de imagen
	Plan de inventario
	iPhone
	Equipo portátil
	Linux en portátil
	Windows en portátil
	Grupo de biblioteca
	Like
	Mac 1
	Mac 2
	Mac air
	Equipo
	Equipo en entorno virtual
	Actualizador de equipos

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Mac mini
	Mac Pro
	Dispositivos
	Mensaje
	Microsoft
	Microsoft 365
	Microsoft Exchange
	Microsoft Exchange office
	Microsoft OneNote
	Archivo de Microsoft OneNote
	Archivo de Microsoft PowerPoint
	Base de datos Microsoft SQL Server
	Grupo de bases de datos Microsoft SQL Server
	Instancia de Microsoft SQL Server

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Microsoft Teams
	Archivo de Microsoft Word
	Mobile
	Dispositivo NAS
	Red compartida
	Cinta de red
	NFS
	Archivo Notary
	Contenedor Odin
	Contenedor Odin (en ejecución)
	Grupo Odin
	Oracle VM
	Socio
	PCS temporal

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Archivo PDF
	Fotografías
	Envío de datos físicos
	Pool
	Grupo de pool
	Postgre SQL
	Publicaciones
	Perfil
	Cinta protegida
	QNAP
	Duplicados de servidor de recuperación
	Motor Red Hat Virtualization (oVirt)
	Recordatorios
	Réplica

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Réplica (en ejecución)
	Grupo de recursos
	Clúster de Scale Computing HC3
	Secuencia de comandos
	Servidor
	Ranura
	Clúster SQL
	Synology
	Tableta
	Tableta Android
	Tableta Apple
	Cinta
	Biblioteca de cintas
	Tarea

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Archivo de texto
	Unidad
	Cuadro desconocido
	Equipo de configuración desconocido
	Pool no reconocido
	Ususario
	Plan de validación
	vCenter Server
	Archivo de vídeo
	Vídeos
	Virtual Appliance
	Aplicación virtual
	Máquina virtual de Azure
	Máquina virtual de Azure (en ejecución)

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Máquina virtual ECP Veil
	Máquina virtual ECP Veil (en ejecución)
	Máquina virtual HCI
	Máquina virtual HCI (en ejecución)
	Máquina virtual Hyper-V
	Máquina virtual Hyper-V (en ejecución)
	Inicio de máquina virtual Hyper-V
	Máquina virtual KVM
	Máquina virtual KVM (en ejecución)
	Máquina virtual Odin
	Máquina virtual Odin (en ejecución)
	Máquina virtual Red Hat Virtualization (oVirt)
	Máquina virtual Red Hat Virtualization (oVirt) (en ejecución)
	Máquina virtual Scale Computing HC3

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Máquina virtual Scale Computing HC3 (en ejecución)
	Réplica de máquina virtual Scale Computing HC3
	Réplica de máquina virtual Scale Computing HC3 (en ejecución)
	Máquina virtual VMware
	Máquina virtual VMware (en ejecución)
	Inicio de máquina virtual VMware
	Plataforma de infraestructuras Virtuozzo
	Máquina virtual y plantillas
	Plan de replicación de máquina virtual
	Sitio web
	Cinta Worm
	Archivo ZIP

Grupos de los dispositivos

Con los grupos de dispositivos, puede proteger varias cargas de trabajo similares con un plan de grupos. El plan se aplica a todo el grupo y no se puede revocar desde un miembro del grupo.

© Acronis International GmbH, 2003-2025

Una carga de trabajo puede ser miembro de más de un grupo. Una carga de trabajo incluida en un grupo de dispositivos también puede estar protegida por planes individuales.

Puede agregar solo cargas de trabajo del mismo tipo a un grupo de dispositivos. Por ejemplo, en **Hyper-V** solo puede crear grupos de equipos virtuales de Hyper-V. En **Equipos con agentes**, solo puede crear grupos de equipos con los agentes instalados.

No se pueden crear grupos de dispositivos en ningún grupo de tipo **Todos**, como el grupo raíz **Todos los dispositivos** ni grupos integrados como **Equipos con agentes** > **Todos**, **Microsoft 365** > su organización > **Usuarios** > **Todos los usuarios**.

Grupos integrados y grupos personalizados

Grupos integrados

Después de registrar una carga de trabajo en la consola de Cyber Protect, aparecerá en uno de los grupos raíz integrados de la pestaña **Dispositivos**, como **Equipos con agentes**, **Microsoft 365** o **Hyper-V**.

Todas las cargas de trabajo que no son de nube a nube registradas también se mostrarán en el grupo raíz **Todos los dispositivos**. Un grupo raíz integrado independiente con el nombre de su inquilino contiene todas las cargas de trabajo que no son de nube a nube y todas las unidades de este inquilino.

No puede eliminar ni editar los grupos raíz ni aplicarles planes.

Algunos de los grupos raíz contienen uno o más niveles de subgrupos integrados; por ejemplo, **Equipos con agentes** > **Todos**, **Microsoft 365** > su organización > **Teams** > **Todos los equipos**, **Google Workspace** > su organización > **Unidades compartidas** > **Todas las unidades compartidas**.

No puede editar ni eliminar los subgrupos integrados.

Grupos personalizados

La protección de todas las cargas de trabajo en un grupo integrado puede que no sea conveniente, ya que podría haber cargas de trabajo que necesiten ajustes de protección diferentes o una planificación de protección diferente.

En algunos de los grupos raíz, por ejemplo en **Equipos con agentes**, **Microsoft 365** o **Google Workspace**, podrá crear subgrupos personalizados. Estos subgrupos pueden ser estáticos o dinámicos.

Puede editar, cambiar el nombre o eliminar cualquier grupo personalizado.

Grupos dinámicos y estáticos

Puede crear el siguiente tipo de grupos personalizados:

© Acronis International GmbH, 2003-2025

- Estático
- Dinámico

Grupos estáticos

Los grupos estáticos contienen cargas de trabajo añadidas manualmente.

El contenido de un grupo estático solo cambia cuando añade o elimina una carga de trabajo de forma explícita.

Ejemplo: Crea un grupo estático para el departamento de contabilidad de su empresa y luego añade manualmente los equipos de los contables a este grupo. Cuando aplica un plan de grupo, los equipos de ese grupo están protegidos. Si se contrata a un nuevo contable, deberá añadir su equipo al grupo estático manualmente.

Grupos dinámicos

Los grupos dinámicos contienen cargas de trabajo que coinciden con criterios específicos. Estos criterios se definen de antemano al crear una consulta de búsqueda que incluye atributos (por ejemplo, `osType`), sus valores (por ejemplo, `Windows`) y operadores de búsqueda (por ejemplo, `IN`).

De este modo, puede crear un grupo dinámico para todos los equipos cuyo sistema operativo sea Windows o un grupo dinámico que contenga todos los usuarios en su organización de Microsoft 365 cuyas direcciones de correo electrónico empiecen por `john`.

Todas las cargas de trabajo que tienen los atributos y valores obligatorios se añaden automáticamente al grupo y cualquier carga de trabajo que pierda uno de dichos atributos o valores se elimina automáticamente del grupo.

Ejemplo 1: Los nombres de servidor host de los equipos que pertenecen al departamento de contabilidad contienen la palabra contabilidad. Usted busca los equipos cuyos nombres contienen contabilidad y luego guarda los resultados de búsqueda como un grupo dinámico. A continuación, aplica un plan de protección al grupo. Si se contrata un nuevo contable, su equipo incluirá contabilidad en el nombre y se añadirá automáticamente al grupo dinámico en cuanto lo registre en la consola de Cyber Protect.

Ejemplo 2: El departamento de contabilidad forma una unidad organizativa de Active Directory independiente. Especifique la unidad organizativa (OU) de contabilidad como un atributo obligatorio y guarde los resultados de la búsqueda como un grupo dinámico. A continuación, aplica un plan de protección al grupo. Si se contrata un nuevo contable, se añadirá el equipo del contable al grupo dinámico en cuanto el mismo se añada a la OU de Active Directory y se registre en la consola de Cyber Protect (lo que ocurra primero).

Grupos de nube a nube y grupos que no son de nube a nube

Los grupos de la nube a la nube contienen cargas de trabajo de Microsoft 365 o Google Workspace de las que un agente de la nube hace copias de seguridad.

Los grupos que no son de nube a nube contienen todos los demás tipos de cargas de trabajo.

© Acronis International GmbH, 2003-2025

Planes compatibles con grupos de dispositivos

La tabla siguiente resume los planes que puede aplicar a un grupo de dispositivos.

Grupo	Planes disponibles	Ubicación del plan
Cargas de trabajo de nube a nube (cargas de trabajo de Microsoft 365 y Google Workspace)	Plan de copias de seguridad	**Gestión** > **Copia de seguridad de aplicaciones en la nube**
Cargas de trabajo que no son de nube a nube	Plan de protección	**Gestión** > **Planes de protección**
	Plan de administración remota	**Gestión** > **Planes de administración remota**
	Plan de programación	**Gestión** > **Planes de programación**

Los recursos de la nube, como los usuarios de Microsoft 365 o Google Workspace, los recursos compartidos de OneDrive y Google Drive, Microsoft Teams o los grupos de Azure AD se sincronizan con la consola de Cyber Protect justo después de añadir una organización de Microsoft 365 o Google Workspace a la consola. El resto de cambios de una organización se sincronizan una vez al día.

Si necesita sincronizar un cambio inmediatamente, en la consola de Cyber Protect, vaya a **Dispositivos** > **Microsoft 365** o **Dispositivos** > **Google Workspace** respectivamente, seleccione la organización que desee y haga clic en **Actualizar**.

Creación de un grupo estático

Puede crear un grupo estático vacío y añadirle cargas de trabajo.

De manera alternativa, puede seleccionar cargas de trabajo y crear un grupo estático nuevo desde su selección.

No se pueden crear grupos de dispositivos en ningún grupo de tipo **Todos**, como el grupo raíz **Todos los dispositivos** ni grupos integrados como **Equipos con agentes** > **Todos**, **Microsoft 365** > su organización > **Usuarios** > **Todos los usuarios**.

Pasos para crear un grupo estático

En la ventana principal

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo raíz que contiene las cargas de trabajo para las que desea crear un grupo estático.
2. [Opcional] Para crear un grupo anidado, vaya a un grupo estático existente.

© Acronis International GmbH, 2003-2025

Nota
La creación de grupos estáticos anidados no está disponible para las cargas de trabajo de nube a nube.

3. Haga clic en **+ Nuevo grupo estático** debajo del árbol de grupos o en **Nuevo grupo estático** en el panel **Acciones**.
4. Especifique un nombre para el nuevo grupo.
5. [Opcional] Añada un comentario para el grupo.
6. Haga clic en **Aceptar**.

En el árbol de grupos

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo raíz que contiene las cargas de trabajo para las que desea crear un grupo estático.
2. Haga clic en el icono de engranaje que hay junto al nombre del grupo en el que desea crear un nuevo grupo estático.

Nota
La creación de grupos estáticos anidados no está disponible para las cargas de trabajo de nube a nube.

3. Haga clic en **Nuevo grupo estático**.
4. Especifique un nombre para el nuevo grupo.
5. [Opcional] Añada un comentario para el grupo.
6. Haga clic en **Aceptar**.

De la selección

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo raíz que contiene las cargas de trabajo para las que desea crear un grupo estático.

Nota
No se pueden crear grupos de dispositivos en ningún grupo de tipo **Todos**, como el grupo raíz **Todos los dispositivos** ni grupos integrados como **Equipos con agentes** > **Todos**, **Microsoft 365** > su organización > **Usuarios** > **Todos los usuarios**.

2. Seleccione las casillas de verificación junto a las cargas de trabajo para las que desea crear un nuevo grupo y, a continuación, haga clic en **Agregar al grupo**.
3. En el árbol de carpetas, seleccione el nivel principal del grupo y haga clic en **Nuevo grupo estático**.

© Acronis International GmbH, 2003-2025

Nota
La creación de grupos estáticos anidados no está disponible para las cargas de trabajo de nube a nube.

4. Especifique un nombre para el nuevo grupo.
5. [Opcional] Añada un comentario para el grupo.
6. Haga clic en **Aceptar**.
   El nuevo grupo aparecerá en el árbol de carpetas.
7. Haga clic en **Listo**.

Añadir cargas de trabajo a un grupo estático

Puede seleccionar el grupo de destino primero y, a continuación, añadir cargas de trabajo a él.

De manera alternativa, puede seleccionar las cargas de trabajo primero y, a continuación, añadirlas a un grupo.

Pasos para añadir cargas de trabajo a un grupo estático

Seleccionar el grupo de destino en primer lugar

1. Haga clic en **Dispositivos** y vaya a su grupo de destino.
2. Seleccione el grupo de destino y haga clic en **Añadir dispositivos**.
3. En el árbol de carpetas, seleccione el grupo que contiene las cargas de trabajo necesarias.
4. Seleccione las casillas de verificación junto a las cargas de trabajo que desea añadir y, a continuación, haga clic en **Agregar**.

Seleccionar cargas de trabajo en primer lugar

1. Haga clic en **Dispositivos** y seleccione el grupo raíz que contiene las cargas de trabajo necesarias.
2. Seleccione las casillas de verificación junto a las cargas de trabajo que desea añadir y, a continuación, haga clic en **Agregar al grupo**.
3. En el árbol de carpetas, seleccione el grupo de destino y haga clic en **Listo**.

Creación de un grupo dinámico

Puede crear un grupo dinámico mediante la búsqueda de cargas de trabajo con atributos específicos cuyos valores defina en una consulta de búsqueda. A continuación, guarde los resultados de la búsqueda como un grupo dinámico.

Los atributos que se admiten para la búsqueda y la creación de grupos dinámicos difieren para los recursos informáticos de nube a nube y los recursos informáticos que no son de nube a nube. Para obtener más información sobre los atributos admitidos, vea "Atributos de búsqueda para cargas de

© Acronis International GmbH, 2003-2025

trabajo que no son de nube a nube" (p. 417) y "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 416).

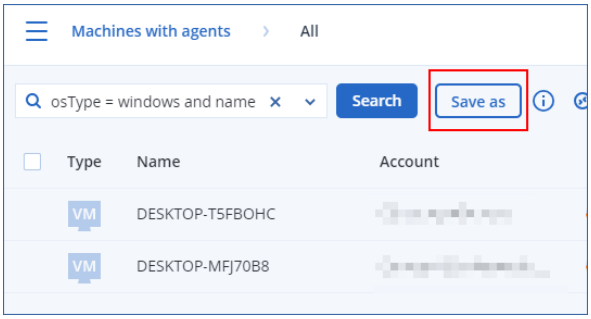
Los grupos dinámicos se crean en sus respectivos grupos raíz. No se admiten grupos dinámicos anidados.

No se pueden crear grupos de dispositivos en ningún grupo de tipo **Todos**, como el grupo raíz **Todos los dispositivos** ni grupos integrados como **Equipos con agentes** > **Todos**, **Microsoft 365** > su organización > **Usuarios** > **Todos los usuarios**.

Pasos para crear un grupo dinámico

Cargas de trabajo que no son de nube a nube

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo que contiene las cargas de trabajo para las que desea crear un nuevo grupo dinámico.
2. Busque las cargas de trabajo con los atributos de búsqueda y operadores compatibles.
   Puede usar múltiples atributos y operadores en una sola consulta. Para obtener más información sobre los atributos admitidos, consulte "Atributos de búsqueda para cargas de trabajo que no son de nube a nube" (p. 417).
3. Haga clic en **Guardar como** junto al campo de búsqueda.



Nota
El botón **Guardar como** no está disponible cuando no se permite crear un grupo dinámico en un nivel específico. Por ejemplo, en el grupo raíz **Dispositivos** > **Todos los dispositivos**.
Seleccione otro nivel (por ejemplo, **Dispositivos** > **Equipos con agentes** > **Todos**), y luego repita los pasos anteriores. Con esta búsqueda, puede crear un grupo dinámico dentro de **Equipos con agentes**, y no dentro de **Equipos con agentes** > **Todos**.

4. Especifique un nombre para el nuevo grupo.
5. [Opcional] En el campo **Comentario**, añada una descripción del nuevo grupo.
6. Haga clic en **Aceptar**.

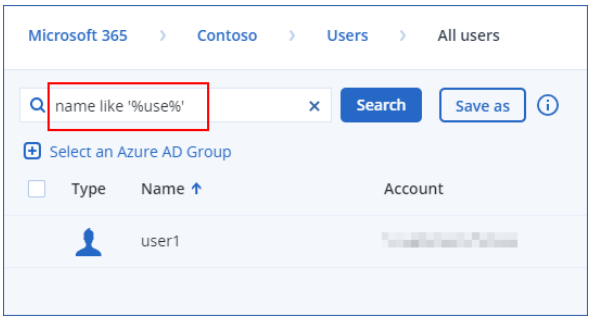
Cargas de trabajo de la nube a la nube

1. Haga clic en **Dispositivos** y, a continuación, seleccione **Microsoft 365** o **Google Workspace**.
2. Seleccione el grupo que contiene los recursos informáticos para los que desea crear un nuevo grupo dinámico. Por ejemplo, **Usuarios** > **Todos los usuarios**.

© Acronis International GmbH, 2003-2025

3. Busque las cargas de trabajo con los atributos de búsqueda y operadores compatibles o mediante la selección de usuarios de Microsoft 365 desde un grupo de Active Directory específico.

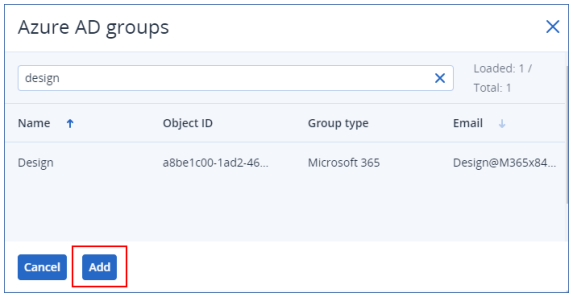
   Puede usar múltiples atributos y operadores en una sola consulta. Para obtener más información sobre los atributos admitidos, consulte "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 416).



4. [Solo para **Microsoft 365** > **Usuarios**] Para seleccionar usuarios de un grupo específico de Active Directory, haga lo siguiente:
   a. Navegue a **Usuarios** > **Todos los usuarios**.
   b. Haga clic en **Seleccionar un grupo de Azure AD**.

      Se abrirá una lista de grupos de Active Directory en su organización.

      En esta lista, puede buscar un grupo específico u ordenar los grupos por nombre o correo electrónico.
   c. Seleccione el grupo de Active Directory que desee y haga clic en **Agregar**.

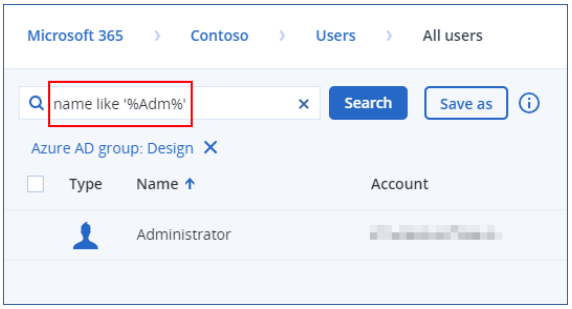


   d. [Opcional] Para incluir o excluir usuarios específicos desde el grupo de Active Directory seleccionado, cree una consulta de búsqueda con atributos y operadores de búsqueda compatibles.

      Puede usar múltiples atributos y operadores en una sola consulta. Para obtener más información sobre los atributos admitidos, consulte "Atributos de búsqueda para cargas de

© Acronis International GmbH, 2003-2025

trabajo de la nube a la nube" (p. 416).



5. Haga clic en **Guardar como** junto al campo de búsqueda.

Nota
El botón **Guardar como** no está disponible cuando no se permite crear un grupo dinámico en un nivel específico. Por ejemplo, en **Microsoft 365** > su organización > **Usuarios**.
Seleccione otro nivel (por ejemplo, **Microsoft 365** > su organización > **Usuarios** > **Todos**), y luego repita los pasos anteriores. Con esta búsqueda, puede crear un grupo dinámico dentro de **Microsoft 365** > su organización > **Usuarios** >, y no dentro de **Usuarios** > **Todos**.

6. Especifique un nombre para el nuevo grupo.
7. [Opcional] En el campo **Comentario**, añada una descripción del nuevo grupo.
8. Haga clic en **Aceptar**.

Operadores de búsqueda

La tabla siguiente resume los operadores que puede usar en sus consultas de búsqueda.

Puede usar más de un operador en una única consulta.

Operador	Compatibilidad con	Significado	Ejemplos
`AND`	Todas las cargas de trabajo	Operador de conjunción lógica	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Todas las cargas de trabajo	Operador de disyunción lógica	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Todas las cargas de trabajo	Operador de negación lógica	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Todas las cargas de trabajo	Este operador comprueba si una expresión se corresponde con algún valor de una lista de ellos.	`osType IN ('windows', 'linux')`

© Acronis International GmbH, 2003-2025

Operador	Compatibilidad con	Significado	Ejemplos
`NOT IN`	Todas las cargas de trabajo	Este operador es el opuesto del operador `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wildcard pattern'`	Todas las cargas de trabajo	Este operador comprueba si una expresión se corresponde con el modelo de comodines.
		Puede utilizar los siguientes operadores comodín:
		• * o % El asterisco y el símbolo de porcentaje representa a ningún carácter, a uno o a varios
		• _ El guion bajo representa un solo carácter
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

`NOT LIKE 'wildcard pattern'`	Todas las cargas de trabajo	Este operador es el opuesto del operador `LIKE`.
		Puede utilizar los siguientes operadores comodín:
		• * o % El asterisco y el símbolo de porcentaje representa a ningún carácter, a uno o a varios
		• _ El guion bajo representa un solo carácter
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

`RANGE (<starting_value>, <ending_value>)`	Todas las cargas de trabajo	Este operador comprueba si una expresión se encuentra dentro de un intervalo de valores.	`ip RANGE ('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Con esta consulta, puede filtrar todos

© Acronis International GmbH, 2003-2025

Operador	Compatibilidad con	Significado	Ejemplos
		Las solicitudes de búsqueda con cadenas alfanuméricas utilizan el orden de clasificación ASCII, pero no distinguen mayúsculas y minúsculas.	los nombres que empiezan por A, B y C, como `Alice`, `Bob` y `Claire`. Sin embargo, solo la letra D cumple los requisitos, por lo que los nombres con más letras, como `Diana` o `Don` no se incluirán. También puede utilizar la siguiente consulta para obtener los mismos resultados: `name >= 'a' AND name <= 'd'`
= o ==	Todas las cargas de trabajo	Operador *Igual que*	`osProductType = 'server'`
!= o <>	Todas las cargas de trabajo	Operador *No es igual que*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	Cargas de trabajo que no son de nube a nube	Operador *Menor que*	`memorySize < 1024`
>	Cargas de trabajo que no son de nube a nube	Operador *Mayor que*.	`diskSize > 300GB`
<=	Cargas de trabajo que no son de nube a nube	Operador *Menor o igual que*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Cargas de trabajo que no son de nube a nube	Operador *Mayor o igual que*	`nextBackupTime >= '2022-08-11'`

Atributos de búsqueda para cargas de trabajo de la nube a la nube

La tabla siguiente resume los atributos que puede usar en sus consultas de búsqueda para cargas de trabajo de Microsoft 365 y Google Workspace.

Para ver qué atributos puede utilizar en las consultas de búsqueda para otros tipos de cargas de trabajo, consulte "Atributos de búsqueda para cargas de trabajo que no son de nube a nube" (p. 417).

© Acronis International GmbH, 2003-2025

Atributo	Significado	Se puede utilizar en	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`name`	Nombre que se muestra de una carga de trabajo de Microsoft 365 o Google Workspace	Todos los recursos de la nube a la nube	`name = 'My Name'` `name LIKE '*nam*'`	Sí

`email`	Dirección de correo electrónico para un usuario o grupo de Microsoft 365 o un usuario de Google Workspace	Microsoft 365 > Grupos
		Microsoft 365 > Usuarios
		Google Workspace > Usuarios
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				Sí

`siteName`	Nombre de un sitio asociado a un grupo de Microsoft 365	Microsoft 365 > Grupos	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Sí
`url`	Dirección web para un grupo de Microsoft 365 o un sitio de SharePoint	Microsoft 365 > Grupos Microsoft 365 > Colecciones de sitios	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Sí

Atributos de búsqueda para cargas de trabajo que no son de nube a nube

La tabla siguiente resume los atributos que puede usar en sus consultas de búsqueda para cargas de trabajo que no son de nube a nube.

Para ver qué atributos puede utilizar en las consultas de búsqueda para cargas de trabajo de la nube a la nube, consulte "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 416).

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
General			
`name`	Nombre de la carga de trabajo, como: • Nombre de host para	`name = 'en-00'`	Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	equipos físicos • Nombre para equipos virtuales • Nombre de la base de datos • Dirección de correo electrónico para buzones de correo		
`id`	ID del dispositivo. Para ver el ID del dispositivo, debajo de **Dispositivos**, seleccione uno, haga clic en **Detalles** > **Todas las propiedades**. El ID aparece en el campo `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sí

`resourceType`	Tipo de carga de trabajo
	Valores posibles:
	• `'machine'`
	• `'exchange'`
	• `'mssql_server'`
	• `'mssql_instance'`
	• `'mssql_database'`
	• `'mssql_database_folder'`
	• `'msexchange_database'`
	• `'msexchange_storage_group'`
	• `'msexchange_mailbox.msexchange'`
	• `'msexchange_mailbox.office365'`
	• `'mssql_aag_group'`
	• `'mssql_aag_database'`
	• `'virtual_machine.vmww'`
	• `'virtual_machine.vmwesx'`
	• `'virtual_host.vmwesx'`
		`resourceType = 'machine'`
		`resourceType in ('virtual_center.vmwesx', 'machine')`
		Nota
		Algunos tipos de recursos, como MS SQL y MS Exchange, pueden considerarse como grupos de recursos. Si su búsqueda o consulta de grupo dinámico no devuelve los resultados esperados, intente agregar el prefijo `group.` al principio del nombre del recurso. Consulte "Tipo de grupo de carga de trabajo" (p. 420).
			Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • virtual_machine.vcd • virtual_machine.ovirt • virtual_machine.azure		

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• `virtual_machine.nutanix` • `'bootable_media'`		

	Tipo de grupo de carga de trabajo
	
	Valores posibles:
	• `group.computers`
	• `group.mssql_server`
	• `group.mssql_instance`
	• `group.mssql_system_databases`
	• `group.mssql_database`
	• `group.mssql_aag_group`
	• `group.mssql_aag_replica`
	• `group.mssql_aag_database`
	• `group.msexchange_cluster`
	• `group.msexchange_server`
	• `group.msexchange_cas`
	• `group.msexchange_online_server`
	• `group.msexchange_infostore`
	• `group.msexchange_storage_group`
	• `group.msexchange_database`
	• `group.msexchange_mailboxes`
	• `group.social_resources`
	• `group.all`
	• `group.all_vcd_vms`
	• `group.vcd`
	• `group.vcenter`
	• `group.ovirt_vengine`
		`resourceType = 'group.mssql_server'`
		
		`resourceType in ('group.mssql_database', 'group.msexchange_database')`
			Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• `group.veil_vengine` • `group.nutanix_vengine` • `group.datacenter` • `group.hosts_and_clusters` • `group.cluster` • `group.host` • `group.virtual_application` • `group.resource_pool` • `group.virtual_folder` • `group.vms_and_templates` • `group.vms_folder` • `group.virtual_project` • `group.nas_devices` • `group.vcd_organization` • `group.vcd_organizations` • `group.azure` • `group.azure_subscriptions` • `group.azure_subscription` • `group.azure_resource_group` • `group.azure_all_devices` • `group.externalrmm` • `group.mail_servers`		
`chassis`	Tipo de chasis. Valores posibles: • `laptop` • `desktop` • `server` • `other` • `unknown`	`chassis = 'laptop'` `chassis IN ('laptop', 'desktop')`	Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`ip`	Dirección IP (solo para equipos físicos).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Sí

`comment`	Comentario dirigido a un dispositivo. Se puede especificar automática o manualmente.
	Valor predeterminado:
	• La descripción del equipo en Windows se copia automáticamente como un comentario para equipos físicos que ejecutan Windows. Este valor se sincroniza cada 15 minutos.
	• Vacío para otros dispositivos.
	Nota
	La sincronización automática se deshabilita si se ha añadido texto manualmente en el campo de comentarios. Para volver a habilitar la sincronización, borre el texto.
	Para actualizar los comentarios sincronizados automáticamente de sus cargas de trabajo, reinicie Acronis Managed Machine Service en **Windows Services** o ejecute los siguientes comandos en el símbolo del sistema:
	`net stop mms`
	`net start mms`
		`comment = 'important machine'`
		`comment = ''` (todos los equipos sin ningún comentario)
			Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos

	Para ver un comentario de dispositivo, en **Dispositivos**, seleccione el dispositivo, haga clic en **Detalles** y busque la sección **Comentario**.
	
	Para añadir un comentario o modificarlo de forma manual, haga clic en **Agregar** o **Editar**.
	
	Los dispositivos en los que está instalado un agente de protección tienen dos campos de comentarios independientes:
	
	• Comentario del agente
	  ◦ La descripción del equipo en Windows se copia automáticamente como un comentario para equipos físicos que ejecutan Windows. Este valor se sincroniza cada 15 minutos.
	  ◦ Vacío para otros dispositivos.
	
	Nota
	La sincronización automática se deshabilita si se ha añadido texto manualmente en el campo de comentarios. Para volver a habilitar la sincronización, borre el texto.
	
	• Comentario del		

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	dispositivo ◦ Si el comentario del agente se especifica automáticamente, se copia como comentario del dispositivo. Los comentarios del agente que se añaden manualmente no se copian como comentarios del dispositivo. ◦ Los comentarios del dispositivo no se copian como comentarios del agente. Un dispositivo puede tener uno o ambos comentarios especificados o tener ambos en blanco. Si se especifican ambos comentarios, el comentario del dispositivo tiene prioridad. Para ver un comentario del agente, en **Configuración** > **Agentes**, seleccione el dispositivo con el agente, haga clic en **Detalles** y busque la sección **Comentario**. Para ver un comentario de dispositivo, en **Dispositivos**, seleccione el dispositivo, haga clic en **Detalles** y busque la sección **Comentario**. Para añadir un comentario		

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	o modificarlo de forma manual, haga clic en **Agregar** o **Editar**.		
`isOnline`	Disponibilidad de la carga de trabajo. Valores posibles: • `true` • `false`	`isOnline = true`	No
`hasAsz`	Disponibilidad Secure Zone. Valores posibles: • `true` • `false`	`hasAsz = true`	Sí

`tzOffset`	Desplazamiento de la zona horaria del tiempo universal coordinado (UTC), en minutos.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Sí

CPU, memoria, discos			
`cpuArch`	Arquitectura de CPU. Valores posibles: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Sí
`cpuName`	Nombre de CPU.	`cpuName LIKE '%XEON%'`	Sí
`memorySize`	Tamaño de la RAM en megabytes.	`memorySize < 1024`	Sí
`diskSize`	Tamaño del disco duro en gigabytes o megabytes (solo para equipos físicos).	`diskSize < 300GB` `diskSize >= 3000000MB`	No
Sistema operativo			
`osName`	Nombre del sistema operativo.	`osName LIKE '%Windows XP%'`	Sí
`osType`	Tipo de sistema operativo.	`osType = 'windows'`	Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	Valores posibles: • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	
`osArch`	Arquitectura del sistema operativo. Valores posibles: • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Sí
`osProductType`	Tipo de producto de sistema operativo. Valores posibles: • `'dc'` Significa controlador de dominio. **Nota** Cuando el rol de controlador de dominio se asigna a un servidor Windows, el `osProductType` cambia de `server` a `dc`. Esos equipos no se incluirán en los resultados de búsqueda de `osProductType='server'`. • `'server'` • `'workstation'`	`osProductType = 'server'`	Sí
`osSp`	Paquete de servicio del sistema operativo.	`osSp = 1`	Sí
`osVersionMajor`	Versión principal del sistema operativo.	`osVersionMajor = 1`	Sí
`osVersionMinor`	Versión menor del sistema operativo.	`osVersionMinor > 1`	Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
Agente			
`agentVersion`	Versión del agente de protección instalado.	`agentVersion LIKE '12.0.*'`	Sí
`hostId`	ID interno del agente de protección. Para ver el ID del agente de protección, en **Dispositivos**, seleccione uno, haga clic en **Detalles** > **Todas las propiedades**. Compruebe el valor `id` de la propiedad `agent`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sí
`virtualType`	Tipo de máquina virtual. Valores posibles: • `'vmwesx'` Equipos virtuales VMware • `'mshyperv'` Equipos virtuales Hyper-V • `'pcs'` Equipos virtuales Virtuozzo • `'hci'` Equipos virtuales de la Virtuozzo Hybrid Infrastructure • `'scale'` Equipos virtuales de Scale Computing HC3 • `'ovirt'` Máquinas virtuales oVirt • `'vcd'` Equipos virtuales de VMware Cloud Director	`virtualType = 'vmwesx'`	Sí
`insideVm`	Equipo virtual con un agente dentro.	`insideVm = true`	Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	Valores posibles: • `true` • `false`		
Ubicación			
`tenant`	El nombre del inquilino al que pertenece el dispositivo.	`tenant = 'Unit 1'`	Sí
`tenantId`	El identificador del inquilino al que pertenece el dispositivo. Para ver el ID del inquilino, debajo de **Dispositivos**, seleccione uno, haga clic en **Detalles** > **Todas las propiedades**. El ID aparece en el campo `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Sí
`ou`	Dispositivos que pertenecen a la unidad organizativa de Active Directory.	`ou IN ('RnD', 'Computers')`	Sí
`customerUuid`	Dispositivos que pertenecen al ID de inquilino del **Cliente** especificado.	`customerUuid = 'd96c5dde-5466-489d-9c74-df7dbd8c2148'`	No
Estado			
`state`	Estado del dispositivo. Valores posibles: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'`	`state = 'backup'`	No

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	Estado de la protección. Valores posibles: • ok • warning • error • critical • protected • notProtected	status = 'ok' status IN ('error', 'warning')	No
protectedByPlan	Dispositivos que están protegidos por un plan de protección con un ID determinado. Para ver el ID del plan, en **Gestión** > **Planes de protección**, seleccione un plan, Haga clic en la barra de la columna **Estado** y, a continuación, en el nombre del estado. Se creará una nueva búsqueda con el ID del plan.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
okByPlan	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **OK**.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
errorByPlan	Dispositivos que están protegidos por un plan de protección con un ID	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	determinado y tienen el estado **Error**.		
`warningByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Advertencia**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`runningByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **En ejecución**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`interactionByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Interacción necesaria**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No

`lastBackupTime*`	La fecha y la hora de la última copia de seguridad realizada correctamente.
	El formato es `"AAAA-MM-DD HH:MM"`.
		`lastBackupTime > '2023-03-11'`
		`lastBackupTime <= '2023-03-11 00:15'`
		`lastBackupTime is null`
			No

`lastBackupTryTime*`	La hora del último intento de realización de la copia de seguridad. El formato es `"AAAA-MM-DD HH:MM"`.	`lastBackupTryTime >= '2023-03-11'`	No
`nextBackupTime*`	La hora de la siguiente copia de seguridad. El formato es `"AAAA-MM-DD HH:MM"`.	`nextBackupTime >= '2023-08-11'`	No

`lastVAScanTime*`	La fecha y la hora de la última evaluación de vulnerabilidades realizada correctamente.	`lastVAScanTime > '2023-03-11'`
		`lastVAScanTime <= '2023-03-11 00:15'`
		`lastVAScanTime is null`
			Sí

© Acronis International GmbH, 2003-2025

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	El formato es `"AAAA-MM-DD HH:MM"`.		
`lastVAScanTryTime*`	La hora del último intento de realización de la evaluación de vulnerabilidades. El formato es `"AAAA-MM-DD HH:MM"`.	`lastVAScanTimeTryTime >= '2022-03-11'`	Sí
`nextVAScanTime*`	La hora de la siguiente evaluación de vulnerabilidades. El formato es `"AAAA-MM-DD HH:MM"`.	`nextVAScanTime <= '2023-08-11'`	Sí
`network_status`	Estado del aislamiento de red para Endpoint detection and response (EDR). Valores posibles: • `connected` • `isolated`	`network_status= 'connected'`	Sí

Nota

Si omite el valor de horas y minutos, la hora de inicio se tomará como AAAA-MM-DD 00:00 y la hora de finalización como AAAA-MM-DD 23:59:59. Por ejemplo, `lastBackupTime = 2023-01-20` significa que los resultados de búsqueda incluirán todas las copias de seguridad en el intervalo entre `lastBackupTime >= 2023-01-20 00:00` y `lastBackupTime <= 2023-01-20 23:59:59`.

Edición de un grupo dinámico

Edite un grupo dinámico mediante el cambio de la consulta de búsqueda que define el contenido del grupo.

En los grupos dinámicos que se basan en Active Directory, también puede cambiar el grupo de Active Directory.

Pasos para editar un grupo dinámico

Mediante el cambio de la consulta de búsqueda

© Acronis International GmbH, 2003-2025

1. Haga clic en **Dispositivos** y vaya al grupo dinámico que desee editar y selecciónelo.
2. Haga clic en el icono de engranaje situado junto al nombre del grupo y, a continuación, haga clic en **Editar**. De forma alternativa, haga clic en **Editar** en el panel **Acciones**.
3. Cambie la consulta de búsqueda modificando los atributos de búsqueda, sus valores o los operadores de búsqueda, y haga clic en **Buscar**.
4. Haga clic en **Guardar** junto al campo de búsqueda.

Mediante el cambio del grupo de Active Directory

Nota
Este procedimiento se aplica a grupos dinámicos basados en Active Directory. Los grupos dinámicos basados en Active Directory solo están disponibles en **Microsoft 365** > **Usuarios**.

1. Haga clic en **Dispositivos**, vaya a **Dispositivos** > **Microsoft 365** > su organización > **Usuarios**.
2. Seleccione el grupo dinámico que desee editar.
3. Haga clic en el icono de engranaje situado junto al nombre del grupo y, a continuación, haga clic en **Editar**. De forma alternativa, haga clic en **Editar** en el panel **Acciones**.
4. Cambie el contenido del grupo mediante una de las siguientes operaciones:
   - Cambie el grupo de Active Directory que ya ha seleccionado haciendo clic en su nombre y, a continuación, seleccione un nuevo grupo de Active Directory de la lista que se abra.
   - Edite la consulta de búsqueda y haga clic en **Buscar**.
     La consulta de búsqueda está limitada al grupo de Active Directory seleccionado actualmente.
5. Haga clic en **Guardar** junto al campo de búsqueda.

También puede guarde los cambios sin sobrescribir el grupo actual. Para guardar la configuración editada como un grupo nuevo, haga clic en el botón de la flecha que hay junto al campo de búsqueda y, a continuación en **Guardar como**.

Nota
Los grupos que se crean utilizando la opción **Guardar como** heredan los criterios de descubrimiento del grupo dinámico original. Por lo tanto, los nuevos criterios de descubrimiento que configure se añaden a los criterios heredados y se guardan en el nuevo grupo dinámico.

Solo los grupos creados a partir de la categoría de grupo **Todos** no heredan criterios.

Eliminar un grupo

Cuando elimine un grupo de dispositivos, todos los planes aplicados al grupo se revocarán. Las cargas de trabajo del grupo dejarán de estar protegidas si no se aplican otros planes a ellas.

Pasos para eliminar un grupo de dispositivos

1. Haga clic en **Dispositivos** y vaya al grupo que desee eliminar.
2. Haga clic en el icono de engranaje situado junto al nombre del grupo y, a continuación, haga clic

© Acronis International GmbH, 2003-2025

en **Eliminar**.

3. Haga clic en **Eliminar** para confirmar su elección.

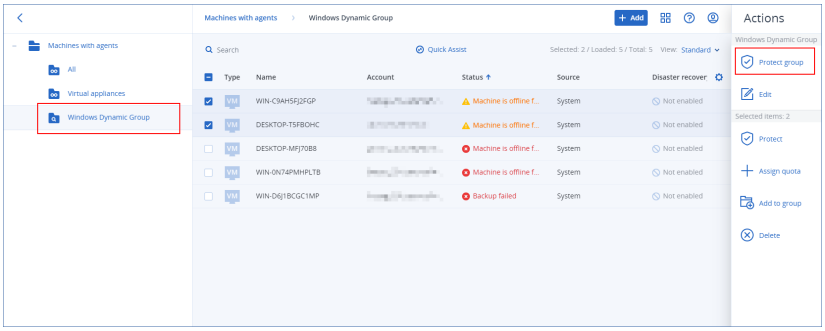
Aplicar un plan a un grupo

Puede aplicar un plan a un grupo mediante la selección del grupo primero y la asignación de un plan a este.

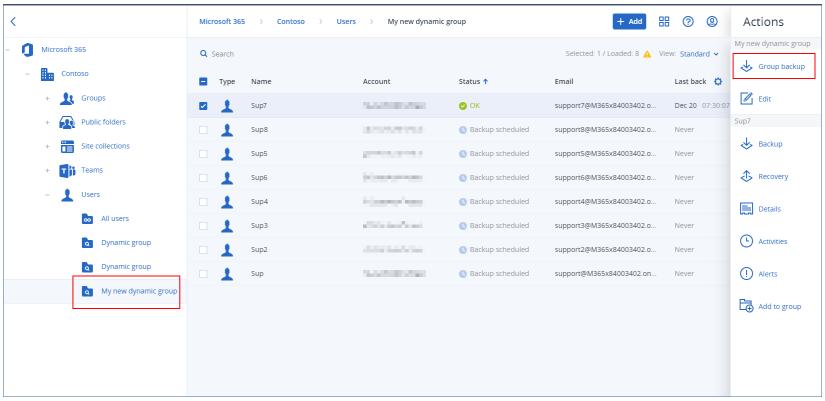
De manera alternativa, puede abrir el plan para editarlo y después añadir un grupo a este.

Pasos para aplicar un plan a un grupo

1. Haga clic en **Dispositivos** y vaya al grupo al que quiera aplicar un plan.
2. [Para cargas de trabajo que no son de nube a nube] Haga clic en **Proteger grupo**.



   Se mostrará una lista de planes que pueden aplicarse.
3. [Para cargas de trabajo de la nube a la nube] Haga clic en **Agrupar copia de seguridad**.



   Se mostrará una lista de planes de copia de seguridad que pueden aplicarse.
4. [Para aplicar un plan existente] Seleccione el plan y haga clic en **Aplicar**.
5. [Para crear un plan nuevo] Haga clic en **Crear plan**, seleccione el tipo de plan y cree el nuevo plan.

   Para obtener más información sobre los tipos de planes disponibles y cómo crearlos, consulte "Planes compatibles con grupos de dispositivos" (p. 409).

© Acronis International GmbH, 2003-2025

Nota
Los planes de copias de seguridad que se aplican a los grupos de dispositivos de la nube a la nube se programan automáticamente para ejecutarse una vez al día. No puede ejecutar estos planes bajo demanda haciendo clic en **Ejecutar ahora**.

Revocación de un plan desde un grupo

Puede revocar un plan desde un grupo mediante la selección del grupo primero y la revocación del plan desde este.

De manera alternativa, puede abrir el plan para editarlo y después eliminar el grupo de este.

Pasos para revocar un plan desde un grupo

1. Haga clic en **Dispositivos** y vaya al grupo desde el que quiera revocar un plan.
2. [Para cargas de trabajo que no son de nube a nube] Haga clic en **Proteger grupo**.
   Se mostrará una lista de planes que están aplicados al grupo.
3. [Para cargas de trabajo de la nube a la nube] Haga clic en **Agrupar copia de seguridad**.
   Se mostrará una lista de planes de copias de seguridad que están aplicados al grupo.
4. Seleccione el plan que desea revocar.
5. [Para cargas de trabajo que no son de nube a nube] Haga clic en el icono de puntos suspensivos (...) y haga clic en **Revocar**.
6. [Para cargas de trabajo de la nube a la nube] Haga clic en el icono de engranaje y, a continuación, haga clic en **Revocar**.

Cómo trabajar con el módulo de control de dispositivos

Como parte de los planes de protección del servicio Cyber Protection, el módulo de control de dispositivos[1] aprovecha un subconjunto funcional del agente de prevención de pérdida de datos[2] de cada equipo protegido para detectar y evitar el acceso no autorizado y la transmisión de datos

[1]Como parte de un plan de protección, el módulo de control de dispositivos aprovecha un subconjunto funcional del agente de prevención de pérdida de datos de cada equipo protegido para detectar y evitar el acceso no autorizado y la transmisión de datos en los canales del equipo local. Esto incluye el acceso de usuario a dispositivos y puertos periféricos, la impresión de documentos, las operaciones de copiar y pegar del portapapeles, el formato de medios y las operaciones de extracción, así como la sincronización con dispositivos móviles conectados de manera local. El módulo del control de dispositivos proporciona control granular y contextual sobre los tipos de dispositivos y los puertos a los que los usuarios tienen acceso en el equipo protegido y las acciones que los usuarios pueden llevar a cabo sobre los dispositivos.
[2]Un componente de cliente del sistema de prevención de pérdida de datos que protege al equipo servidor del acceso no autorizado, la transmisión y el almacenamiento de datos confidenciales, protegidos o sensibles al aplicar una combinación de técnicas de análisis de contenido y contexto y políticas de prevención de pérdida de datos administradas de forma centralizada. Cyber Protection proporciona un agente para la prevención de pérdida de datos con todas las funciones. Sin embargo, la funcionalidad del agente en un equipo protegido se limita al conjunto de funciones de prevención de pérdida de datos disponibles para las licencias de Cyber Protection y depende del plan de protección que se aplique al equipo.

© Acronis International GmbH, 2003-2025

en los canales del equipo local. Proporciona un control detallado sobre una amplia gama de vías de fuga de datos, incluido el intercambio de datos mediante dispositivos extraíbles, impresoras, dispositivos virtuales y redirigidos y el portapapeles de Windows.

El módulo está disponible parar las ediciones Cyber Protect Essentials, Cyber Protect Standard y Cyber Protect Advanced con licencias por carga de trabajo.

Nota

En equipos Windows, las características del control de dispositivos requieren la instalación del agente de prevención de pérdida de datos. Se instalará automáticamente para las cargas de trabajo protegidas si el módulo de **Control de dispositivos** está habilitado en sus planes de protección.

El módulo de control de dispositivos se basa en las funciones de prevención de pérdida de datos[1] del agente para ejercer control contextual sobre las operaciones de acceso y traspaso de datos en el equipo protegido. Esto incluye el acceso de usuario a dispositivos y puertos periféricos, la impresión de documentos, las operaciones de copiar y pegar del portapapeles, el formato de medios y las operaciones de extracción, así como la sincronización con dispositivos móviles conectados de manera local. El agente de prevención de pérdida de datos incluye un marco para todos los componentes de la gestión y administración central del módulo de control de dispositivos y, por lo tanto, se deberá instalar en los equipos que se protejan con el módulo de control de dispositivos. El agente permite, restringe o deniega las acciones de usuario según la configuración del control de dispositivos que recibe del plan de protección que se aplica al equipo protegido.

El módulo de control de dispositivos controla el acceso a varios dispositivos periféricos, tanto si se usan directamente en equipos protegidos o si se redirigen a entornos de virtualización alojados en equipos protegidos. Reconoce dispositivos redirigidos al escritorio remoto de Windows Server, Citrix XenDesktop / XenApp / XenServer y VMware Horizon. También puede controlar las operaciones de copia de datos entre el portapapeles del sistema operativo invitado que se ejecuta en VMware Workstation/Player, Oracle VM VirtualBox o Windows Virtual PC, y el portapapeles del sistema operativo anfitrión que se ejecute en el equipo protegido.

El módulo de control de dispositivos puede proteger equipos que ejecutan estos sistemas operativos:

Control de dispositivos

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 – Windows Server 2022
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)

[1] Un sistema de tecnologías integradas y medidas organizativas destinado a detectar y evitar la divulgación o el acceso accidental o intencional a datos confidenciales, protegidos o sensibles por parte de entidades no autorizadas de fuera o dentro de la organización, o la transferencia de tales datos a entornos que no son de confianza.

© Acronis International GmbH, 2003-2025

- macOS 13 (Ventura)
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)

Nota
El Agente para la prevención de pérdida de datos para macOS solo es compatible con procesadores x64. Los procesadores basados en ARM de Apple Silicon no son compatibles.

Prevención de pérdida de datos

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 – Windows Server 2022

Nota
El Agente para la prevención de pérdida de datos podría estar instalado en sistemas macOS no compatibles porque es una parte integral del Agente para Mac. En ese caso, la consola de Cyber Protect mostrará que el Agente para la prevención de pérdida de datos está instalado en el ordenador, pero la función de control del dispositivos y de prevención de pérdida de datos no funcionará. La función de control de dispositivos solo funcionará en sistemas macOS compatibles con el Agente para la prevención de pérdida de datos.

Limitación del uso del agente para la prevención de la pérdida de datos con Hyper-V

No instale el agente para la prevención de la pérdida de datos en hosts de Hyper-V en clústeres de Hyper-V porque podría causar problemas cuando los empleados usen sus equipos, principalmente en clústeres de Hyper-V con volúmenes compartidos en clúster (CSV).

Si utiliza alguna de las siguientes versiones del agente para Hyper-V, debe eliminar manualmente el agente para la prevención de la pérdida de datos:

- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

Para eliminar el agente para la prevención de la pérdida de datos, en el servidor Hyper-V, ejecute el programa de instalación manualmente y desmarque la casilla de verificación del agente para la prevención de la pérdida de datos o ejecute el siguiente comando:

```
<installer_name> --remove-components=agentForDlp -quiet
```


© Acronis International GmbH, 2003-2025

Puede habilitar y configurar el módulo de control de dispositivos en la sección **Control de dispositivos** de su plan de protección en la consola de Cyber Protect. Para obtener instrucciones, consulte Cómo habilitar o deshabilitar el control de dispositivos.

La sección **Control de dispositivos** muestra un resumen de la configuración del módulo:



- Configuración del acceso: Muestra un resumen de los tipos de dispositivo y puertos con acceso restringido (denegado o de solo lectura), si los hay. De lo contrario, indica que se permiten todos los tipos de dispositivo. Haga clic en este resumen para ver o cambiar la configuración del acceso (consulte cómo ver o cambiar la configuración del acceso).
- Lista de tipos de dispositivo permitidos: Muestra cuántas subclases de dispositivo se permiten al excluirlos del control del acceso del dispositivo, si corresponde. De lo contrario, indica que la lista blanca está vacía. Haga clic en este resumen para ver o cambiar la selección de subclases de dispositivo permitidas (consulte cómo excluir subclases de dispositivo del control de acceso).
- Lista de dispositivos USB permitidos: Muestra cuántos modelos o dispositivos USB se permiten al excluirlos del control del acceso del dispositivo, si corresponde. De lo contrario, indica que la lista blanca está vacía. Haga clic en este resumen para ver o cambiar la lista de dispositivos o modelos USB permitidos (consulte cómo excluir dispositivos USB individuales del control de acceso).
- Exclusiones: Muestra cuántas exclusiones de control de acceso se han establecido para el portapapeles de Windows, las capturas de pantalla, las impresoras y los dispositivos móviles.

Uso del control de dispositivos

Esta sección incluye las instrucciones paso a paso para tareas básicas cuando se utiliza el módulo de control de dispositivos.

Habilitar o deshabilitar el control de dispositivos

Puede habilitar el control de dispositivos al crear un plan de protección. Puede cambiar un plan de protección existente para habilitar o deshabilitar el control de dispositivos.

Para habilitar o deshabilitar el control de dispositivos

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Realice uno de los siguientes procedimientos para abrir el panel del plan de protección:
   - Si va a crear un nuevo plan de protección, seleccione un equipo para proteger, haga clic en **Proteger** y, a continuación, haga clic en **Crear plan**.
   - Si va a cambiar un plan de protección existente, seleccione un equipo protegido, haga clic en **Proteger**, haga clic en el icono de puntos suspensivos (...) junto al nombre del plan de protección y, a continuación, haga clic en **Editar**.
3. En el panel del plan de protección, vaya al área de **control de dispositivos** y habilite o deshabilite el **control de dispositivos**.
4. Realice uno de los siguientes procedimientos para aplicar los cambios:
   - Para crear un plan de protección, haga clic en **Crear**.
   - Para editar un plan de protección, haga clic en **Guardar**.

También puede acceder al plan de protección desde la pestaña Administración. Sin embargo, esta opción no está disponible en todas las ediciones del servicio Cyber Protection.

Habilitación del uso del módulo de control de dispositivos en macOS

La configuración del control de dispositivos de un plan de protección es efectiva solo después de cargar el controlador del control de dispositivos en la carga de trabajo protegida. Esta sección describe cómo cargar el controlador del control de dispositivos para habilitar el uso del módulo de control de dispositivos en macOS. Es una operación única que requiere privilegios del administrador en el equipo de endpoint.

Versiones de macOS compatibles:

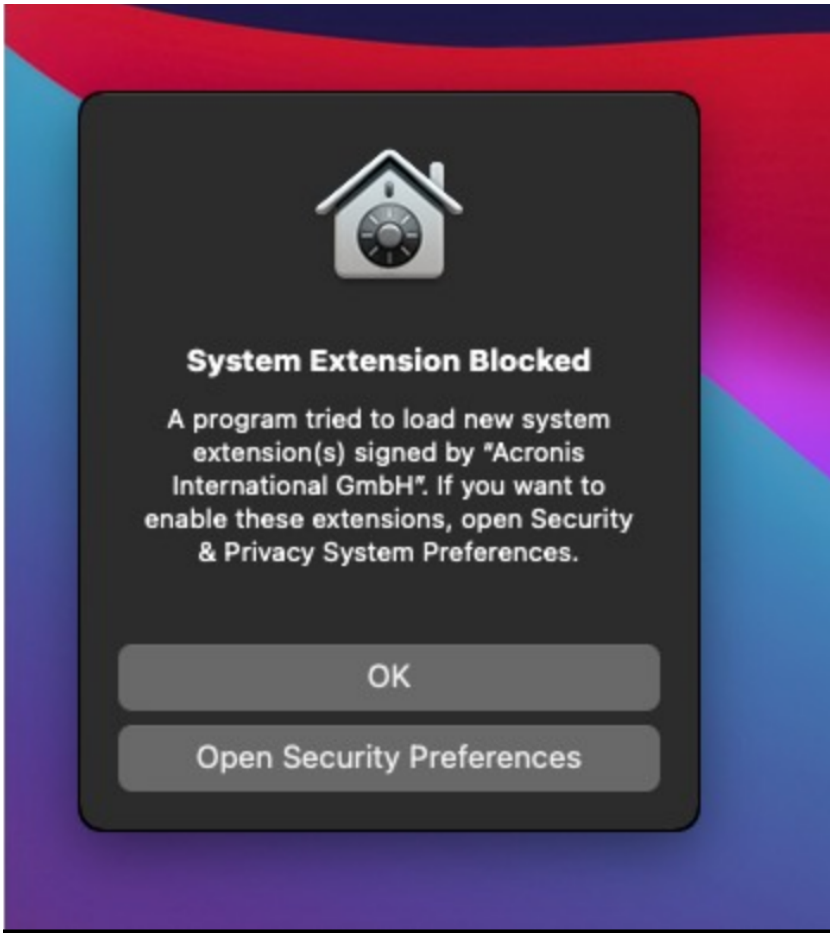
- macOS 10.15 (Catalina) y posterior
- macOS 11.2.3 (Big Sur) y posterior
- macOS 12.2 (Monterey) y posterior
- macOS 13.2 (Ventura) y posterior
- macOS 14 (Sonoma) y versiones posteriores
- macOS 15 (Sequoia) y versiones posteriores

Pasos para habilitar el uso del módulo de control de dispositivos en macOS

1. Instale el Agente para Mac en el equipo que desea proteger.
2. Habilite la configuración del control de dispositivos en el plan de protección.
3. Aplique el plan de protección.

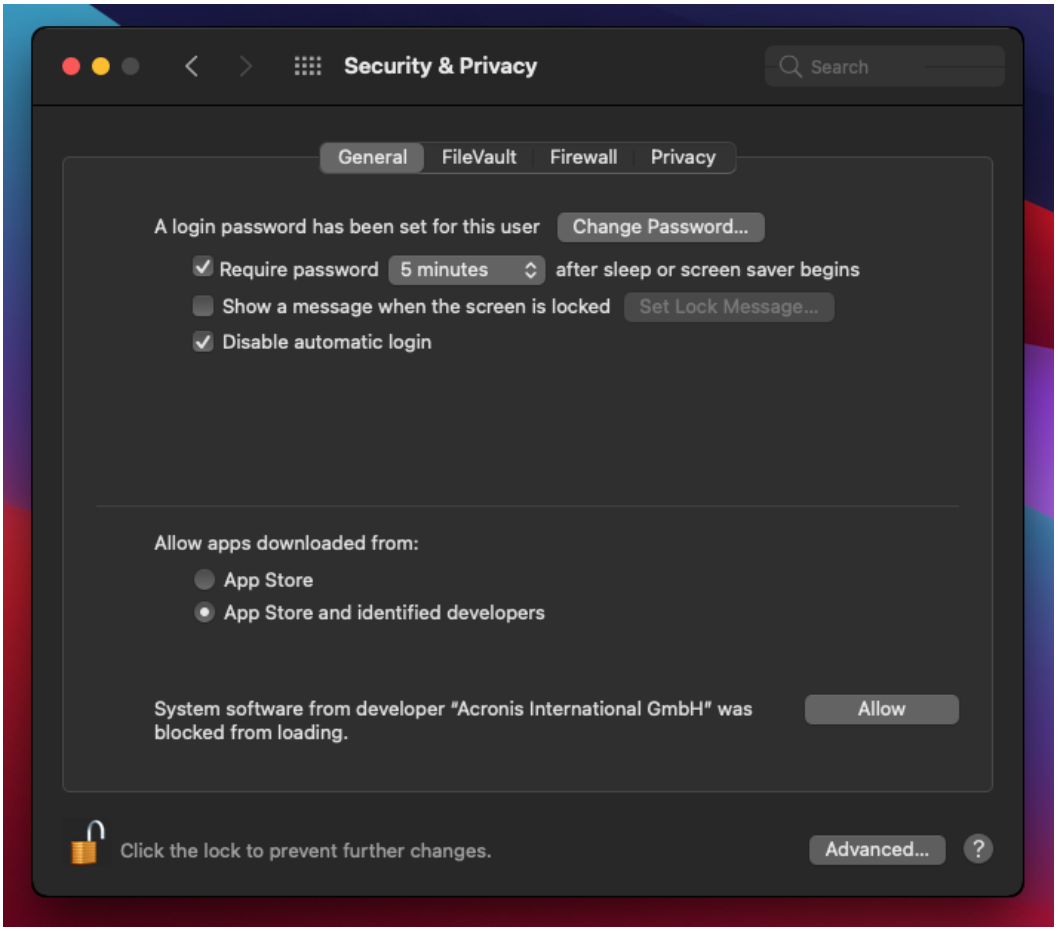
© Acronis International GmbH, 2003-2025

4. Aparecerá la advertencia "Extensión del sistema bloqueada" en la carga de trabajo protegida. Haga clic en **Abrir preferencias de seguridad**.



© Acronis International GmbH, 2003-2025

5. En el panel **Seguridad y privacidad** que aparece, seleccione **App Store y desarrolladores identificados** y haga clic en **Permitir**.



6. En el cuadro de diálogo que aparece, haga clic en **Reiniciar** para reiniciar la carga de trabajo y activar la configuración del control de dispositivos.

Nota
No tiene que repetir estos pasos si ha deshabilitado y vuelto a habilitar la configuración del control de dispositivos.

Ver o cambiar la configuración del acceso

En el panel del plan de protección, puede administrar la configuración del acceso del módulo de control del dispositivo. De esta forma, puede permitir o denegar el acceso a determinados tipos de dispositivos, así como habilitar o deshabilitar notificaciones y alertas.

Para ver o cambiar la configuración del acceso

1. Abra el panel del plan de protección para un plan de protección y habilite el control de dispositivos en dicho plan (consulte Cómo habilitar o deshabilitar el control de dispositivos).
2. Haga clic en el icono de la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en el enlace junto a **Configuración del acceso**.

© Acronis International GmbH, 2003-2025

3. En la página para administrar la configuración del acceso, consulte o cambie la configuración del acceso como convenga.

Nota
Los ajustes de acceso configurados en el control del dispositivo pueden ser anulados cuando se utilizan tanto el control del dispositivo como Advanced DLP para proteger un recurso informático. Cosulte "Habilitar Advanced Data Loss Prevention en los planes de protección" (p. 1228).

Habilitar o deshabilitar las notificaciones del sistema operativo y alertas del servicio

Cuando gestione la configuración del acceso, puede habilitar o deshabilitar las notificaciones del sistema operativo y alertas del servicio que informan de los intentos de usuario de llevar a cabo acciones que no están permitidas.

Para habilitar o deshabilitar las notificaciones del sistema operativo

1. Siga los pasos que se incluyen en cómo ver o cambiar la configuración del acceso.
2. En la página para gestionar la configuración del acceso, seleccione o elimine la casilla de verificación **Mostrar notificaciones del sistema operativo a los usuarios finales si intentan utilizar un tipo de dispositivo o puerto bloqueados**.

Para habilitar o deshabilitar las alertas del servicio

1. Siga los pasos que se incluyen en cómo ver o cambiar la configuración del acceso.
2. En la página para gestionar la configuración del acceso, seleccione o elimine la casilla de verificación **Mostrar alerta** en los tipos de dispositivo que desee.

La casilla de verificación **Mostrar alerta** solo estará disponible para los tipos de dispositivo con acceso restringido (solo lectura o acceso denegado), excepto para las capturas de pantalla.

Excluir subclases de dispositivo del control de acceso

En el panel del plan de protección, puede escoger las subclases de dispositivos que desea excluir del control de acceso. Como resultado, se permitirá el acceso a dichos dispositivos independientemente de la configuración del acceso de control de dispositivos.

Para excluir subclases de dispositivo del control de acceso

1. Abra el panel del plan de protección para un plan de protección y habilite el control de dispositivos en dicho plan (consulte Cómo habilitar o deshabilitar el control de dispositivos).
2. Haga clic en el icono de la flecha junto al conmutador del **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en el enlace junto a **Lista de tipos de dispositivo permitidos**.
3. En la página para administrar la lista blanca, consulte o cambie la selección de subclases de dispositivos para excluirlas del control de acceso.

© Acronis International GmbH, 2003-2025

Excluir dispositivos USB individuales del control de acceso

En el panel del plan de protección, puede especificar los dispositivos USB o los modelos de dispositivos USB individuales que desea excluir del control de acceso. Como resultado, se permitirá el acceso a dichos dispositivos independientemente de la configuración del acceso de control de dispositivos.

Para excluir un dispositivo USB del control de acceso

1. Abra el panel del plan de protección para un plan de protección y habilite el control de dispositivos en dicho plan (consulte Cómo habilitar o deshabilitar el control de dispositivos).
2. Haga clic en el icono de la flecha junto al conmutador del **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en el enlace junto a **Lista de dispositivos USB permitidos**.
3. En la página para administrar la lista de permitidos, haga clic en **Añadir desde la base de datos**.
4. En la página para seleccionar dispositivos USB, seleccione los dispositivos que desee de entre los registrados en la Base de datos de dispositivos USB.
5. Haga clic en el botón **Añadir a la lista de permitidos**.

Para dejar de excluir un dispositivo USB del control de acceso

1. Abra el panel del plan de protección para un plan de protección y habilite el control de dispositivos en dicho plan (consulte Cómo habilitar o deshabilitar el control de dispositivos).
2. Haga clic en el icono de la flecha junto al conmutador del **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en el enlace junto a **Lista de dispositivos USB permitidos**.
3. En la página para administrar la lista de permitidos, haga clic en el icono de eliminar al final del elemento de la lista que representa el dispositivo USB deseado.

Agregar o eliminar dispositivos USB de la base de datos

Para excluir un dispositivo USB específico del control de acceso, debe añadirlo a la Base de datos de dispositivos USB. Entonces podrá añadir dispositivos a la lista blanca seleccionándolos en la base de datos.

Los siguientes procedimientos se aplican a los planes de protección que tienen habilitada la función de control del dispositivo.

Pasos para añadir dispositivos USB a la base de datos

1. Abra el plan de protección de un dispositivo para editarlo:
   Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.

© Acronis International GmbH, 2003-2025

Nota
Debe habilitar el control de dispositivos en el plan para acceder a la configuración del control de dispositivos.

2. Haga clic en el icono de la flecha junto al conmutador del **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en el enlace junto a **Lista de dispositivos USB permitidos**.
3. En la página **Lista de dispositivos USB permitidos**, haga clic en **Añadir desde la base de datos**.
4. En la página para administrar la base de datos de dispositivos USB, haga clic en **Añadir a la base de datos**.
5. En el cuadro de diálogo **Agregar dispositivo USB** que aparece, haga clic en la máquina a la que se conecta el dispositivo USB.
   En la lista de equipos solo se muestran las máquinas que están en línea.
   La lista de dispositivos USB solo se muestra en las máquinas que tienen instalado el agente para la Prevención de pérdida de datos.
   Los dispositivos USB se muestran en la vista de árbol. El primer nivel del árbol representa un modelo de dispositivo. El segundo nivel representa un dispositivo específico de ese modelo.
   Un icono azul junto a la descripción del dispositivo indica que está conectado actualmente al equipo. Si el dispositivo no está conectado al equipo, el icono aparecerá en gris.
6. Seleccione las casillas de verificación de los dispositivos USB que desea añadir a la base de datos y, a continuación, haga clic en **Añadir a la base de datos**.
   Los dispositivos USB seleccionados se añadirán a la base de datos.
7. Cierre o guarde el plan de protección.

Pasos para añadir dispositivos USB a la base de datos desde el panel de detalles del equipo

Nota
Este procedimiento solo se aplica a los dispositivos que están en línea y que tienen instalado el agente para la Prevención de pérdida de datos. No puede ver la lista de dispositivos USB para un equipo sin conexión o que no tenga instalado el agente para la Prevención de pérdida de datos.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un equipo al que haya estado conectado alguna vez el dispositivo USB deseado y, en el menú de la derecha, haga clic en **Inventario**.
   Se abrirá el panel de información del equipo.
3. En el panel de información del equipo, haga clic en la pestaña **Dispositivos USB**.
   Se abrirá la lista de dispositivos USB que se conocen en el equipo seleccionado.
   Los dispositivos USB se muestran en la vista de árbol. El primer nivel del árbol representa un modelo de dispositivo. El segundo nivel representa un dispositivo específico de ese modelo.
   Un icono azul junto a la descripción del dispositivo indica que está conectado actualmente al equipo. Si el dispositivo no está conectado al equipo, el icono aparecerá en gris.

© Acronis International GmbH, 2003-2025

4. Seleccione las casillas de verificación de los dispositivos USB que desee añadir a la base de datos y haga clic en **Añadir a la base de datos**.

Para añadir dispositivos USB a la base de datos desde alertas del servicio

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. Busque una alerta del control de dispositivos que le informe del acceso denegado al dispositivo USB.
3. En la vista simple de la alerta, haga clic en **Permitir este dispositivo USB**.
   Esto excluirá el dispositivo USB del control de acceso y lo agregará a la base de datos para futuras referencias.

Pasos para añadir dispositivos USB mediante la importación de una lista de dispositivos a la base de datos

Puede importar un archivo JSON con una lista de dispositivos USB a la base de datos. Consulte "Importar una lista de dispositivos USB a la base de datos" (p. 455).

Para eliminar dispositivos USB de la base de datos

1. Abra el plan de protección de un dispositivo para editarlo:
   Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.

   Nota
   Debe habilitar el control de dispositivos en el plan para acceder a la configuración del control de dispositivos.

2. Haga clic en la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en la fila **Lista de dispositivos USB permitidos**.
3. En la página para administrar la lista blanca, haga clic en **Añadir desde la base de datos**.
4. En la página para seleccionar dispositivos USB de la base de datos, haga clic en el icono de los tres puntos (...) al final del elemento de lista que representa el dispositivo, haga clic en **Eliminar** y confirme.
   Los dispositivos USB se eliminarán de la base de datos.
5. Cierre o guarde el plan de protección.

Ver alertas de control de dispositivos

El módulo de control de dispositivos se puede configurar para crear alertas de intentos de usuario denegados para utilizar determinados tipos de dispositivo (consulte Habilitar o deshabilitar las notificaciones del sistema operativo y alertas del servicio). Siga estos pasos para ver las alertas.

Para ver alertas de control de dispositivos

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**.
2. Busque alertas con el siguiente estado:"El acceso al dispositivo periférico está bloqueado".

© Acronis International GmbH, 2003-2025

Consulte Alertas de control de dispositivos para obtener más información.

Configuración del acceso

En la página **Configuración del acceso**, puede permitir o denegar el acceso a determinados tipos de dispositivos, así como habilitar o deshabilitar notificaciones de sistema operativo y alertas del control de dispositivos.

Nota
Los ajustes de acceso configurados en el control del dispositivo pueden ser anulados cuando se utilizan tanto el control del dispositivo como Advanced DLP para proteger un recurso informático. Cosulte "Habilitar Advanced Data Loss Prevention en los planes de protección" (p. 1228).

La configuración del acceso le permite limitar el acceso de usuario a los siguientes tipos de dispositivos y puertos:

- **Extraíble** (control de acceso por tipo de dispositivo): Dispositivos con cualquier interfaz para conectar a un equipo (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc.) que el sistema operativo reconoce como dispositivos de almacenamiento extraíbles (por ejemplo, memorias USB, lectores de tarjetas, unidades de disco magneto-óptico, etc.). El control de dispositivos clasifica todos los discos duros conectados mediante USB, FireWire, y PCMCIA como dispositivos extraíbles. También clasifica algunos discos duros (normalmente con SATA y SCSI) como dispositivos extraíbles si son compatibles con la función de conexión directa y no tienen instalado el sistema operativo actualmente en ejecución.

  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso a dispositivos extraíbles para controlar las operaciones de copia de datos en o desde cualquier dispositivo extraíble en un equipo protegido. Los derechos de acceso no afectan a dispositivos cifrados con BitLocker o FileVault (solo al sistema de archivos HFS+).

  Este tipo de dispositivo es compatible con Windows y macOS.
- **Extraíble cifrada** (control de acceso por tipo de dispositivo): dispositivos extraíbles cifrados con la unidad BitLocker (en Windows) o con FileVault (en macOS).

  En macOS, solo son compatibles las unidades extraíbles cifradas que utilizan el sistema de archivos HFS+ (también conocido como HFS Plus, Mac OS Extended o HFS Extended). Las unidades extraíbles cifradas que utilizan el sistema de archivos APFS se tratan como unidades extraíbles.

  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso a dispositivos extraíbles cifrados para controlar las operaciones de copia de datos en o desde cualquier dispositivo extraíble cifrado en un equipo protegido. Los derechos solo afectan a dispositivos cifrados con BitLocker o FileVault (solo al sistema de archivos HFS+).

  Este tipo de dispositivo es compatible con Windows y macOS.
- **Impresoras** (control de acceso por tipo de dispositivo): Las impresoras físicas con cualquier interfaz para conectarse a un equipo (USB, LPT, Bluetooth, etc.), así como aquellas a las que se accede desde un equipo en red.

© Acronis International GmbH, 2003-2025

Puede otorgar o denegar el acceso a impresoras para controlar la impresión de documentos en cualquier impresora en un equipo protegido.

Nota
Cuando cambie la configuración de acceso a las impresoras a **Rechazar**, deberá reiniciar las aplicaciones y procesos que tienen acceso a las impresoras para aplicar la nueva configuración de acceso. Para garantizar que la configuración de acceso se aplica correctamente, reinicie las cargas de trabajo protegidas.

Este tipo de dispositivo solo es compatible con Windows.

- **Portapapeles** (control de acceso por tipo de dispositivo): Portapapeles de Windows.
  Puede otorgar o denegar el acceso al portapapeles para controlar las operaciones para copiar y pegar datos mediante el portapapeles de Windows en un equipo protegido.

Nota
Cuando cambie la configuración de acceso al portapapeles a **Rechazar**, deberá reiniciar las aplicaciones y procesos que tienen acceso al portapapeles para aplicar la nueva configuración de acceso. Para garantizar que la configuración de acceso se aplica correctamente, reinicie las cargas de trabajo protegidas.

Este tipo de dispositivo solo es compatible con Windows.

- **Captura de pantalla** (control de acceso por tipo de dispositivo): permite hacer capturas de toda la pantalla, de la ventana activa o de una porción seleccionada de la pantalla.
  Puede otorgar o denegar el acceso a la captura de pantalla para controlar la captura de pantalla en un equipo protegido.

Nota
Cuando cambie la configuración de acceso a la captura de pantalla a **Rechazar**, deberá reiniciar las aplicaciones y procesos que tienen acceso a la captura de pantalla para aplicar la nueva configuración de acceso. Para garantizar que la configuración de acceso se aplica correctamente, reinicie las cargas de trabajo protegidas.

Este tipo de dispositivo solo es compatible con Windows.

- **Dispositivos móviles** (control de acceso por tipo de dispositivo): Dispositivos (como smartphones Android, etc.) que se comunican con un equipo mediante el Protocolo de transferencia de medios (MTP), con cualquier interfaz utilizada para conectarse a un equipo (USB, IP, Bluetooth).
  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso a dispositivos móviles para controlar las operaciones de copia de datos en o desde cualquier dispositivo móvil basado en MTP en un equipo protegido.

© Acronis International GmbH, 2003-2025

Nota

Cuando cambie la configuración de acceso a dispositivos móviles a **Sólo lectura** o **Rechazar**, deberá reiniciar las aplicaciones y los procesos que tienen acceso a los dispositivos móviles para aplicar la nueva configuración de acceso. Para garantizar que la configuración de acceso se aplica correctamente, reinicie las cargas de trabajo protegidas.

Este tipo de dispositivo solo es compatible con Windows.

- **Bluetooth** (control de acceso por tipo de dispositivo): Dispositivos Bluetooth externos e internos con cualquier interfaz para conectarse a un equipo (USB, PCMCIA, etc.). Esta configuración controla el uso de dispositivos de este tipo en lugar del intercambio de datos mediante estos dispositivos.

  Puede otorgar o denegar el acceso al Bluetooth para controlar el uso de dispositivos Bluetooth en un equipo protegido.

  Nota

  En macOS, los derechos de acceso al Bluetooth no afectan a los dispositivos HID Bluetooth. El acceso a estos dispositivos siempre está permitido para evitar que los dispositivos HID inalámbricos (ratones y teclados) se deshabiliten en el hardware de iMac y Mac Pro.

  Este tipo de dispositivo es compatible con Windows y macOS.
- **Unidades ópticas** (control de acceso por tipo de dispositivo): Unidades de CD/DVD/BD externas e internas (incluidos escritores) con cualquier interfaz para conectarse a un equipo (IDE, SATA, USB, FireWire, PCMCIA, etc.).

  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso a unidades de disco óptico para controlar las operaciones de copia de datos en o desde cualquier unidad de disco óptico en un equipo protegido.

  Este tipo de dispositivo es compatible con Windows y macOS.
- **Unidades de disquetes** (control de acceso por tipo de dispositivo): Unidades de disquetes externas e internas con cualquier interfaz para conectarse a un equipo (IDE, USB, PCMCIA, etc.). El sistema operativo reconoce algunos modelos de unidades de disquetes como dispositivos extraíbles, en cuyo caso el control de dispositivos también las identifica como dispositivos extraíbles.

  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso a unidades de disquete para controlar las operaciones de copia de datos en o desde cualquier unidad de disquete en un equipo protegido.

  Este tipo de dispositivo solo es compatible con Windows.
- **USB** (control de acceso por interfaz de dispositivo): Cualquier dispositivo conectado a un puerto USB, excepto hubs.

  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso al puerto USB para controlar las operaciones de copia de datos en o desde dispositivos conectados a cualquier puerto USB en un equipo protegido.

  Este tipo de dispositivo es compatible con Windows y macOS.

© Acronis International GmbH, 2003-2025

- **FireWire** (control de acceso por interfaz de dispositivo): Cualquier dispositivo conectado a un puerto FireWire (IEEE 1394), excepto hubs.

  Puede otorgar acceso completo, acceso de solo lectura o denegar el acceso al puerto FireWire para controlar las operaciones de copia de datos en o desde dispositivos conectados a cualquier puerto FireWire en un equipo protegido.

  Este tipo de dispositivo es compatible con Windows y macOS.
- **Dispositivos redirigidos** (control de acceso por interfaz de dispositivo): Dispositivos asignados (discos duros, unidades extraíbles y unidades ópticas), dispositivos USB y el portapapeles redirigido a sesiones de aplicaciones o escritorios virtuales.

  El control de dispositivos reconoce los dispositivos redirigidos mediante protocolos remotos de Microsoft RDP, Citrix ICA, VMware PCoIP y HTML5/WebSockets en entornos de virtualización Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer y VMware Horizon alojados en equipos de Windows protegidos. También puede controlar las operaciones de copia de datos entre el portapapeles de Windows del sistema operativo invitado que se ejecute en VMware Workstation, VMware Player, Oracle VM VirtualBox o Windows Virtual PC, y el portapapeles del sistema operativo anfitrión que se ejecute en un equipo de Windows protegido.

  Este tipo de dispositivo solo es compatible con Windows.

  Puede configurar el acceso a dispositivos redirigidos del siguiente modo:
  - **Dispositivos asignados**: puede otorgar acceso completo, acceso de solo lectura o denegar el acceso para controlar las operaciones de copia de datos en o desde cualquier disco duro, unidad extraíble o unidad óptica redirigida a la sesión alojada en un equipo protegido.
  - **Entrada de portapapeles**: puede otorgar o denegar el acceso para controlar las operaciones de copia de datos mediante el portapapeles a la sesión alojada en un equipo protegido.

    Nota
    Cuando cambie la configuración de acceso a la entrada de portapapeles a **Rechazar**, deberá reiniciar las aplicaciones y procesos que tienen acceso al portapapeles para aplicar la nueva configuración de acceso. Para garantizar que la configuración de acceso se aplica correctamente, reinicie las cargas de trabajo protegidas.

  - **Salida de portapapeles**: puede otorgar o denegar el acceso para controlar las operaciones de copia de datos mediante el portapapeles desde la sesión alojada en un equipo protegido.

    Nota
    Cuando cambie la configuración de acceso a la salida de portapapeles a **Rechazar**, deberá reiniciar las aplicaciones y procesos que tienen acceso al portapapeles para aplicar la nueva configuración de acceso. Para garantizar que la configuración de acceso se aplica correctamente, reinicie las cargas de trabajo protegidas.

  - **Puertos USB**: puede otorgar o denegar el acceso para controlar las operaciones de copia de datos desde dispositivos conectados a cualquier puerto USB redirigido a la sesión alojada en un equipo protegido.

© Acronis International GmbH, 2003-2025

La configuración del control de dispositivos afecta a todos los usuarios por igual. Por ejemplo, si deniega el acceso a dispositivos extraíbles, impedirá que cualquier usuario copie datos en o desde esos dispositivos en un equipo protegido. Es posible otorgar acceso de manera selectiva a dispositivos USB individuales al excluirlos del control de acceso (consulte Lista de tipos de dispositivo permitidos y Lista de dispositivos USB permitidos).

Cuando el acceso a un dispositivo esté controlado tanto por su tipo como por su interfaz, tiene prioridad denegar el acceso a nivel de interfaz. Por ejemplo, si se deniega el acceso a puertos USB (interfaz del dispositivo), se denegará el acceso a dispositivos móviles conectados a un puerto USB independientemente de si el acceso a estos está permitido o denegado (tipo de dispositivo). Para permitir el acceso a un dispositivo de ese tipo, debe permitir tanto su interfaz como su tipo.

Nota
Si el plan de protección utilizado en macOS está configurado para tipos de dispositivo que solo son compatibles con Windows, macOs ignorará la configuración de estos tipos de dispositivo.

Importante
Si un dispositivo extraíble, un dispositivo extraíble cifrado, una impresora o un dispositivo Bluetooth están conectados a un puerto USB y se permite el acceso a ese dispositivo, se anula el conjunto de denegación de acceso a nivel de interfaz USB. Si permite el acceso a ese tipo de dispositivo, se permitirá el acceso al dispositivo independientemente de si se ha denegado el acceso al puerto USB.

Notificaciones del sistema operativo y alertas del servicio

Se puede configurar el control de dispositivos para mostrar notificaciones del sistema operativo a los usuarios finales si intentan utilizar un tipo de dispositivo bloqueado en equipos protegidos. Cuando esté seleccionada la casilla de verificación **Mostrar notificaciones del sistema operativo a los usuarios finales si intentan utilizar un tipo de dispositivo o puerto bloqueados** en la configuración del acceso, el agente mostrará un mensaje emergente en el área de notificaciones del equipo protegido si ocurre alguno de estos eventos:

- Un intento denegado para utilizar un dispositivo en un puerto USB o FireWire. Esta notificación aparecerá cuando el usuario conecte un dispositivo USB o FireWire denegado a nivel de interfaz (por ejemplo, cuando se deniegue el acceso al puerto USB) o a nivel de tipo (por ejemplo, cuando se deniegue el uso de dispositivos extraíbles). La notificación informa de que el usuario no tiene acceso al dispositivo/controlador especificado.
- Un intento denegado de copiar un objeto de datos (como un archivo) desde un dispositivo específico. Esta notificación aparece cuando se deniega el acceso de lectura a estos dispositivos: unidades de disquetes, unidades de disco óptico, unidades extraíbles, unidades extraíbles cifradas, unidades móviles, unidades asignadas redirigidas y datos entrantes redirigidos del portapapeles. La notificación informa de que el usuario no tiene acceso al objeto de datos especificado del dispositivo especificado.

  La notificación de lectura denegada también se muestra cuando se deniega el acceso de lectura o escritura al Bluetooth, al puerto FireWire, al puerto USB y al puerto USB redirigido.

© Acronis International GmbH, 2003-2025

- Un intento denegado de copiar un objeto de datos (como un archivo) a un dispositivo específico. Esta notificación aparece cuando se deniega el acceso de escritura a estos dispositivos: unidades de disquetes, unidades de disco óptico, unidades extraíbles, unidades extraíbles cifradas, unidades móviles, portapapeles locales, capturas de pantalla, impresoras, unidades asignadas redirigidas y datos de salida redirigidos del portapapeles. La notificación informa de que el usuario no puede enviar el objeto de datos especificado al dispositivo especificado.

Los intentos por parte del usuario de acceder a los tipos de dispositivo bloqueados en los ordenadores protegidos pueden crear alertas que se registrarán en la consola de Cyber Protect. Se pueden habilitar alertas para cada tipo de dispositivo (excepto capturas de pantalla) o puerto de manera individual si se selecciona la casilla de verificación **Mostrar alerta** en la configuración del acceso. Por ejemplo, si el acceso a las unidades extraíbles está limitado a solo lectura y la casilla de verificación **Mostrar alerta** está seleccionada para ese tipo de unidades, se registrará una alerta cada vez que los usuarios de un equipo protegido intenten copiar los datos a una unidad extraíble. Consulte Alertas de control de dispositivos para obtener más información.

Consulte también Pasos para habilitar o deshabilitar notificaciones del sistema operativo y alertas del servicio.

Lista de tipos de dispositivo permitidos

En la página **Lista de tipos de dispositivo permitidos**, puede escoger las subclases de dispositivos que desea excluir del control de acceso de dispositivos. Como resultado, se permitirá el acceso a dichos dispositivos independientemente de la configuración del acceso del módulo de control de dispositivos.

El módulo de control de dispositivos ofrece la opción de permitir el acceso a dispositivos de determinadas subclases en un tipo de dispositivo denegado. Esta opción le permite denegar todos los dispositivos de determinado tipo, excepto algunas subclases de dispositivos de este tipo. Puede resultar útil, por ejemplo, cuando necesite denegar el acceso a todos los puertos USB al mismo tiempo que permite el uso de un teclado y un ratón USB.

Al configurar el módulo de control de dispositivos, puede especificar qué subclases de dispositivos desea excluir del control de acceso de dispositivos. Cuando un dispositivo pertenezca a una subclase excluida, se permitirá el acceso a dicho dispositivo independientemente de si el tipo o puerto está denegado o no. Puede excluir de forma selectiva las siguientes subclases de dispositivo del control de acceso de dispositivos:

- **HID USB (ratón, teclado, etc.)**: Cuando se selecciona, permite el acceso a dispositivos de interfaz humana (ratón, teclado, etc.) conectados a un puerto USB aunque los puertos USB estén denegados. De forma predeterminada, se selecciona este elemento para que el acceso denegado al puerto USB no deshabilite el teclado o el ratón.
  Compatible con Windows y macOS.
- **Tarjetas de red USB y FireWire**: Cuando se selecciona, permite el acceso a tarjetas de red conectadas a un puerto USB o FireWire (IEEE 1394) aunque los puertos USB y/o FireWire estén denegados.

© Acronis International GmbH, 2003-2025

Compatible con Windows y macOS.

- **Escáneres USB y dispositivos de captura de imágenes fijas**: cuando se selecciona, permite el acceso a escáneres y dispositivos de captura de imágenes fijas conectados a un puerto USB aunque los puertos USB estén denegados.
  Compatible solo con Windows.
- **Dispositivos de audio USB**: cuando se selecciona, permite el acceso a dispositivos de audio, como auriculares o micrófonos, conectados a un puerto USB aunque los puertos USB estén denegados.
  Compatible solo con Windows.
- **Cámaras USB**: cuando se selecciona, permite el acceso a cámaras web conectadas a un puerto USB aunque los puertos USB estén denegados.
  Compatible solo con Windows.
- **HID Bluetooth (ratón, teclado, etc.)**: cuando se selecciona, permite el acceso a dispositivos de interfaz humana (ratón, teclado, etc.) conectados mediante Bluetooth aunque este esté denegado.
  Compatible solo con Windows.
- **Copiar/pegar desde el portapapeles en la aplicación**: cuando se selecciona, permite copiar y pegar datos mediante el portapapeles en la misma aplicación aunque el portapapeles esté denegado.
  Compatible solo con Windows.

Nota
La configuración de los subtipos de dispositivo no compatibles se ignora si está configurada en el plan de protección aplicado.

Cuando añada tipos de dispositivo a la lista blanca, tenga en cuenta lo siguiente:

- Con la lista blanca de tipos de dispositivo solo permitirá una subclase de dispositivos completa. No puede permitir un modelo de dispositivo específico si deniega al resto de dispositivos de la misma subclase. Por ejemplo, si excluye las cámaras USB del control de acceso de dispositivos, permite el uso de cualquier cámara USB, sin importar el modelo o el proveedor. Para saber cómo permitir modelos o dispositivos individuales, consulte Lista de dispositivos USB permitidos.
- Los tipos de dispositivo solo se pueden seleccionar de una lista cerrada de subclases de dispositivos. Si el dispositivo que desea permitir pertenece a una subclase diferente, no podrá permitirlo mediante la lista blanca de tipos de dispositivo. Por ejemplo, una subclase como los lectores de tarjetas inteligentes USB no se puede agregar a la lista blanca. Para permitir un lector de tarjetas inteligentes USB cuando los puertos USB están denegados, siga las instrucciones que aparecen en Lista de dispositivos USB permitidos.
- La lista blanca de tipos de dispositivo solo funciona con dispositivos que utilizan controladores de Windows estándar. Puede que el control de dispositivos no reconozca la subclase de algunos dispositivos USB con controladores propios. Como resultado, no podrá permitir el acceso a esos dispositivos USB mediante la lista blanca de tipos de dispositivo. En este caso, podría permitir el acceso por dispositivo o modelo (consulte Lista de dispositivos USB permitidos).

© Acronis International GmbH, 2003-2025

Lista de dispositivos USB permitidos

La lista blanca está diseñada para permitir el uso de determinados dispositivos USB independientemente de cualquier otra configuración de control de dispositivos. Puede añadir dispositivos individuales o modelos de dispositivos a la lista blanca para deshabilitar el control de acceso en dichos dispositivos. Por ejemplo, si añade un dispositivo móvil con un ID único a la lista blanca, se permitirá el uso de dicho dispositivo específico aunque se denieguen otros dispositivos USB.

En la página **Lista de dispositivos USB permitidos**, puede especificar los dispositivos USB o los modelos de dispositivos USB individuales que desea excluir del control de acceso de dispositivos. Como resultado, se permitirá el acceso a dichos dispositivos independientemente de la configuración del acceso del módulo de control de dispositivos.

Existen dos maneras de identificar dispositivos en una lista blanca:

- Modelo de dispositivo: Identifica de forma colectiva todos los dispositivos de un modelo determinado. Cada modelo de dispositivo se identifica por el ID del proveedor (VID) y el del producto (PID), como por ejemplo USB\VID_0FCE&PID_E19E.

  Esta combinación de VID y PID no identifica un dispositivo específico, sino un modelo de dispositivo. Al añadir un modelo de dispositivo a la lista blanca, se permitirá el acceso a cualquier dispositivo de ese modelo. Por ejemplo, así podrá permitir el uso de impresoras USB de un modelo concreto.
- Dispositivo único: Identifica un dispositivo específico. Cada dispositivo único se identifica por el ID del proveedor (VID), el del producto (PID) y un número de serie, como por ejemplo USB\VID_0FCE&PID_E19E\D55E7FCA.

  No todos los dispositivos USB tienen asignado un número de serie. Puede añadir un dispositivo a la lista blanca como un dispositivo único si se le ha asignado un número de serie durante la producción. Por ejemplo, una memoria USB con un número de serie exclusivo.

Para añadir un dispositivo a la lista blanca, deberá añadirlo primero a la Base de datos de dispositivos USB. Entonces podrá añadir dispositivos a la lista blanca seleccionándolos en la base de datos.

La lista blanca se gestiona en una página de configuración individual llamada **Lista de dispositivos USB permitidos**. Cada elemento de la lista representa un dispositivo o modelo de dispositivo e incluye estos campos:

- **Descripción**: El sistema operativo asigna una descripción específica cuando se conecta el dispositivo USB. Puede modificar la descripción del dispositivo en la base de datos de dispositivos USB (consulte la Página de gestión de la base de datos de USB).
- **Tipo de dispositivo**: Se muestra "Único" si el elemento de la lista es un dispositivo único o "Modelo" si es un modelo de dispositivo.

© Acronis International GmbH, 2003-2025

- **Sólo lectura** Cuando se selecciona, solo permite recibir datos del dispositivo. Si el dispositivo no es compatible con el acceso de solo lectura, se bloqueará el acceso al mismo. Borre esta casilla de verificación para permitir el acceso completo al dispositivo.
- **Reiniciar**: cuando se selecciona, hace que el dispositivo simule la desconexión/reconexión cuando un nuevo usuario inicia sesión. Algunos dispositivos USB necesitan reiniciarse para funcionar, por lo que le recomendamos que seleccione esta casilla de verificación para esos dispositivos (ratón, teclado, etc.). También le recomendamos borrar esta casilla de verificación para dispositivos de almacenamiento de datos (como memorias USB, unidades de disco óptico, discos duros externos, etc.).
  Puede que el control de dispositivos no pueda reiniciar algunos dispositivos USB con controladores propios. Si no hay acceso a dicho dispositivo, deberá retirar el dispositivo del puerto USB y volver a insertarlo.

Nota
El campo **Reinicializar** está oculto de forma predeterminada. Para mostrarla en la tabla, haga clic en el icono de engranaje en la esquina superior derecha de la tabla y seleccione la casilla de verificación **Reinicializar**.

Nota
Los campos **Sólo lectura** y **Reinicializar** no son compatibles con macOS. Si estos campos están configurados en el plan de protección aplicado, se ignorarán.

Puede añadir o eliminar dispositivos o modelos de la lista blanca del siguiente modo:

- Haga clic en **Añadir desde la base de datos** encima de la lista y seleccione los dispositivos que desee de entre los registrados en la Base de datos de dispositivos USB. El dispositivo seleccionado se añadirá a la lista y podrá configurar sus ajustes y confirmar los cambios.
- Haga clic en **Permitir este dispositivo USB** si aparece una alerta informándole de que el acceso al dispositivo USB está denegado (consulte Alertas de control de dispositivos). Se añadirá el dispositivo a la lista blanca y a la base de datos de dispositivos USB.
- Haga clic en el icono eliminar al final de un elemento de la lista. Se eliminará el respectivo dispositivo o modelo de la lista blanca.

Base de datos de dispositivos USB

El módulo de control de dispositivos mantiene una base de datos de dispositivos USB desde la que puede agregar dispositivos a la lista de exclusiones (consulte Lista de dispositivos USB permitidos). Puede registrar un dispositivo USB en una base de datos de estas formas:

- Agregar un dispositivo a la página que aparece al añadir un dispositivo a la lista de exclusión (consulte Página de administración de la base de datos de dispositivos USB).
- Agregue un dispositivo desde la pestaña de dispositivos USB del panel de inventario de un ordenador en la consola de Cyber Protect (consulte Lista de dispositivos USB en un equipo).
- Permitir que el dispositivo reciba una alerta al denegar el acceso al dispositivo USB (consulte Alertas de control de dispositivos).

© Acronis International GmbH, 2003-2025

Consulte también Cómo agregar o eliminar dispositivos USB de la base de datos.

Página de administración de la base de datos de dispositivos USB

Cuando configure la lista de dispositivos USB permitidos, puede agregar un dispositivo desde la base de datos. Si escoge esta opción, aparecerá una página de administración con una lista de dispositivos. En esta página puede ver la lista de todos los dispositivos registrados en la base de datos y seleccionarlos para añadirlos a la lista de permitidos, así como para llevar a cabo estas operaciones:

Registrar un dispositivo en la base de datos

1. Haga clic en **Añadir a la base de datos** en la parte de arriba de la página.
2. En el cuadro de diálogo **Agregar dispositivo USB** que aparece, seleccione la máquina a la que se conecta el dispositivo USB.
   En la lista de equipos solo se muestran las máquinas que están en línea.
   La lista de dispositivos USB solo se muestra en las máquinas que tienen instalado el agente para la Prevención de pérdida de datos.
   Los dispositivos USB se muestran en la vista de árbol. El primer nivel del árbol representa un modelo de dispositivo. El segundo nivel representa un dispositivo específico de ese modelo.
   Un icono azul junto a la descripción del dispositivo indica que está conectado actualmente al equipo. Si el dispositivo no está conectado al equipo, el icono aparecerá en gris.
3. Seleccione la casilla de verificación del dispositivo USB que desea registrar y haga clic en **Añadir a la base de datos**.

Cambiar la descripción de un dispositivo

1. En la página **Base de datos de dispositivos USB**, haga clic en el icono de los tres puntos (...) al final del elemento de lista que representa el dispositivo y, a continuación, haga clic en **Editar**.
2. Haga cambios en la descripción en el cuadro de diálogo que aparece.

Eliminar un dispositivo de la base de datos

1. Haga clic en el icono de puntos suspensivos (...) al final del elemento de lista que representa el dispositivo.
2. Haga clic en **Eliminar** y confirme la operación.

La lista de la página ofrecerá la siguiente información sobre cada dispositivo:

- **Descripción**: Un identificador leíble del dispositivo. Puede cambiar la descripción según sea necesario.
- **Tipo de dispositivo**: Se muestra "Único" si el elemento de la lista es un dispositivo único o "Modelo" si es un modelo de dispositivo. Un dispositivo único debe tener un número de serie y un ID del proveedor (VID) y del producto (PID), mientras que un modelo de dispositivo se identifica por una combinación del VID y el PID.
- **ID del proveedor**, **ID del producto**, **número de serie**: Estos valores componen el ID del dispositivo de la siguiente forma: USB\VID_<vendor ID>&PID_<product ID>\<serial number>.

© Acronis International GmbH, 2003-2025

- **Cuenta**: Indica el inquilino al que pertenece este dispositivo. Este es el inquilino que contiene la cuenta de usuario que se utiliza para registrar el dispositivo en la base de datos.

  Nota
  Esta columna está oculta de forma predeterminada. Para mostrarla en la tabla, haga clic en el icono de engranaje en la esquina superior derecha de la tabla y, a continuación, seleccione **Cuenta**.

La primera columna a la izquierda está diseñada para seleccionar los dispositivos que se desean añadir a la lista de permitidos: Seleccione la casilla de verificación de cada dispositivo que desee añadir y haga clic en el botón **Añadir a la lista de permitidos**. Para seleccionar o borrar todas las casillas de verificación, haga clic en la casilla de verificación del encabezado de la columna.

Puede buscar o filtrar la lista de dispositivos:

- Haga clic en **Buscar** en la parte de arriba de la página y escriba una cadena de búsqueda. La lista mostrará los dispositivos cuya descripción coincida con la cadena que ha escrito.
- Haga clic en **Filtro** y, a continuación, configure y aplique un filtro en la casilla de verificación que aparece. La lista se limita a los dispositivos con el tipo, el ID del proveedor, el ID del producto y la cuenta que haya seleccionado al configurar el filtro. Para cancelar el filtro y mostrar todos los dispositivos, haga clic en **Restablecer a los valores predeterminados**.

Exportar la lista de dispositivos USB de la base de datos

Puede exportar la lista de dispositivos USB añadidos a la base de datos.

1. Abra el plan de protección de un dispositivo para editarlo.
2. Haga clic en el icono de la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en la fila **Lista de dispositivos USB permitidos**.
3. En la página Lista de dispositivos USB permitidos, haga clic en **Agregar desde la base de datos**.
4. En la página para administrar la base de datos de dispositivos USB, haga clic en **Exportar**. Se abrirá el cuadro de diálogo Examinar estándar.
5. Seleccione la ubicación en la que desee guardar el archivo, introduzca un nuevo nombre de archivo si es necesario y haga clic en **Guardar**.

La lista de dispositivos USB se exportará a un archivo JSON.

Puede editar el archivo JSON resultante para añadir o eliminar dispositivos de este y realizar cambios masivos de las descripciones de dispositivos.

Importar una lista de dispositivos USB a la base de datos

En lugar de agregar dispositivos USB desde la consola de Cyber Protect, puede importar una lista de dispositivos USB. La lista es un archivo en formato JSON.

© Acronis International GmbH, 2003-2025

Nota
Puede importar archivos JSON a una base de datos que no contenga los dispositivos descritos en el archivo. Para importar un archivo modificado a la base de datos desde la que se exportó, primero deberá limpiar la base de datos ya que no puede importar entradas duplicadas. Si exporta la lista de dispositivos USB, la modifica e intenta importarla a la misma base de datos sin limpiarla, la importación fallará.

1. Abra el plan de protección de un dispositivo para editarlo.
2. Haga clic en el icono de la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en la fila **Lista de dispositivos USB permitidos**.
3. En la página Lista de dispositivos USB permitidos, haga clic en **Agregar desde la base de datos**.
4. Arrastre y suelte el archivo que desea importar o búsquelo.

La consola de Cyber Protect comprueba si la lista contiene entradas duplicadas que ya existan en la base de datos y las omite. Se añadirán los dispositivos USB que no se encuentren en la base de datos.

Lista de dispositivos USB en un equipo

El panel de inventario de un ordenador en la consola de Cyber Protect incluye la pestaña **Dispositivos USB**. Si el equipo está en línea y tiene instalada la Prevención de pérdida de datos, la pestaña **Dispositivos USB** mostrará una lista con todos los dispositivos USB que han estado conectados alguna vez al equipo.

Los dispositivos USB se muestran en la vista de árbol. El primer nivel del árbol representa un modelo de dispositivo. El segundo nivel representa un dispositivo específico de ese modelo.

La lista ofrece la siguiente información sobre cada dispositivo:

- **Descripción**: El sistema operativo asigna una descripción cuando se conecta el dispositivo USB. Esta descripción puede servir de identificador leíble del dispositivo.
  Un icono azul junto a la descripción del dispositivo indica que está conectado actualmente al equipo. Si el dispositivo no está conectado al equipo, el icono aparecerá en gris.
- **ID del dispositivo**: El identificador que el sistema operativo asignó al dispositivo. El identificador tiene el siguiente formato: USB\VID_<vendor ID>&PID_<product ID>\<serial number> donde <serial number> es opcional. Ejemplos: USB\VID_0FCE&PID_ADDE\D55E7FCA (dispositivo con un número de serie); USB\VID_0FCE&PID_ADDE (dispositivo sin número de serie).

Para agregar dispositivos USB a la base de datos, seleccione las casillas de verificación de los dispositivos que desee y, a continuación, haga clic en el botón **Añadir a la base de datos**.

Exclusión de procesos del control de acceso

El acceso al portapapeles de Windows, a las capturas de pantalla, a las impresoras y a los dispositivos móviles está controlado por hooks inyectados en los procesos. Si los procesos no

© Acronis International GmbH, 2003-2025

tienen hooks, el acceso a estos dispositivos no estará controlado.

Nota
La exclusión de procesos de control de acceso no es compatible con macOS. Si se configura una lista de procesos excluidos en el plan de protección aplicado, se ignorarán.

En la página **Exclusiones**, puede especificar una lista de procesos que no tendrán hooks. Esto significa que los controles de acceso del portapapeles (local y redirigido), de las capturas de pantalla, de las impresoras y de los dispositivos móviles no se aplicarán a dichos procesos.

Por ejemplo, ha aplicado un plan de protección que deniega el acceso a impresoras y, a continuación, ha iniciado la aplicación Microsoft Word. Cualquier intento de imprimir desde esta aplicación se bloqueará. Sin embargo, si añade el proceso de Microsoft Word a la lista de exclusiones, la aplicación no tendrá hooks. Como resultado, no se bloqueará la impresión desde Microsoft Word, pero sí seguirá bloqueada desde otras aplicaciones.

Pasos para añadir procesos a exclusiones

1. Abra el plan de protección de un dispositivo para editarlo:
   Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.

   Nota
   Debe habilitar el control de dispositivos en el plan para acceder a la configuración del control de dispositivos.

2. Haga clic en la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en la fila **Exclusiones**.
3. En la página **Exclusiones**, en la fila **Procesos y carpetas**, haga clic en **+Añadir**.
4. Añada los procesos que desea excluir del control de acceso.
   Por ejemplo, `C:\Folder\subfolder\process.exe`.
   Puede utilizar comodines:
   - * remplaza cualquier número de caracteres.
   - ? remplaza un carácter.

   Por ejemplo:

   ```
   C:\Folder\*
   *\Folder\SubFolder?\*
   *\process.exe
   ```
5. Haga clic en la marca de verificación y, a continuación, haga clic en **Listo**.
6. En el plan de protección, haga clic en **Guardar**.
7. Reinicie los procesos que excluyó para garantizar que los hooks se eliminan correctamente.

Los procesos excluidos tendrán acceso al portapapeles, a las capturas de pantalla, a las impresoras y a los dispositivos móviles independientemente de la configuración de acceso de esos dispositivos.

© Acronis International GmbH, 2003-2025

Pasos para eliminar un proceso de las exclusiones

Abra el plan de protección de un dispositivo para editarlo:

Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.

Nota
Debe habilitar el control de dispositivos en el plan para acceder a la configuración del control de dispositivos.

1. Haga clic en la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en la fila **Exclusiones**.
2. En la página **Exclusiones**, haga clic en el icono de la papelera junto al proceso que quiere eliminar de las exclusiones.
3. Haga clic en **Listo**.
4. En el plan de protección, haga clic en **Guardar**.
5. Reinicie el proceso para garantizar que los hooks se inyectan correctamente.

La configuración de acceso desde el plan de protección se aplicará a los procesos que elimine de las exclusiones.

Pasos para editar un proceso en las exclusiones

1. Abra el plan de protección de un dispositivo para editarlo:
   Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.

   Nota
   Debe habilitar el control de dispositivos en el plan para acceder a la configuración del control de dispositivos.

2. Haga clic en la flecha junto al conmutador de **Control de dispositivos** para expandir la configuración y, a continuación, haga clic en la fila **Exclusiones**.
3. En la página **Exclusiones**, haga clic en el icono **Editar** junto al proceso que quiere editar.
4. Aplique los cambios y haga clic en la marca de verificación para confirmar.
5. Haga clic en **Listo**.
6. En el plan de protección, haga clic en **Guardar**.
7. Reinicie los procesos afectados para garantizar que sus cambios se aplican correctamente.

Alertas de control de dispositivos

El control de dispositivos mantiene un registro de eventos mediante el seguimiento de los intentos del usuario de acceder a los tipos de dispositivos, interfaces o puertos controlados. Algunos eventos pueden crear alertas que se registrarán en la consola de Cyber Protect. Por ejemplo, se puede

© Acronis International GmbH, 2003-2025

configurar el módulo del control de dispositivos para evitar el uso de unidades extraíbles con el registro de una alerta cuando un usuario intente copiar datos a o de dicho dispositivo.

Cuando configure el módulo de control de dispositivos, se pueden habilitar alertas para la mayoría de los elementos enumerados en el tipo de dispositivo (excepto capturas de pantalla) o puerto. Si se habilitan las alertas, cada vez que los usuarios intenten llevar a cabo una operación que no esté permitida se generará una alerta. Por ejemplo, si el acceso a las unidades extraíbles está limitado a solo lectura y la opción **Mostrar alerta** está seleccionada para ese tipo de unidades, se generará una alerta cada vez que los usuarios de un equipo protegido intenten copiar los datos a una unidad extraíble.

Para ver las alertas en la consola de Cyber Protect, vaya a **Supervisión** > **Alertas**. Para cada alerta de control de dispositivo, la consola proporciona la siguiente información sobre el respectivo evento:

- **Tipo**: Advertencia.
- **Estado**: Se muestra "El acceso al dispositivo periférico está bloqueado".
- **Mensaje**: Muestra "El acceso a '<device type or port>' en '<computer name>' está bloqueado". Por ejemplo, "El acceso a 'Extraíble' en 'accountant-pc' está bloqueado".
- **Fecha y hora**: La fecha y la hora en las que ocurrió el evento.
- **Dispositivo**: El nombre del equipo en el que ocurrió el evento.
- **Nombre del plan**: El nombre del plan de protección que causó el evento.
- **Origen**: El tipo de dispositivo o puerto involucrado en el evento. Por ejemplo, si se deniega el intento de acceso de un usuario a una unidad extraíble, en este campo se indicará "Unidad extraíble".
- **Acción**: La operación que causó el evento. Por ejemplo, si se deniega el intento de un usuario de copiar datos a un dispositivo, en este campo se indicará "Escribir". Para obtener más información, consulte Valores del campo acción.
- **Nombre**: El nombre del objeto de destino del evento, como el archivo que el usuario intentó copiar o el dispositivo que intentó utilizar. Si no se identifica el objeto de destino, no se mostrará.
- **Información**: Información adicional acerca del dispositivo objeto del evento, como el ID del dispositivo para los dispositivos USB. Si no hay disponible información adicional sobre el dispositivo objeto, no se mostrará.
- **Usuario**: El nombre del usuario que causó el evento.
- **Proceso**: La ruta cualificada completa al archivo ejecutable de la aplicación que causó el evento. En algunos casos, puede que se muestre el nombre del proceso en lugar de la ruta. No se mostrará si la información del proceso no está disponible.

Si se aplica una alerta a un dispositivo USB (incluidas las unidades extraíbles y las unidades extraíbles cifradas), el administrador podrá añadir el dispositivo a la lista blanca directamente desde la alerta, lo que evitará que el módulo de control de dispositivos tenga acceso limitado a ese dispositivo específico. Si hace clic en **Permitir este dispositivo USB**, se añadirá a la lista blanca de

© Acronis International GmbH, 2003-2025

dispositivos USB en la configuración del módulo de control de dispositivos y también a la Base de datos de dispositivos USB para posteriores referencias.

Consulte también Pasos para ver alertas de control de dispositivos.

Valores del campo acción

El campo **Acción** de las alertas puede incluir estos valores:

- **Leer**: Obtener datos del dispositivo o el puerto.
- **Escribir**: Enviar datos al dispositivo o el puerto.
- **Formatear**: Acceso directo (formateo, comprobación de disco, etc.) al dispositivo. En el caso de un puerto, se aplica al dispositivo conectado a ese puerto.
- **Expulsar**: Eliminar el dispositivo del sistema o extraer el medio del dispositivo. En el caso de un puerto, se aplica al dispositivo conectado a ese puerto.
- **Imprimir**: Enviar un documento a la impresora.
- **Copiar audio**: Copiar/pegar los datos de audio mediante el portapapeles local.
- **Copiar archivo**: Copiar/pegar un archivo mediante el portapapeles local.
- **Copiar imagen**: Copiar/pegar una imagen mediante el portapapeles local.
- **Copiar texto**: Copiar/pegar el texto mediante el portapapeles local.
- **Copiar contenido no identificado**: Copiar/pegar otros datos mediante el portapapeles local.
- **Copiar datos RTF (imagen)**: Copiar/pegar una imagen mediante el portapapeles local utilizando el formato de texto enriquecido.
- **Copiar datos RTF (archivo)**: Copiar/pegar un archivo mediante el portapapeles local utilizando el formato de texto enriquecido.
- **Copiar datos RTF (texto, imagen)**: Copiar/pegar texto y una imagen mediante el portapapeles local utilizando el formato de texto enriquecido.
- **Copiar datos RTF (texto, archivo)**: Copiar/pegar texto y un archivo mediante el portapapeles local utilizando el formato de texto enriquecido.
- **Copiar datos RTF (imagen, archivo)**: Copiar/pegar una imagen y un archivo mediante el portapapeles local utilizando el formato de texto enriquecido.
- **Copiar datos RTF (texto, imagen, archivo)**: Copiar/pegar texto, una imagen y un archivo mediante el portapapeles local utilizando el formato de texto enriquecido.
- **Eliminar**: Eliminar datos del dispositivo (por ejemplo, una unidad extraíble, una unidad móvil, etc.).
- **Acceso al dispositivo**: Acceso a algunos dispositivos o puertos (por ejemplo, un dispositivo Bluetooth, un puerto USB, etc.).
- **Audio entrante**: Copiar/pegar datos de audio del equipo del cliente a la sesión alojada mediante el portapapeles redirigido.
- **Archivo entrante**: Copiar/pegar un archivo del equipo del cliente a la sesión alojada mediante el portapapeles redirigido.

© Acronis International GmbH, 2003-2025

- **Imagen entrante**: Copiar/pegar una imagen del equipo del cliente a la sesión alojada mediante el portapapeles redirigido.
- **Texto entrante**: Copiar/pegar texto del equipo del cliente a la sesión alojada mediante el portapapeles redirigido.
- **Contenido no identificado entrante**: Copiar/pegar otro contenido del equipo del cliente a la sesión alojada mediante el portapapeles redirigido.
- **Datos RTF entrantes (imagen)**: Copiar/pegar una imagen del equipo del cliente a la sesión alojada mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF entrantes (archivo)**: Copiar/pegar un archivo del equipo del cliente a la sesión alojada mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF entrantes (texto, imagen)**: Copiar/pegar texto y una imagen del equipo del cliente a la sesión alojada mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF entrantes (texto, archivo)**: Copiar/pegar texto y un archivo del equipo del cliente a la sesión alojada mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF entrantes (imagen, archivo)**: Copiar/pegar una imagen y un archivo del equipo del cliente a la sesión alojada mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF entrantes (texto, imagen, archivo)**: Copiar/pegar texto, una imagen y un archivo del equipo del cliente a la sesión alojada mediante el portapapeles redirigido utilizando el Formato de texto enriquecido.
- **Insertar**: Conectar un dispositivo USB o un dispositivo FireWire.
- **Audio saliente**: Copiar/pegar datos de audio de la sesión alojada al equipo del cliente mediante el portapapeles redirigido.
- **Archivo saliente**: Copiar/pegar un archivo de la sesión alojada al equipo del cliente mediante el portapapeles redirigido.
- **Imagen saliente**: Copiar/pegar una imagen de la sesión alojada al equipo del cliente mediante el portapapeles redirigido.
- **Texto saliente**: Copiar/pegar texto de la sesión alojada al equipo del cliente mediante el portapapeles redirigido.
- **Contenido no identificado saliente**: Copiar/pegar otro contenido de la sesión alojada al equipo del cliente mediante el portapapeles redirigido.
- **Datos RTF salientes (imagen)**: Copiar/pegar una imagen de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF salientes (archivo)**: Copiar/pegar un archivo de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF salientes (texto, imagen)**: Copiar/pegar texto y una imagen de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF salientes (texto, archivo)**: Copiar/pegar texto y un archivo de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.

© Acronis International GmbH, 2003-2025

- **Datos RTF salientes (imagen, archivo)**: Copiar/pegar una imagen y un archivo de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF salientes (texto, imagen, archivo)**: Copiar/pegar texto, una imagen y un archivo de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Cambiar nombre**: Cambiar el nombre a los archivos de un dispositivo (por ejemplo, de dispositivos extraíbles, dispositivos móviles y otros).

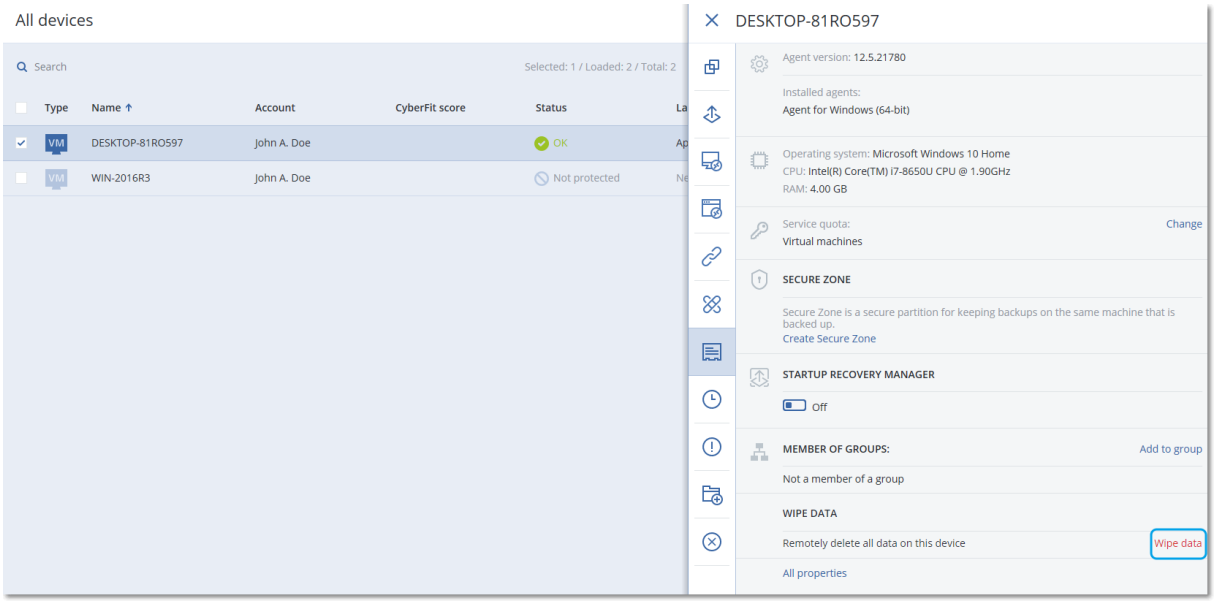
Borrado de datos de una carga de trabajo gestionada

Nota
El borrado remoto está disponible con el paquete Advanced Security.

Borrado remoto permite a un administrador de Cyber Protection y al propietario de un equipo eliminar los datos de un equipo gestionado (por ejemplo, en caso de pérdida o robo). De este modo se puede evitar el acceso no autorizado a información confidencial.

El borrado remoto solo está disponible para equipos que ejecutan versiones de Windows 10 o posteriores. De forma predeterminada, se utiliza la función `doWipeProtected`. Si no está disponible, se utiliza la función `doWipe`. Para obtener más información sobre estas funciones, consulte la documentación de Microsoft.

Para recibir el comando de borrado, el equipo debe estar encendido y conectado a Internet.



Pasos para borrar los datos de un equipo

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo cuyos datos desea borrar.

© Acronis International GmbH, 2003-2025

Nota
Puede borrar datos de un solo equipo al mismo tiempo.

3. Haga clic en **Detalles** y, a continuación, en **Borrar datos**.
   Si el equipo que ha seleccionado está fuera de línea, la opción **Borrar datos** no es accesible.
4. Confirme su elección.
5. Introduzca las credenciales de administrador local del equipo y, a continuación, haga clic en **Borrar datos**.

Nota
Puede comprobar los detalles del proceso de borrado y quién lo inició desde **Supervisión** > **Actividades**.

Ver cargas de trabajo gestionados por integraciones RMM

Nota
Esta característica solo está disponible si se ha habilitado el servicio PSA.

Cuando integra una plataforma RMM como parte del servicio PSA, puede ver y supervisar la información de los dispositivos gestionados por la plataforma RMM. Esta información está disponible en la pestaña **Dispositivos** de la consola de Cyber Protect.

Ver cargas de trabajo gestionadas por integraciones RMM

1. Vaya a **Dispositivos** > **Todos los dispositivos**.
2. Ordene la columna **Integración con RMM** para localizar las integraciones que correspondan.
3. Seleccione la carga de trabajo que corresponda.
4. En el panel **Acciones**, seleccione **Detalles**.
5. En el panel que se muestra, podrá ver una de las siguientes tres opciones, según la carga de trabajo configurada:
   - Si los servicios de Acronis están definidos por la carga de trabajo sin la integración RMM: Si la carga de trabajo está configurada para trabajar solo con servicios de Acronis, no se mostrará ninguna información acerca de la integración RMM.
   - Si los servicios de Acronis y la integración RMM están configurados para la carga de trabajo: Los detalles de los servicios de Acronis y la integración RMM se ubican en dos pestañas, **Información general** e **Integración RMM**. Haga clic en **Integración RMM** para ver los detalles de la integración, lo que incluye el nombre y el tipo de la carga de trabajo (facilitado por la plataforma RMM), la descripción y la ubicación. Asimismo, se mostrarán todos los complementos del agente RMM instalados y habilitados.

© Acronis International GmbH, 2003-2025

- Si la carga de trabajo está configurada solo con una integración RMM: Se mostrarán los detalles de la integración RMM, lo que incluye el nombre y el tipo de la carga de trabajo (facilitados por la plataforma RMM), la descripción y la ubicación. Asimismo, se mostrarán todos los complementos del agente RMM instalados y habilitados.

Nota
Cuando la carga de trabajo está configurada con una integración de RMM (ya sea en conjunto con servicios de Acronis o solo con una integración RMM), puede hacer lo siguiente:

- Inicie una conexión remota (disponible para las integraciones Datto RMM, N-able N-central y N-able RMM).
- Revise los complementos instalados en el dispositivo de RMM de terceros (disponible solo para N-able RMM).
- Acceda directamente a los detalles del dispositivo de RMM de terceros (disponible para Datto RMM, N-able N-central y NinjaOne).

Cargas de trabajo de CyberApp

Las cargas de trabajo de CyberApp las crean ISV (Proveedores de software independientes) y aparecen en la consola de Cyber Protect después de habilitar una integración CyberApp. Deben cumplirse las siguientes condiciones:

- El punto de extensión **cargas de trabajo y acciones** deben estar habilitadas en CyberApp.
- Se debe definir al menos un **tipo de carga de trabajo** en CyberApp.
- El servicio del conector alojado por el ISV debe garantizar que las cargas de trabajo de CyberApp se añaden a la plataforma de Acronis y se actualizan.

Para obtener más información sobre el Portal de proveedores y la creación de CyberApps, consulte la Guía del usuario del portal de proveedores.

Cargas de trabajo agregadas

Una carga de trabajo física puede tener un agente de Cyber Protect y uno o varios agentes de CyberApp instalados al mismo tiempo. En ese caso, la misma carga de trabajo tendrá más de una representación en la pantalla **Todos los dispositivos**: se mostrará un registro independiente para la carga de trabajo de Acronis y para cada carga de trabajo de CyberApp. Si la unión automática de las cargas de trabajo está habilitad y configurada desde el portal de proveedores o desde la consola de Cyber Protect, el sistema comparará las direcciones del host y las direcciones MAC de las cargas de trabajo de Acronis y las de CyberApp y unirá todas las representaciones en una sola carga de trabajo agregada. También puede unir o deshacer manualmente la unión de las cargas de trabajo en la consola de Cyber Protect.

© Acronis International GmbH, 2003-2025

Trabajar con cargas de trabajo de CyberApp

Además de las acciones estándar integradas en la consola de Cyber Protect, puede ejecutar las acciones que estén disponibles después de que las cargas de trabajode CyberApp aparezcan en la consola: una de forma manual las cargas de trabajo en un carga de trabajo agregada y ejecute las acciones personalizadas configuradas en las CyberApps.

Unir

Requisitos previos

- Las cargas de trabajo de diferentes fuentes están disponibles para el inquilino.

Puede unir manualmente una carga de trabajo de Acronis con una o varias cargas de trabajo de CyberApp en una sola carga de trabajo agregada.

Pasos para unir cargas de trabajo manualmente en una carga de trabajo agregadas

1. En la pantalla **Todos los dispositivos**, seleccione las cargas de trabajo que desee unir.

   Nota
   La acción de unión se muestra si selecciona cargas de trabajo de diferentes fuentes, como una carga de trabajo de Acronis y una carga de trabajo de CyberApp.

2. Haga clic en **Unir cargas de trabajo**.

Realizar acciones personalizadas

Requisitos previos

- Hay una integración de CyberApp que tiene definidas **Acciones de carga de trabajo** habilitadas para el inquilino.

Las acciones personalizadas son acciones configuradas en CyberApp y que se vuelven disponibles para la correspondiente carga de trabajo de CyberApp cuando habilita la integración de CyberApp para el inquilino.

Pasos para realizar acciones personalizadas

1. En la pantalla **Todos los dispositivos**, haga clic en la carga de trabajo.
2. Haga clic en **Acciones integradas de la aplicación**.
3. Haga clic en la acción.

Trabajar con cargas de trabajo agregadas

Además de las acciones estándar integradas en la consola de Cyber Protect, puede ejecutar las siguientes operaciones con las cargas de trabajo agregadas: ver detalles, deshacer unión de cargas de trabajo de origen y ejecutar acciones personalizadas configuradas en las CyberApps.

© Acronis International GmbH, 2003-2025

Ver detalles

Requisitos previos

- Hay al menos una carga de trabajo agregada disponible para el inquilino.

Pasos para consultar los detalles de una carga de trabajo agregada

1. En la pantalla **Todos los dispositivos**, haga clic en la carga de trabajo agregada.
2. Haga clic en **Detalles**.
   Los detalles de la carga de trabajo agregada están separadas en pestañas. Cada pestaña muestra la información de cada representación de la carga de trabajo.

Deshacer unión

Requisitos previos

- Hay al menos una carga de trabajo agregada disponible para el inquilino.

Cuando deshace la unión de una carga de trabajo agregada, ya no se mostrará en la lista de dispositivos. En su lugar, verá una entrada individual para cada carga de trabajo de origen que se ha unido en la carga de trabajo agregada.

Pasos para deshacer la unión de una carga de trabajo agregada

1. En la pantalla **Todos los dispositivos**, haga clic en la carga de trabajo agregada de la que desee deshacer la unión.
2. Haga clic en **Deshacer unión de cargas de trabajo de origen**.
3. Haga clic en **Deshacer unión** en la ventana de confirmación.

Realizar acciones personalizadas

Requisitos previos

- Hay al menos una integración de CyberApp que tiene definidas **Acciones de carga de trabajo** habilitadas para el inquilino.

Las acciones personalizadas son acciones configuradas en CyberApps y que se vuelven disponibles para la correspondiente carga de trabajo de CyberApp cuando habilita la integración de CyberApp para el inquilino.

Pasos para realizar acciones personalizadas

1. En la pantalla **Todos los dispositivos**, haga clic en la carga de trabajo.
2. Haga clic en **Acciones integradas de la aplicación**.
3. Realice una de las siguientes acciones según las acciones personalizadas disponibles:
   - Si la carga de trabajo agregada tiene una carga de trabajo de CyberApp, haga clic en la acción.
   - Si la carga de trabajo agregada tiene más de una carga de trabajo de CyberApp, haga clic en el nombre de la CyberApp y, a continuación, haga clic en la acción.

© Acronis International GmbH, 2003-2025

Vinculación de cargas de trabajo a usuarios específicos

Nota
Esta característica solo está disponible si se ha habilitado el servicio PSA.

Al enlazar una carga de trabajo a un usuario específico, puede vincular automáticamente la carga de trabajo a los nuevos tickets del centro de asistencia creados por el usuario o asignados a este.

Pasos para enlazar una carga de trabajo a un usuario

1. Vaya a **Dispositivos** > **Todos los dispositivos** y seleccione la carga de trabajo que corresponda.
2. En el panel **Acciones**, seleccione **Enlazar a un usuario**.
3. Seleccione el usuario correspondiente.
   También puede cambiar el usuario seleccionado para las cargas de trabajo enlazadas existentes, según sea necesario.
4. Haga clic en **Listo**.
   El usuario seleccionado se muestra ahora en la columna **Usuario enlazado**.

Pasos para dejar de enlazar una carga de trabajo a un usuario

1. Vaya a **Dispositivos** > **Todos los dispositivos** y seleccione la carga de trabajo que corresponda.
2. En el panel **Acciones**, seleccione **Enlazar a un usuario**.
3. Haga clic en **Desenlazar usuario**.
4. Haga clic en **Listo**.

Viendo el último usuario que ha iniciado sesión

Si activa el ajuste **Mostrar último inicio de sesión** en el plan de administración remota que se aplica a una carga de trabajo, el sistema registrará información sobre los usuarios que inician sesión en el dispositivo. Puede ver esta información en el panel de control o en los detalles de la carga de trabajo.

Para más información sobre el ajuste **Mostrar último inicio de sesión**, consulte Planes de administración remota.

Pasos para ver el usuario que inició sesión por última vez en un dispositivo

1. Haga clic en **Dispositivos**.
   Se abre la pantalla **Todos los dispositivos**. En la columna **Último inicio de sesión**, puede ver el nombre del usuario que inició sesión por última vez en cada dispositivo. En la columna **Última hora de inicio de sesión**, compruebe la hora en que el usuario inició sesión por última vez en cada dispositivo.
2. Haga clic en un dispositivo cuyos detalles quiera comprobar.

© Acronis International GmbH, 2003-2025

3. Haga clic en el icono **Detalles**.
4. En la sección **Últimos usuarios que iniciaron sesión**, compruebe el nombre de usuario que inició sesión por última vez en el dispositivo y la fecha y hora del último inicio de sesión.

Nota
El sistema lista hasta 5 usuarios diferentes que iniciaron sesión por última vez en el dispositivo.

#CyberFit Score para equipos

#CyberFit Score le proporciona una evaluación de seguridad y un mecanismo de puntuación que valora el estado de seguridad de su equipo. Identifica huecos de seguridad en el entorno de TI y vectores de ataque abiertos contra los endpoints, y ofrece recomendaciones mediante un informe acciones de mejora. Esta característica se encuentra disponible en todas las ediciones de Cyber Protect.

La funcionalidad #CyberFit Score es compatible en:

- Windows 7 (primera versión) y versiones posteriores
- Windows Server 2008 R2 y versiones posteriores

Cómo funciona

El agente de protección instalado en un equipo realiza una evaluación de seguridad y calcula el #CyberFit Score para dicho equipo. El #CyberFit Score de un equipo se recalcula de forma automática y periódica.

Mecanismo de puntuación de #CyberFit Score

El #CyberFit Score de un equipo se calcula en función de los parámetros siguientes:

- Protección antimalware 0-275
- Protección de la copia de seguridad 0-175
- Cortafuegos 0-175
- Red privada virtual (VPN) 0-75
- Cifrado de disco completo 0-125
- Seguridad de red 0-25

El valor máximo de #CyberFit Score para un equipo es de 850.

Parámetro	¿Qué es lo que se evalúa?	Recomendaciones para los usuarios	Puntuación
Antimalware	El agente comprueba si hay software	Hallazgos: • Tiene la protección antimalware habilitada (+275 puntos)	275: hay software antimalware instalado en un

© Acronis International GmbH, 2003-2025

	antimalware instalado en un equipo.	• No tiene protección antimalware; su sistema puede estar en peligro (0 puntos) Recomendaciones de #CyberFit Score: Debería tener una solución antimalware instalada y habilitada en su equipo para protegerse frente a riesgos de seguridad. Consulte sitios web como AV-Test o AV-Comparatives para ver una lista de soluciones antimalware recomendadas.	equipo 0: no hay software antimalware instalado en un equipo
Copia de seguridad	El agente comprueba si hay una solución de copia de seguridad instalada en una máquina.	Hallazgos: • Tiene una solución de copia de seguridad que protege sus datos (+175 puntos) • No se ha encontrado ninguna solución de copia de seguridad; sus datos pueden estar en peligro (0 puntos) Recomendaciones de #CyberFit Score: Le recomendamos que realice con regularidad una copia de seguridad de su información para prevenir la pérdida de datos o los ataques de ransomware. A continuación se indican algunas soluciones de copia de seguridad que debería considerar: • Acronis Cyber Protect/Cyber Backup/True Image • Copias de seguridad de Windows Server (Windows Server 2008 R2 y versiones posteriores)	175: hay una solución de copia de seguridad instalada en un equipo 0: no hay una solución de copia de seguridad instalada en un equipo
Cortafuegos	El agente comprueba si hay un cortafuegos disponible y habilitado en su entorno. El agente hace lo siguiente: 1. Comprueba el cortafuegos de Windows y la protección de red para ver si hay activado algún	Hallazgos: • Tiene un cortafuegos habilitado para las redes públicas y privadas, o se ha encontrado una solución cortafuegos de terceros (+175 puntos) • Tiene un cortafuegos habilitado únicamente para las redes públicas (+100 puntos) • Tiene un cortafuegos habilitado únicamente para las redes privadas (+75 puntos) • No tiene ningún cortafuegos habilitado; su conexión de red no está protegida (0 puntos) Recomendaciones de #CyberFit Score:	100: el cortafuegos público de Windows está habilitado 75: el cortafuegos privado de Windows está habilitado 175: el cortafuegos público y privado de Windows está habilitado

© Acronis International GmbH, 2003-2025

	cortafuegos público. 2. Comprueba el cortafuegos de Windows y la protección de red para ver si hay activado algún cortafuegos privado. 3. Si los cortafuegos público y privado de Windows están deshabilitados, comprueba si hay alguna solución cortafuegos o agente de terceros.	Le recomendamos que habilite un cortafuegos para sus redes públicas y privadas con el fin de mejorar la seguridad frente a ataques maliciosos contra su sistema. A continuación encontrará guías detalladas sobre cómo configurar su cortafuegos de Windows en función de sus necesidades de seguridad y la arquitectura de la red: Guías para usuarios finales/empleados: Cómo configurar el cortafuegos de Windows Defender en su equipo Cómo configurar el cortafuegos de Windows en su equipo Guías para administradores del sistema e ingenieros: Cómo implementar el cortafuegos de Windows Defender con una mayor seguridad Cómo crear reglas avanzadas en el cortafuegos de Windows	O hay habilitado un cortafuegos de terceros 0: ni un cortafuegos de Windows ni una solución de cortafuegos de terceros están habilitados
Red privada virtual (VPN)	El agente comprueba si hay alguna solución VPN instalada en un equipo, y si está habilitada y en funcionamiento.	Hallazgos: • Tiene una solución de VPN y puede recibir y enviar datos de forma segura entre redes públicas y compartidas (+75 puntos) • No se ha encontrado ninguna solución de VPN; su conexión a las redes públicas y compartidas no está protegida (0 puntos) Recomendaciones de #CyberFit Score: Le recomendamos que utilice una VPN para acceder a su red empresarial y sus datos confidenciales. Es esencial que utilice una VPN para mantener sus comunicaciones protegidas y privadas, especialmente si utiliza el acceso gratuito a Internet de una cafetería, una biblioteca, un aeropuerto, etcétera. A continuación se indican algunas soluciones VPN que debería considerar: • Acronis Business VPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear	75: la VPN está habilitada y en funcionamiento 0: la VPN no está habilitada

© Acronis International GmbH, 2003-2025

		• ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
Cifrado de disco	El agente comprueba si un equipo tiene habilitado el cifrado de disco. El agente comprueba si BitLocker de Windows está activado.	Hallazgos: • Tiene habilitado el cifrado del disco completo; su equipo está protegido frente a alteraciones físicas (+125 puntos) • Solo están cifrados algunos discos duros; su equipo puede estar en peligro de ser alterado físicamente (+75 puntos) • No se ha encontrado ningún cifrado de disco; su equipo está en peligro de ser alterado físicamente (0 puntos) Recomendaciones de #CyberFit Score: Le recomendamos que active Windows BitLocker para mejorar la protección de sus datos y archivos. Guía: Cómo activar el cifrado del dispositivo en Windows	125: todos los discos están cifrados 75: al menos uno de sus discos está cifrado, aunque también hay discos sin cifrar 0: ningún disco está cifrado
Seguridad de red (tráfico NTLM saliente a servidores remotos)	El agente comprueba si un equipo tiene restringido el tráfico NTLM saliente a servidores remotos.	Hallazgos: • Se ha denegado el tráfico NTLM saliente a servidores remotos; sus credenciales están protegidas (+25 puntos) • No se ha denegado el tráfico NTLM saliente a servidores remotos; sus credenciales pueden ser vulnerables a la exposición (0 puntos) Recomendaciones de #CyberFit Score: Para mejorar la protección de seguridad, le recomendamos que deniegue todo el tráfico NTLM saliente a servidores remotos. En el vínculo siguiente puede encontrar información acerca de cómo se cambia la configuración	25: el tráfico NTLM saliente está establecido en DenyAll 0: el tráfico NTLM saliente está establecido en otro valor

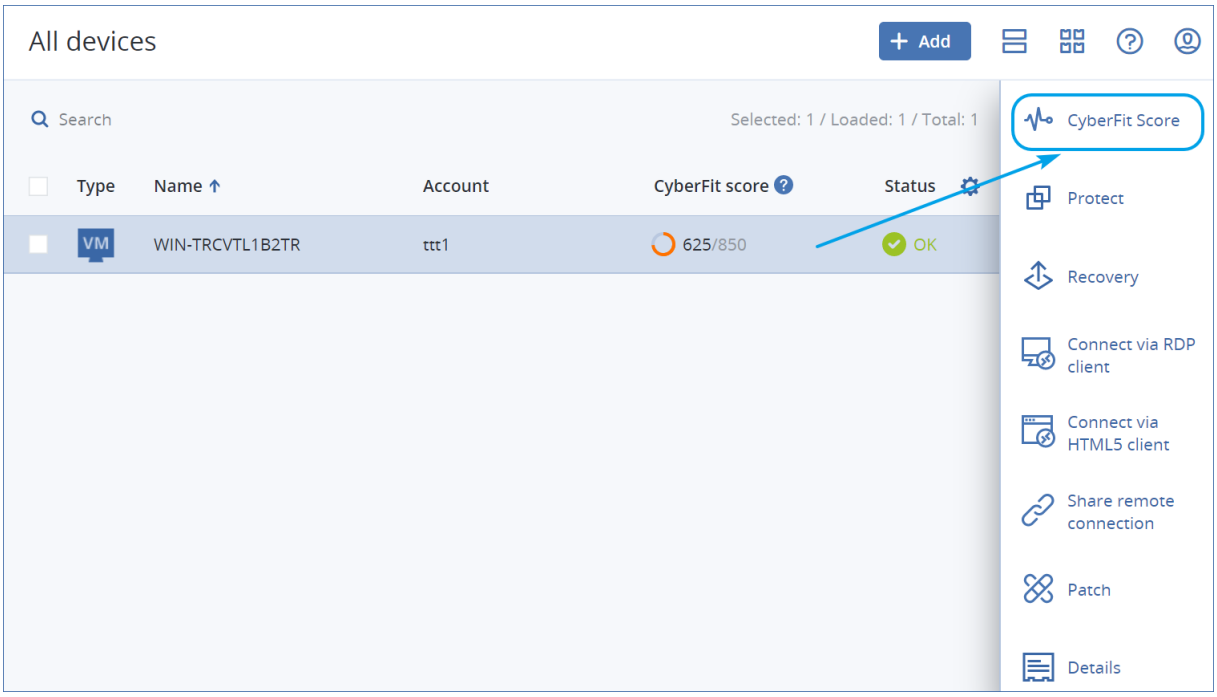
© Acronis International GmbH, 2003-2025

		NTLM y cómo se añaden excepciones. Guía: Restringir tráfico NTLM saliente a servidores remotos	

Una vez sumados los puntos obtenidos en cada métrica, se calcula el #CyberFit Score total de un equipo, cuyos valores se pueden dividir en las siguientes franjas para reflejar el nivel de protección de los endpoints:

- 0-579: Malo
- 580-669: Razonable
- 670-739: Bueno
- 740-799: Muy bueno
- 800-850: Excelente

Para ver el #CyberFit Score de sus equipos en la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**. En la lista de dispositivos, verá la columna **#CyberFit Score**. También puede ejecutar un análisis #CyberFit Score de un equipo para comprobar su postura de seguridad.



También puede obtener información sobre el #CyberFit Score en el widget y en las páginas del informe.

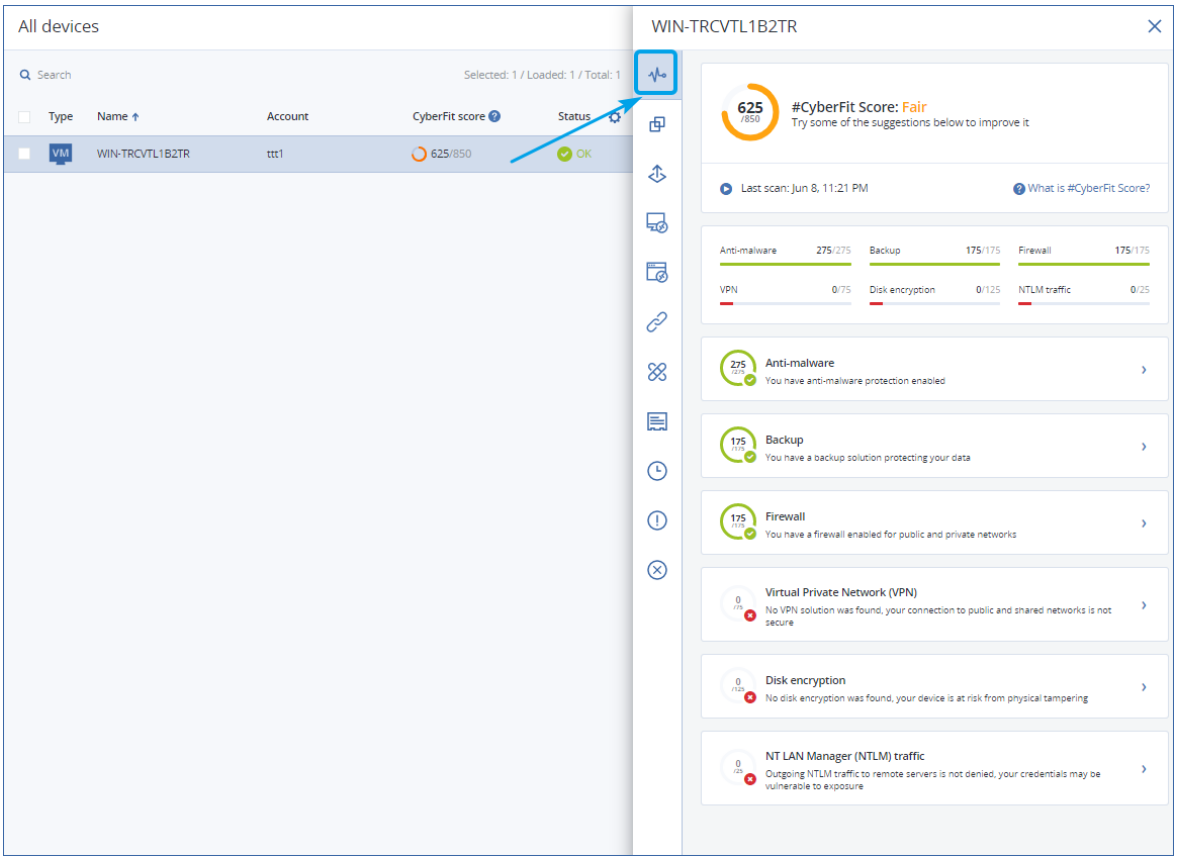
Ejecución de un análisis #CyberFit Score

Para ejecutar un análisis #CyberFit Score

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Seleccione el equipo y haga clic en **#CyberFit Score**.

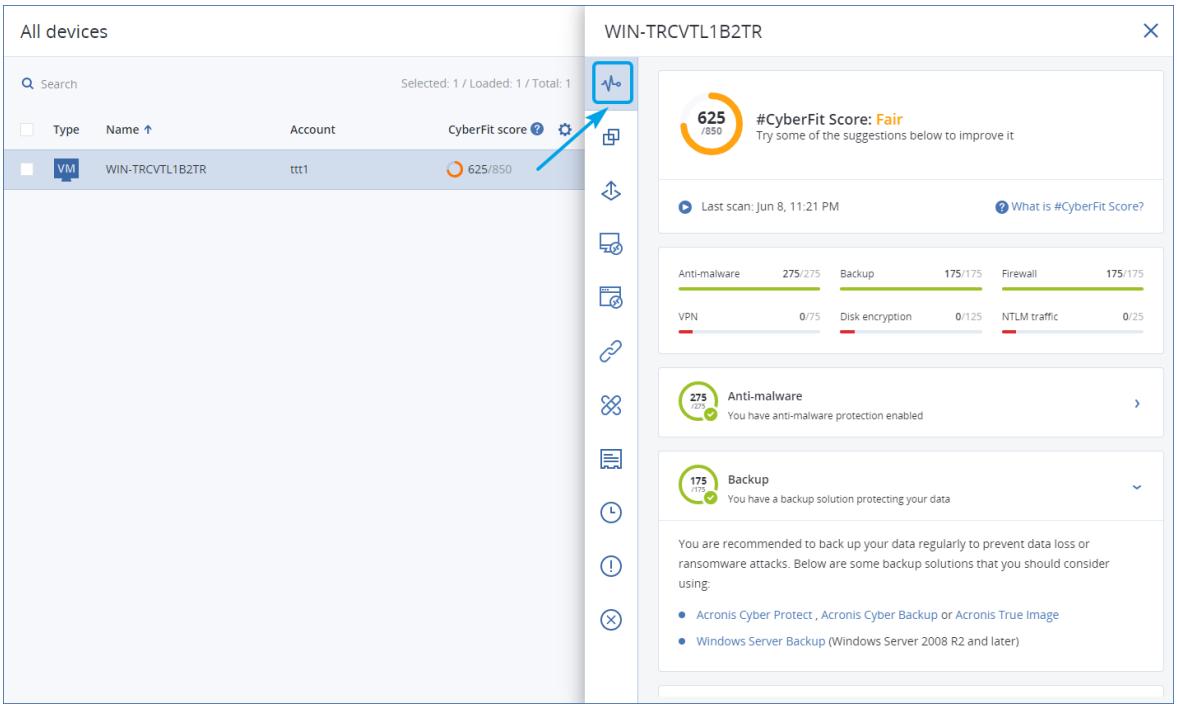
© Acronis International GmbH, 2003-2025

3. Si nunca se ha analizado el equipo, haga clic en **Ejecutar un primer análisis**.
4. Una vez completado el análisis, verá el #CyberFit Score total del equipo, junto con la puntuación de los seis parámetros evaluados: Antimalware, Copia de seguridad, Cortafuegos, Red privada virtual (VPN), Cifrado del disco y tráfico NT LAN Manager (NTLM).



5. Para comprobar cómo puede aumentar la puntuación de las métrica cuya configuración de seguridad puede mejorarse, expanda la sección correspondiente y lea las recomendaciones.

© Acronis International GmbH, 2003-2025



6. Después de seguir las recomendaciones, puede recalcular el #CyberFit Score del equipo haciendo clic en el botón de la flecha, justo debajo del #CyberFit Score total.

Secuencia de comandos cibernética

Con Cyber Scripting, puede usar secuencias de comandos para automatizar operaciones rutinarias en máquinas Windows y macOS de su entorno, como instalar software, modificar configuraciones, iniciar o detener servicios y crear cuentas. Así, puede disminuir el tiempo que invierte en dichas operaciones y reducir el riesgo de error al realizarlas manualmente.

Cyber Scripting está disponible para administradores y usuarios a nivel de cliente, así como para administradores de partners (proveedores de servicios). Para obtener más información sobre los diferentes niveles de administración, consulte "Niveles de administración en la consola de Cyber Protect" (p. 373).

Las secuencias de comandos que puede usar deben aprobarse con anticipación. Solo los administradores con el rol de **Administrador de cibernética** pueden aprobar y probar nuevas secuencias de comandos. Para obtener más información sobre cómo cambiar el estado de las secuencias de comandos, consulte "Cambio del estado de la secuencia de comandos" (p. 486).

Según su rol de usuario, puede realizar diferentes operaciones con secuencias de comandos y planes de programación. Para obtener más información sobre los roles, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

Requisitos previos

- La funcionalidad de Cyber Scripting requiere la licencia RMM (modo de licencia basado en servicios) o la licencia de Seguridad y RMM (modo de licencia basado en soluciones).

© Acronis International GmbH, 2003-2025

- Para utilizar todas las funciones de la Programación cibernética, como la edición de secuencias de comandos, la ejecución de secuencias de comandos, la creación de planes de programación, etc., debe habilitar la autenticación de doble factor para su cuenta.

Limitaciones

- Se admiten estos lenguajes de programación:
  - PowerShell
  - Bash
- Las operaciones de la Programación cibernética solo pueden ejecutarse en equipos de destino con un agente de protección instalado.

Plataformas compatibles

La Programación cibernética está disponible para cargas de trabajo de Windows y macOS.

La siguiente tabla resume las versiones compatibles.

Sistema operativo	Versión
Windows	Windows 7 SP1 y posteriores: todas las ediciones
	Windows 8/8.1: todas las ediciones (x86, x64), excepto las ediciones Windows RT
	Windows 10: ediciones Home, Pro, Education, Enterprise, IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 y posteriores: ediciones Standard, Enterprise, Datacenter, Foundation y Web
	Windows Server 2012/2012 R2: todas las ediciones
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

© Acronis International GmbH, 2003-2025

Roles de usuario y derechos de la Programación cibernética

Las acciones disponibles con secuencias de comandos y planes de programación dependen del estado de la secuencia de comandos y de su rol de usuario.

Los administradores pueden gestionar objetos, como planes o cargas de trabajo, en sus propios inquilinos y en sus inquilinos secundarios, con las siguientes limitaciones:

- Los inquilinos de clientes pueden restringir el acceso a los administradores de partners.
- Los administradores de clientes y los administradores de partners que gestionan el inquilino de clientes principal pueden acceder a las unidades en todo momento.

Los administradores no pueden ver ni acceder a objetos en un nivel superior al de su propio inquilino.

Los administradores de nivel inferior tienen acceso de solo lectura a los planes de programación de sus cargas de trabajo a través de un administrador de nivel superior.

Estos roles proporcionan derechos con respecto a la Programación cibernética:

- **Administrador de la empresa**
  Este rol concede todos los derechos de administrador en todos los servicios. Con respecto a la Programación cibernética, concede los mismos derechos que el rol de administrador de cibernética.
- **Administrador de cibernética**
  Este rol otorga todos los derechos, incluida la aprobación de las secuencias de comandos que pueden utilizarse en el inquilino y la capacidad de ejecutar secuencias de comandos con el estado **Probando**.
- **Administrador**
  Este rol concede permisos parciales con la capacidad de ejecutar secuencias de comandos aprobadas y de crear y ejecutar planes de programación que utilizan secuencias de comandos aprobadas.
- **Administrador de solo lectura**
  Este rol concede permisos limitados con la capacidad de ver las secuencias de comandos y los planes de protección que utiliza el inquilino.
- **Usuario**
  Este rol concede permisos parciales, con la capacidad de ejecutar secuencias de comandos aprobadas y de crear y ejecutar planes de programación que utilizan secuencias de comandos aprobadas, pero solo en el equipo propiedad del usuario.

La siguiente tabla resume todas las acciones disponibles según el estado de la secuencia de comandos y el rol de usuario.

© Acronis International GmbH, 2003-2025

Rol	Objeto	Estado de la secuencia de comandos		
		Borrador	**Probando**	**Aprobado**
Administrador de cibernética **Administrador de la empresa**	Plan de programación	Editar (Eliminar un borrador de secuencia de comandos de un plan) Eliminar Revoque Deshabilitar Detener	Crear Editar Aplicar Habilitar Ejecutar Eliminar Revoque Deshabilitar Detener	Crear Editar Aplicar Habilitar Ejecutar Eliminar Revoque Deshabilitar Detener
	Secuencia de comandos	Crear Editar Cambiar estado Clonar Eliminar Cancelar ejecución	Crear Editar Cambiar estado Ejecutar Clonar Eliminar Cancelar ejecución	Crear Editar Cambiar estado Ejecutar Clonar Eliminar Cancelar ejecución
Administrador **Usuario** (para sus propias cargas de trabajo)	Plan de programación	Vista Editar Revoque Deshabilitar Detener	Vista Cancelar ejecución	Crear Editar Aplicar Habilitar Ejecutar Eliminar Revoque Deshabilitar Detener
	Secuencia de comandos	Crear Editar Clonar	Vista Clonar Cancelar	Ejecutar Clonar Cancelar

© Acronis International GmbH, 2003-2025

		Eliminar Cancelar ejecución	ejecución	ejecución
Administrador de solo lectura	Plan de programación	Vista	Vista	Vista
	Secuencia de comandos	Vista	Vista	Vista

Secuencias de comandos

Una secuencia de comandos es un conjunto de instrucciones que se interpretan en el tiempo de ejecución y se ejecutan en un equipo de destino. Ofrece una solución adecuada para automatizar las tareas repetitivas o complejas.

Con Cyber Scripting, puede ejecutar una secuencia de comandos predefinida o crear una personalizada. Puede ver todas las secuencias de comandos que están disponibles en **Gestión** > **Repositorio de secuencias de comandos**. Las secuencias de comandos predefinidas se encuentran en la sección **Biblioteca**. Las secuencias de comandos que ha creado o clonado en su inquilino se encuentran en la sección **Mis secuencias de comandos**.

Puede usar una secuencia de comandos si la incluye en un plan de programación o realiza una operación de **Ejecución rápida de secuencias de comandos**.

Nota
Solo puede usar secuencias de comandos aprobadas que se crearon en su inquilino o que se clonaron en él. Si se eliminó una secuencia de comandos del repositorio o está en estado de **Borrador**, no se ejecutará. Puede verificar los detalles de una operación de secuencias de comando o cancelarla en **Supervisión** > **Actividades**.

La siguiente tabla proporciona más información sobre las posibles acciones con una secuencia de comandos, según su estado.

Estado	Posibles acciones
Borrador	Las nuevas secuencias de comandos que crea y las que clona en su repositorio están en estado de **Borrador**. No puede ejecutar estas secuencias de comandos o incluirlas en planes de programación.
Probando	Los administradores con el rol de **Administrador de cibernética** pueden ejecutar estas secuencias de comandos e incluirlas en planes de programación.
Aprobado	Puede ejecutar estas secuencias de comandos e incluirlas en planes de programación.

© Acronis International GmbH, 2003-2025

Solo los administradores con el rol de **Administrador de cibernética** pueden cambiar el estado de una secuencia de comandos o eliminar una secuencia de comandos aprobada. Para obtener más información, vea "Cambio del estado de la secuencia de comandos" (p. 486).

Creación de una secuencia de comandos

Puede crear una secuencia de comandos mediante la escritura manual del código.

Pasos para crear una secuencia de comandos

1. En la consola de Cyber Protect, vaya a **Gestión** > **Depósito de secuencias de comandos**.
2. En **Mis secuencias de comandos**, haga clic en **Crear secuencia de comandos con IA**.
3. En el panel principal, escriba el cuerpo de la secuencia de comandos.

   Importante
   Cuando cree una secuencia de comandos, incluya comprobaciones de código de salida para cada operación. De lo contrario, podría ignorarse una operación fallida y el estado de la actividad de programación en **Supervisión** > **Actividades** podría mostrarse como **Correcto** de forma errónea.

4. Especifique la configuración de la secuencia de comandos.

Configuración	Descripción
Nombre de secuencia de comandos	Nombre de la secuencia de comandos. El campo se rellena automáticamente, pero puede cambiar el valor.
Descripción	Descripción de la secuencia de comandos. Esta configuración es opcional. [Para secuencias de comandos generadas por IA] El campo se llenará automáticamente al generar la secuencia de comandos. Puede editar la descripción proporcionada por la IA.
Idioma	Idioma de la secuencia de comandos. Los valores disponibles son: • **PowerShell**. Este es el valor predeterminado. • **Bash** [Para secuencias de comandos generadas por IA] Esta configuración se realiza antes de la generación de la secuencia de comandos.
Sistema operativo	Sistema operativo que está instalado en la carga de trabajo objetivo en la que se ejecutará la secuencia de comandos. Los valores disponibles son: • **Windows**. Este es el valor predeterminado. • **macOS** [Para secuencias de comandos generadas por IA] Esta configuración se realiza antes de la generación de la secuencia de comandos.
Estado	Estado de la secuencia de comandos.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	• **Borrador**. Este es el valor predeterminado. Las nuevas secuencias de comandos que crea y las que clona en su repositorio están en el estado de **Borrador**. No se le permite ejecutar secuencias de comandos en **Borrador** o incluirlas en planes de programación. • **En pruebas**. Solo los administradores con el rol de **Administrador de cibernética** pueden cambiar el estado de una secuencia de comandos a **En pruebas**, ejecutar secuencias de comandos en el estado de **En pruebas** y ejecutar planes de programación con dichas secuencias de comandos. • **Aprobada**. Puede ejecutar secuencias de comandos **Aprobadas** e incluirlas en planes de programación. Solo los administradores con el rol de **Administrador de cibernética** pueden cambiar el estado de una secuencia de comandos o eliminar una secuencia de comandos aprobada. Para obtener más información, vea "Cambio del estado de la secuencia de comandos" (p. 486).
Etiquetas	Las etiquetas no distinguen mayúsculas de minúsculas y pueden tener una longitud de 32 caracteres como máximo. No puede utilizar paréntesis, corchetes, comas ni espacios. Esta configuración es opcional. [Para secuencias de comandos generadas por IA] La etiqueta **Generada por IA** se añadirá automáticamente al generar la secuencia de comandos. Puede eliminar manualmente esta etiqueta o añadir más etiquetas.

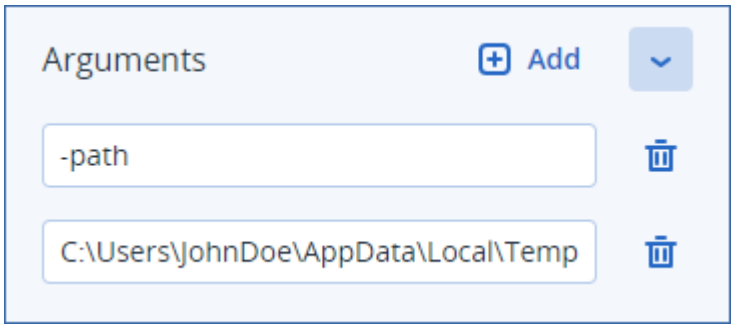
5. [Solo para las secuencias de comandos que requieran credenciales] Especifique las credenciales.
   Puede utilizar una credencial única (por ejemplo, un token) o un par de credenciales (por ejemplo, un nombre de usuario y una contraseña).
6. [Solo para las secuencias de comandos que requieran argumentos] Especifique los argumentos y sus valores del siguiente modo:
   a. Haga clic en **Agregar**.
   b. En el campo **Añadir argumentos**, especifique el argumento.
   c. Haga clic en **Agregar**.
   d. En el segundo campo que aparece, especifique el valor del argumento.

© Acronis International GmbH, 2003-2025

Nota
Solo puede especificar argumentos que ya haya definido en el cuerpo de la secuencia de comandos.



Por ejemplo:



e. Si necesita agregar más de un argumento, repita los pasos anteriores.

7. Haga clic en **Guardar**.

La secuencia de comandos se guarda en su repositorio con el estado **Borrador**.

No puede usar la secuencia de comandos hasta que un administrador con el rol de **Administrador de cibernética** cambie su estado a **Aprobada**. Para obtener más información, consulte "Cambio del estado de la secuencia de comandos" (p. 486).

Para usar una secuencia de comandos en otro inquilino que administre, debe clonar la secuencia de comandos en ese inquilino. Para obtener más información, consulte "Clonación de una secuencia de comandos" (p. 484).

Creación de una secuencia de comandos con IA

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede usar la IA para transformar indicaciones en secuencias de comandos potentes, lo que le ahorrará tiempo y esfuerzo. Puede usar la funcionalidad de las siguientes maneras:

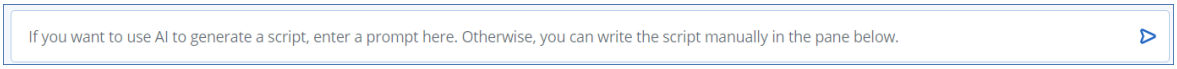
© Acronis International GmbH, 2003-2025

- Introduzca una solicitud para pedirle a la IA que genere una secuencia de comandos desde cero.
- Introduzca una solicitud para pedirle a la IA que revise y complete un código que ha introducido en el cuerpo de la secuencia de comandos. Puede utilizar esta capacidad cuando se ha enfrentado a códigos más complejos.

La funcionalidad utiliza el modelo GPT-4 de OpenAI. Puede usarla para crear hasta 100 secuencias de comandos para su organización al mes, sin ningún coste.

Pasos para crear una secuencia de comandos con IA

1. En la consola de Cyber Protect, vaya a **Gestión** > **Depósito de secuencias de comandos**.
2. En **Mis secuencias de comandos**, haga clic en **Crear una secuencia de comandos con IA**.
3. En al entrada, introduzca una descripción de lo que debería hacer la secuencia de comandos. Asegúrese de que la descripción que introduzca sea lo más clara y detallada posible.

   Por ejemplo:

   ```
   I need a script that deletes Temporary files for all users (including user profiles + Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. En la entrada, haga clic en el botón de la flecha.
5. En la ventana de confirmación, seleccione Idioma y Sistema operativo, y luego haga clic en **Generar**.

   La secuencia de comandos que genera la IA se muestra en el panel principal. El nombre y la descripción de la secuencia de comandos se generan automáticamente por la IA para que coincidan con la secuencia de comandos. La etiqueta **Generada por IA** se asigna automáticamente a la secuencia de comandos.
6. Revise la secuencia de comandos que generó la IA y, si es necesario, edítela manualmente.
7. Si es necesario, edite la configuración de la secuencia de comandos.

Configuración	Descripción
Nombre de secuencia de comandos	Nombre de la secuencia de comandos. El campo se rellena automáticamente, pero puede cambiar el valor.
Descripción	Descripción de la secuencia de comandos. Esta configuración es opcional. [Para secuencias de comandos generadas por IA] El campo se llenará automáticamente al generar la secuencia de comandos. Puede editar la descripción proporcionada por la IA.
Idioma	Idioma de la secuencia de comandos. Los valores disponibles son: • **PowerShell**. Este es el valor predeterminado. • **Bash** [Para secuencias de comandos generadas por IA] Esta configuración se realiza

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	antes de la generación de la secuencia de comandos.
Sistema operativo	Sistema operativo que está instalado en la carga de trabajo objetivo en la que se ejecutará la secuencia de comandos. Los valores disponibles son: • **Windows**. Este es el valor predeterminado. • **macOS** [Para secuencias de comandos generadas por IA] Esta configuración se realiza antes de la generación de la secuencia de comandos.
Estado	Estado de la secuencia de comandos. • **Borrador**. Este es el valor predeterminado. Las nuevas secuencias de comandos que crea y las que clona en su repositorio están en el estado de **Borrador**. No se le permite ejecutar secuencias de comandos en **Borrador** o incluirlas en planes de programación. • **En pruebas**. Solo los administradores con el rol de **Administrador de cibernética** pueden cambiar el estado de una secuencia de comandos a **En pruebas**, ejecutar secuencias de comandos en el estado de **En pruebas** y ejecutar planes de programación con dichas secuencias de comandos. • **Aprobada**. Puede ejecutar secuencias de comandos **Aprobadas** e incluirlas en planes de programación. Solo los administradores con el rol de **Administrador de cibernética** pueden cambiar el estado de una secuencia de comandos o eliminar una secuencia de comandos aprobada. Para obtener más información, vea "Cambio del estado de la secuencia de comandos" (p. 486).
Etiquetas	Las etiquetas no distinguen mayúsculas de minúsculas y pueden tener una longitud de 32 caracteres como máximo. No puede utilizar paréntesis, corchetes, comas ni espacios. Esta configuración es opcional. [Para secuencias de comandos generadas por IA] La etiqueta **Generada por IA** se añadirá automáticamente al generar la secuencia de comandos. Puede eliminar manualmente esta etiqueta o añadir más etiquetas.

8. [Opcional] [Solo para las secuencias de comandos que requieran credenciales] Especifique las credenciales.

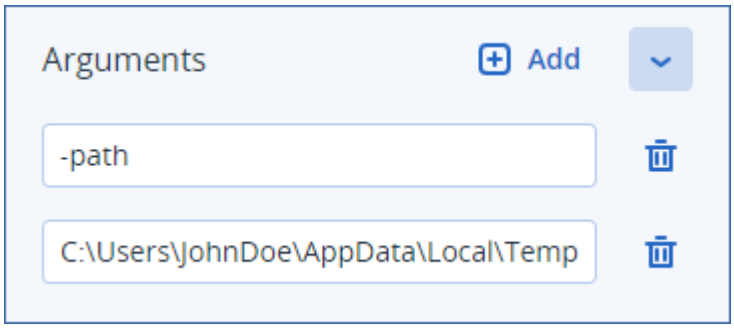
   Puede utilizar una credencial única (por ejemplo, un token) o un par de credenciales (por ejemplo, un nombre de usuario y una contraseña).
9. [Solo para las secuencias de comandos que requieran argumentos] Especifique los argumentos y sus valores del siguiente modo:
   a. Haga clic en **Agregar**.
   b. En el campo **Añadir argumentos**, especifique el argumento.
   c. Haga clic en **Agregar**.
   d. En el segundo campo que aparece, especifique el valor del argumento.

© Acronis International GmbH, 2003-2025

Nota
Solo puede especificar argumentos que ya haya definido en el cuerpo de la secuencia de comandos.



Por ejemplo:



e. Si necesita agregar más de un argumento, repita los pasos anteriores.

10. Haga clic en **Guardar**.
    La secuencia de comandos se guarda en su repositorio con el estado **Borrador**.
    No puede usar la secuencia de comandos hasta que un administrador con el rol de **Administrador de cibernética** cambie su estado a **Aprobada**. Para obtener más información, consulte "Cambio del estado de la secuencia de comandos" (p. 486).
    Para usar una secuencia de comandos en otro inquilino que administre, debe clonar la secuencia de comandos en ese inquilino. Para obtener más información, consulte "Clonación de una secuencia de comandos" (p. 484).

Clonación de una secuencia de comandos

Se debe clonar una secuencia de comandos en los siguientes casos:

- Antes de usar una secuencia de comandos de la **Biblioteca**. En este caso, primero debe clonar la secuencia de comandos en la sección **Mis secuencias de comandos**.
- Cuando quiera clonar secuencias de comandos que creó en un inquilino principal a sus unidades o inquilinos secundarios.

Pasos para clonar una secuencia de comandos

© Acronis International GmbH, 2003-2025

1. En **Depósito de secuencias de comandos**, busque la secuencia de comandos que desee clonar.
2. Realice uno de los siguientes procedimientos:
   - [Si clona una secuencia de comandos desde **Mis secuencias de comandos**] Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre de la secuencia de comandos y, a continuación, haga clic en **Clonar**.
   - [Si clona una secuencia de comandos desde la **Biblioteca**] Haga clic en **Clonar** junto al nombre de la secuencia de comandos que ha seleccionado.
3. En la ventana emergente **Clonar secuencia de comandos**, seleccione uno de los siguientes estados de secuencia de comandos de la lista desplegable **Estado**:
   - **Borrador** (de forma predeterminada): este estado no le permite ejecutar la secuencia de comandos directamente.
   - **Probando**: este estado le permite ejecutar la secuencia de comandos.
   - **Aprobado**: este estado le permite ejecutar la secuencia de comandos.
4. [Si gestiona más de un inquilino o unidad] Seleccione dónde desea clonar la secuencia de comandos.

   En el cuadro de diálogo **Clonar secuencia de comandos**, solo verá los inquilinos que puede gestionar y que tienen la licencia RMM (modelo de licencia basado en servicios) o Seguridad y RMM (modelo de licencia basado en soluciones).

Como resultado, se clona la secuencia de comandos en la sección **Mis secuencias de comandos** del inquilino o la unidad que haya seleccionado. Si gestiona solo un inquilino sin unidades, la secuencia de comandos se copia automáticamente a su sección **Mis secuencias de comandos**.

Importante
Las credenciales que utiliza una secuencia de comandos no se copian al clonarla en un inquilino que no sea original.

Edición o eliminación de una secuencia de comandos

Nota
Según su rol de usuario, puede realizar diferentes operaciones con secuencias de comandos y planes de programación. Para obtener más información sobre los roles, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

Pasos para editar una secuencia de comandos

1. En **Depósito de secuencias de comandos**, vaya a **Mis secuencias de comandos** y busque la secuencia de comandos que desee editar.
2. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre de la secuencia de comandos y, a continuación, haga clic en **Editar**.
3. Edite la secuencia de comandos y haga clic en **Guardar**.
4. [Si edita una secuencia de comandos que utiliza un plan de programación] Confirme su elección haciendo clic en **Guardar secuencia de comandos**.

© Acronis International GmbH, 2003-2025

Nota
La versión más reciente de la secuencia de comandos se utilizará la próxima vez que se ejecute el plan de programación.

Versiones de la secuencia de comandos

Se creará una nueva versión de la secuencia de comandos si edita cualquiera de los atributos de la secuencia de comandos que se indican a continuación:

- cuerpo de la secuencia de comandos
- nombre de la secuencia de comandos
- descripción
- idioma de la secuencia de comandos
- credenciales
- argumentos

Si cambia otros atributos, se añadirán las ediciones a la versión actual de la secuencia de comandos. Para obtener más información acerca de las versiones y cómo compararlas, consulte "Comparación de versiones de secuencias de comandos" (p. 487).

Nota
La secuencia de comandos se actualiza solo cuando modifica el valor en el campo **Estado**. Solo los administradores con el rol de administrador de cibernética pueden cambiar el estado de una secuencia de comandos.

Pasos para eliminar una secuencia de comandos

1. En **Depósito de secuencias de comandos**, vaya a **Mis secuencias de comandos** y busque la secuencia de comandos que desee eliminar.
2. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre de la secuencia de comandos y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Eliminar**.
4. [Si desea eliminar una secuencia de comandos que utiliza un plan de programación] Confirme su elección haciendo clic en **Guardar secuencia de comandos**.

Nota
Los planes de programación que utilicen la secuencia de comandos eliminada no se ejecutarán.

Cambio del estado de la secuencia de comandos

Una nueva secuencia de comandos que se crea y está en el estado de **Borrador** no puede utilizarse hasta que su estado cambie a **Aprobado**. Según el caso de uso, una secuencia de comandos podría estar en estado de **Pruebas** durante un periodo antes de aprobarse.

© Acronis International GmbH, 2003-2025

Nota
Según su rol de usuario, puede realizar diferentes operaciones con secuencias de comandos y planes de programación. Para obtener más información sobre los roles, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

Prerrequisitos

- Su usuario es un administrador al que se le ha asignado el rol de **Administrador de cibernética**.
- Una secuencia de comandos con el estado correspondiente está disponible.

Pasos para cambiar el estado de la secuencia de comandos

1. En **Repositorio de secuencias de comandos**, vaya a **Mis secuencias de comandos**.
2. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre de la secuencia de comandos y, a continuación, haga clic en **Editar**.
3. En la lista desplegable de **Estado**, seleccione el estado.
4. Haga clic en **Guardar**.
5. [Si cambia el estado de una secuencia de comandos aprobada] Para confirmar el cambio, haga clic en **Guardar secuencia de comandos**.

   Nota
   Si el estado de la secuencia de comandos se revirtió a **Borrador**, los planes de programación que utilice no se ejecutarán.
   Solo los administradores con el rol de **Administrador de cibernética** pueden ejecutar secuencias de comandos en el estado de **Pruebas** y planes de programación con dichas secuencias de comandos.

Comparación de versiones de secuencias de comandos

Puede comparar dos versiones de una secuencia de comandos y revertirlas a una versión anterior. También puede comprobar quién creó una versión específica y cuándo.

Pasos para comparar versiones de secuencias de comandos

1. En **Depósito de secuencia de comandos**, vaya a **Mis secuencias de comandos** y busque la secuencia de comandos cuyas versiones desee comparar.
2. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre de la secuencia de comandos y, a continuación, haga clic en **Historial de versiones**.
3. Seleccione las dos versiones que desea comparar y, a continuación, haga clic en **Comparar versiones**.
   Se destacan los cambios que haya en el texto del cuerpo de la secuencia de comandos, los argumentos o las credenciales.

Pasos para revertir a una versión anterior

© Acronis International GmbH, 2003-2025

1. En la ventana **Comparar versiones de secuencias de comandos**, haga clic en **Revertir a esta versión**.
2. En el mensaje emergente **Revertir a una versión anterior**, en la lista desplegable de **Estado**, seleccione el estado de la secuencia de comandos.

Se restaurará la versión seleccionada y se guardará como la más reciente del historial de versiones.

Para restaurar una secuencia de comandos, también puede seleccionar una versión desde la ventana **Historial de versiones** y hacer clic en el botón **Restaurar**.

Importante
Puede ejecutar secuencias de comandos solo con los estados **En Prueba** o **Aprobada**. Para obtener más información, consulte "Cambio del estado de la secuencia de comandos" (p. 486).

Descargar el resultado de una operación de programación

Puede descargar el resultado de una operación de programación como archivo zip. Contiene dos archivos de texto: `stdout` y `stderr`. En `stdout`, puede ver los resultados de una operación de programación completada correctamente. El archivo `stderr` contiene información sobre los errores ocurridos durante la operación de programación.

Pasos para descargar el archivo de salida

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Actividades**.
2. Haga clic en la actividad de Programación cibernética cuyo resultado desee descargar.
3. En la pantalla **Detalles de actividad**, haga clic en **Descargar resultado**.

Depósito de secuencia de comandos

Puede localizar el depósito de secuencias de comandos en la pestaña **Gestión**. En el depósito, puede buscar las secuencias de comandos por nombre y descripción. También puede usar filtros o clasificar las secuencias de comandos por nombre o estado.

Para gestionar una secuencia de comandos, haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre y seleccione la acción deseada. De manera alternativa, haga clic en la secuencia de comandos y utilice los botones de la pantalla que se abre.

El depósito de secuencias de comandos contiene las siguientes secciones:

- **Mis secuencias de comandos**
  Aquí puede buscar las secuencias para utilizar directamente en su entorno. Son las secuencias de comandos que creó desde cero y las que ha clonado.
  Puede filtrar las secuencias de comandos en esta sección según estos criterios:
  - Etiquetas
  - Estado
  - Idioma

© Acronis International GmbH, 2003-2025

  - Sistema operativo
  - Propietario de secuencia de comandos
- **Biblioteca**

  La biblioteca contiene secuencias de comandos predefinidas que puede utilizar en su entorno después de clonarlas en la sección **Mis secuencias de comandos**. Solo puede inspeccionar y clonar estas secuencias de comandos.

  Puede filtrar las secuencias de comandos en esta sección según estos criterios:
  - Etiquetas
  - Idioma
  - Sistema operativo

  Para obtener más información, consulte Secuencias de comandos aprobadas por el Proveedor (70595).

Planes de programación

Un plan de programación le permite ejecutar una secuencia de comandos en varias cargas de trabajo, planificar la ejecución de una secuencia de comandos y configurar los ajustes adicionales.

Puede buscar los planes de programación que creó y los que aplicó a las cargas de trabajo en **Gestión** > **Planes de programación**. Aquí, puede comprobar la ubicación, el propietario o el estado de la ejecución del plan.

Una barra en la que se puede hacer clic muestra los siguientes estados con códigos por colores para los planes de programación:

- En ejecución (azul)
- Comprobando compatibilidad (gris oscuro)
- Deshabilitado (gris claro)
- Correcto (verde)
- Alerta crítica (rojo)
- Error (naranja)
- Advertencia (amarillo)

Al hacer clic en la barra, puede ver el estado de un plan y cuántas cargas de trabajo tiene. También se puede hacer clic en cada estado.

En la pestaña **Planes de programación**, puede gestionar los planes mediante estas acciones:

- Ejecutar
- Detener
- Editar
- Cambiar nombre

© Acronis International GmbH, 2003-2025

- Deshabilitar
- Habilitar
- Clonar
- Exportación. La configuración del plan se exportará en formato JSON al equipo local.
- Eliminar

La visibilidad de un plan de programación y las acciones disponibles en este dependen del propietario del plan y su rol de usuario. Por ejemplo, los administradores de empresa solo pueden ver planes de programación propiedad de partners que se aplican a sus cargas de trabajo y no pueden ejecutar ninguna acción con estos planes.

Para obtener más información sobre quién puede crear y gestionar los planes de programación, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

Pasos para gestionar un plan de programación

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de programación**.
2. Busque el plan que desee gestionar y, a continuación, haga clic en el icono de puntos suspensivos (...) junto a este.
3. Seleccione la acción que quiera y siga las instrucciones que aparecen en pantalla.

Creación de un plan de programación

Puede crear un plan de programación de las siguientes formas:

- En la pestaña **Dispositivos**
  Seleccione las cargas de trabajo y cree un plan de programación para ellas.
- En la pestaña **Gestión** > **Planes de programación**
  Cree un plan de programación y seleccione las cargas de trabajo a las que se va a aplicar el plan.

Pasos para crear un plan de programación en la pestaña Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Seleccione las cargas de trabajo o los grupos de dispositivos a los que desea aplicar un plan de programación y, a continuación, haga clic en **Proteger** o **Proteger grupo**, respectivamente.
3. [Si ya hay planes aplicados] Haga clic en **Agregar plan**.
4. Haga clic en **Crear plan** > **Plan de programación**.
   Se abrirá una plantilla para el plan de programación.
5. [Opcional] Para modificar el nombre del plan de programación, haga clic en el icono del lápiz.
6. Haga clic en **Seleccionar secuencia de comandos**, seleccione la secuencia de comandos que desea utilizar y haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Nota
Solo puede usar sus secuencias de comandos aprobadas del **Repositorio de secuencias de comandos** > **Mis secuencias de comandos**. Solo un administrador con el rol de **Administrador de cibernética** puede usar secuencias de comandos en el estado de **Pruebas**. Para obtener más información sobre los roles, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

7. Configure la planificación y las condiciones de inicio para el plan de programación.
8. Escoja en qué cuenta se ejecutará la secuencia de comandos en la carga de trabajo de destino. Las siguientes opciones están disponibles:
   - Cuenta de sistema (en macOS, esta es la cuenta raíz)
   - Cuenta con sesión iniciada actualmente
9. Especifique durante cuánto tiempo se puede ejecutar la secuencia de comandos en la carga de trabajo de destino.
   Si la secuencia de comandos no ha terminado de ejecutarse en ese periodo de tiempo, se producirá un error en la operación de programación cibernética.
   El valor mínimo que puede especificar es un minuto y el máximo, 1440 minutos.
10. [Solo para secuencias de comandos de PowerShell] Configure la directiva de ejecución de PowerShell.
    Para obtener más información sobre esta política, consulte la documentación de Microsoft.
11. Haga clic en **Crear**.

Pasos para crear un plan de programación en la pestaña Planes de programación

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de programación**.
2. Haga clic en **Crear plan**.
   Se abrirá una plantilla para el plan de programación.
3. [Opcional] Para seleccionar las cargas de trabajo o los grupos de dispositivos a los que desea aplicar el nuevo plan, haga clic en **Añadir cargas de trabajo**.
   a. Haga clic en **Equipos con agentes** para ampliar la lista y seleccione las cargas de trabajo o los grupos de dispositivos que desee.
   b. Haga clic en **Agregar**.

   Para obtener más información sobre cómo crear grupos de dispositivos en el nivel de partner, consulte "Crear grupos de dispositivos estáticos en el nivel de partner" (p. 377) y "Crear un grupo dinámico de dispositivos en el nivel de partner" (p. 377).

   Nota
   También puede seleccionar cargas de trabajo o grupos de dispositivos después de crear el plan.
4. [Opcional] Para modificar el nombre del plan de programación, haga clic en el icono del lápiz.

© Acronis International GmbH, 2003-2025

5. Haga clic en **Seleccionar secuencia de comandos**, seleccione la secuencia de comandos que desea utilizar y haga clic en **Listo**.

   Nota
   Solo puede usar sus secuencias de comandos aprobadas del **Repositorio de secuencias de comandos** > **Mis secuencias de comandos**. Solo un administrador con el rol de **Administrador de cibernética** puede usar secuencias de comandos en el estado de **Pruebas**. Para obtener más información sobre los roles, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

6. Configure la planificación y las condiciones de inicio para el plan de programación.
7. Escoja en qué cuenta se ejecutará la secuencia de comandos en la carga de trabajo de destino. Las siguientes opciones están disponibles:
   - Cuenta de sistema (en macOS, esta es la cuenta raíz)
   - Cuenta con sesión iniciada actualmente
8. Especifique durante cuánto tiempo se puede ejecutar la secuencia de comandos en la carga de trabajo de destino.
   Si la secuencia de comandos no ha terminado de ejecutarse en ese periodo de tiempo, se producirá un error en la operación de programación cibernética.
   El valor mínimo que puede especificar es un minuto y el máximo, 1440 minutos.
9. [Solo para secuencias de comandos de PowerShell] Configure la directiva de ejecución de PowerShell.
   Para obtener más información sobre esta política, consulte la documentación de Microsoft.
10. Haga clic en **Crear**.

Planificación y condiciones de inicio

Planificación

Puede configurar un plan de programación para ejecutarlo una vez o de forma repetida y para que se inicie de forma programada o se active con determinado evento.

Las siguientes opciones están disponibles:

- Ejecutar una vez
  Para esta opción, debe configurar la fecha y la hora en las que se ejecutará el plan.
- Planificar por hora
  Con esta opción, puede configurar los planes de programación que se ejecutarán por hora, día o mes.
  Para que la planificación sea efectiva solo de manera temporal, seleccione la casilla de verificación **Ejecutar dentro de un intervalo de fechas** y configure el periodo durante el que se ejecutará el plan programado.
- Cuando el usuario inicia sesión en el sistema

© Acronis International GmbH, 2003-2025

Puede elegir si el plan de programación se activa si un usuario específico o cualquier usuario inicia sesión.

- Cuando el usuario cierra sesión en el sistema

  Puede elegir si un usuario específico o cualquier usuario que cierre sesión activa el plan de programación.
- Al iniciarse el sistema
- Cuando el sistema está apagado

Nota
Esta opción de planificación solo funciona con las secuencias de comandos que se ejecutan en la cuenta de sistema.

- Cuando el sistema está en línea

Condiciones de inicio

Las condiciones de inicio añaden más flexibilidad a sus planes programados. Si configura varias condiciones, deben cumplirse todas simultáneamente para que se ejecute el plan.

Las condiciones de inicio no son efectivas si ejecuta el plan de forma manual con la opción **Ejecutar ahora**.

Condición	Descripción
Ejecutar solo si la carga de trabajo está en línea	Esta condición se cumple cuando la carga de trabajo de destino se conecta a Internet.
El usuario está inactivo	Esta condición se cumple cuando se está ejecutando el protector de pantalla en el equipo o el equipo está bloqueado.
El usuario cerró la sesión	Si selecciona esta condición, puede posponer un plan programado hasta que el usuario de la carga de trabajo de destino cierre sesión.
Coincidir con intervalo	Si selecciona esta condición, debe definir el intervalo de tiempo en el que puede ejecutarse el plan.
Ahorrar batería	Si selecciona esta condición, podrá asegurarse de que el plan no se interrumpirá porque la batería sea baja. Las siguientes opciones están disponibles: • **No iniciar con alimentación por batería** El plan se iniciará únicamente si el equipo está conectado a una fuente de alimentación. • **Iniciar con alimentación por batería si su nivel es superior a** El plan se iniciará si el equipo está conectado a una fuente de alimentación o si el nivel de la batería es superior al valor especificado.
No iniciar con	Si selecciona esta condición, el plan no se ejecutará si la carga de trabajo de

© Acronis International GmbH, 2003-2025

Condición	Descripción
conexiones de uso medido	destino accede a Internet a través de una conexión de uso medido.
No iniciar con conexiones a las siguientes redes Wi-Fi	Si selecciona esta condición, el plan no se ejecutará si la carga de trabajo de destino está conectada a cualquiera de las redes inalámbricas especificadas. Para utilizar esta condición, debe especificar el SSID de la red prohibida. La restricción se aplica a todas las redes de contengan el nombre especificado como una subcadena en su nombre, sin distinción de mayúsculas y minúsculas. Por ejemplo, si especifica `teléfono` como nombre de red, el plan no se iniciará cuando el dispositivo esté conectado a alguna de las siguientes redes: `Teléfono de Juan`, `wifi_teléfono` o `wifi_de_mi_teléfono`.
Comprobar dirección IP del dispositivo	Si selecciona esta condición, el plan no se ejecutará si alguna de las direcciones IP de la carga de trabajo de destino está dentro o fuera del rango de direcciones IP especificado. Las siguientes opciones están disponibles: • **Iniciar si queda fuera del intervalo IP** • **Iniciar si queda dentro del intervalo IP** Solo se admiten direcciones IPv4.
Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos	Utilice esta opción para establecer el intervalo de tiempo tras el cual se ejecutará el plan, independientemente del resto de condiciones. El plan comenzará cuando se cumplan el resto de las condiciones o cuando termine este periodo, lo que suceda primero. Esta opción no está disponible si ha seleccionado la opción **Ejecutar una vez** para la programación.

Administración de cargas de trabajo de destino para un plan

Puede seleccionar las cargas de trabajo o los grupos de dispositivos a los que desea aplicar un plan de programación cuando cree el plan o más adelante.

Los administradores de partner pueden aplicar el mismo plan a las cargas de trabajo de diferentes clientes y crear grupos de dispositivos con cargas de trabajo de diferentes clientes. Para saber cómo crear un grupo de dispositivos en el nivel de partner, consulte "Crear grupos de dispositivos estáticos en el nivel de partner" (p. 377) y "Crear un grupo dinámico de dispositivos en el nivel de partner" (p. 377).

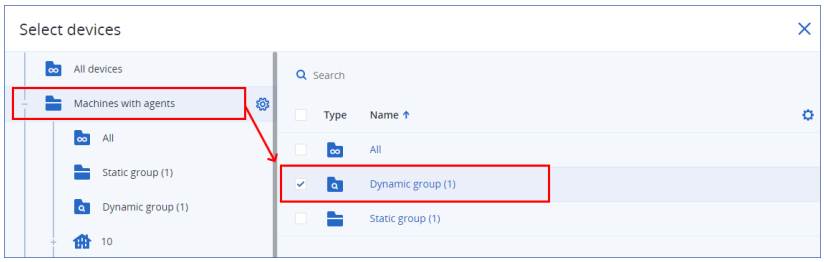
Pasos para añadir cargas de trabajo iniciales a un plan

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de programación**.
2. Haga clic en el nombre del plan para el que desea especificar cargas de trabajo de destino.
3. Haga clic en **Añadir cargas de trabajo**.

© Acronis International GmbH, 2003-2025

4. Seleccione las cargas de trabajo o los grupos de dispositivos que desee y haga clic en **Agregar**.

   Nota
   Para seleccionar un grupo de dispositivos, haga clic en el nivel principal y, a continuación, en el panel principal, marque la casilla de verificación que hay junto a su nombre.

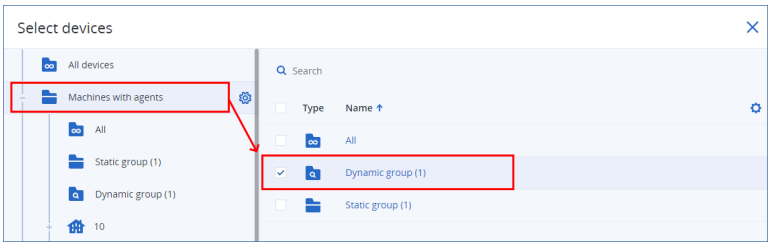
   

5. Haga clic en **Guardar** para guardar el plan editado.

Pasos para gestionar cargas de trabajo existentes para un plan

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de programación**.
2. Haga clic en el nombre del plan cuyas cargas de trabajo de destino desea cambiar.
3. Haga clic en **Gestionar cargas de trabajo**.
   La pantalla **Dispositivos** enumera las cargas de trabajo a las que se aplica el plan de programación actualmente. Si gestiona más de un inquilino, las cargas de trabajo se ordenan por inquilino.
   - Para añadir cargas de trabajo o grupos de dispositivos nuevos, haga clic en **Agregar**.
     a. Seleccione las cargas de trabajo o los grupos de dispositivos que desee. Puede añadir cargas de trabajo desde todos los inquilinos que gestione.

        Nota
        Para seleccionar un grupo de dispositivos, haga clic en el nivel principal y, a continuación, en el panel principal, marque la casilla de verificación que hay junto a su nombre.

     b. Haga clic en **Agregar**.
   - Para eliminar las cargas de trabajo o los grupos de dispositivos, selecciónelos y haga clic en **Eliminar**.
4. Haga clic en **Listo**.
5. Haga clic en **Guardar** para guardar el plan editado.

© Acronis International GmbH, 2003-2025

Importación de planes de programación

Puede importar planes de programación que se exportaron en un archivo JSON. Así, puede ahorrar tiempo y garantizar la coherencia de la configuración entre inquilinos.

Requisitos previos

Un archivo JSON con la configuración del plan está disponible en el equipo desde el que ha iniciado sesión en la consola.

Para importar un plan de programación

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de programación**.
2. Haga clic en **Importar**.
3. En la ventana que se abre, busque el archivo JSON.
4. Haga clic en el archivo y luego en **Abrir**.
   El plan de programación aparece en la pantalla. Ahora puede aplicarlo a las cargas de trabajo.

Ejecución rápida de la secuencia de comandos

Puede ejecutar una secuencia de comandos inmediatamente, sin incluirla en un plan de programación. No puede usar esta operación en más de 150 cargas de trabajo, en cargas de trabajo sin conexión o en grupos de dispositivos.

Debe asignar una cuota de servicio a la carga de trabajo objetivo que admita la funcionalidad de ejecución rápida del script. Además, debe habilitar la licencia RMM (modelo de licencia basado en servicios) o Seguridad y RMM (modo de licencia basado en soluciones) para su inquilino. Se asignará automáticamente una cuota de servicio adecuada si está disponible en el inquilino.

Nota
Solo puede usar sus secuencias de comandos aprobadas del **Repositorio de secuencias de comandos** > **Mis secuencias de comandos**. Solo un administrador con el rol de **Administrador de cibernética** puede usar secuencias de comandos en el estado de **Pruebas**. Para obtener más información sobre los roles, consulte "Roles de usuario y derechos de la Programación cibernética" (p. 476).

Puede iniciar una ejecución rápida de las siguientes formas:

- En la pestaña **Dispositivos**
  Seleccione una o más cargas de trabajo y, a continuación, seleccione qué secuencia de comandos se va a ejecutar en ellas.
- En la pestaña **Gestión** > **Depósito de secuencias de comandos**
  Seleccione una secuencia de comandos y, a continuación, una o más cargas de trabajo de destino.

Pasos para ejecutar una secuencia de comandos desde la pestaña Dispositivos

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione la carga de trabajo en la que desea ejecutar la secuencia de comandos y haga clic en **Proteger**.
3. Haga clic en **Ejecución rápida de la secuencia de comandos**.
4. Haga clic en **Seleccionar secuencia de comandos**, seleccione la secuencia de comandos que desea utilizar y haga clic en **Listo**.
5. Escoja en qué cuenta se ejecutará la secuencia de comandos en la carga de trabajo de destino. Las siguientes opciones están disponibles:
   - Cuenta de sistema (en macOS, esta es la cuenta raíz)
   - Cuenta con sesión iniciada actualmente
6. Especifique durante cuánto tiempo se puede ejecutar la secuencia de comandos en la carga de trabajo de destino.
   Si la secuencia de comandos no ha terminado de ejecutarse en ese periodo de tiempo, se producirá un error en la operación de secuencia de comandos cibernética.
   Puede usar valores entre 1 y 1440 minutos.
7. [Solo para secuencias de comandos de PowerShell] Configure la directiva de ejecución de PowerShell.
   Para obtener más información sobre esta política, consulte la documentación de Microsoft.
8. Haga clic en **Ejecutar ahora**.

Pasos para ejecutar una secuencia de comandos desde la pestaña Depósito de secuencias de comandos

1. En la consola de Cyber Protect, vaya a **Gestión** > **Depósito de secuencias de comandos**.
2. Seleccione la secuencia de comandos que desea ejecutar y haga clic en **Ejecución rápida de la secuencia de comandos**.
3. Haga clic en **Añadir cargas de trabajo** para seleccionar las cargas de trabajo de destino y, a continuación, haga clic en **Agregar**.
4. Haga clic en **Seleccionar secuencia de comandos**, seleccione la secuencia de comandos que desea utilizar y haga clic en **Listo**.
5. Escoja en qué cuenta se ejecutará la secuencia de comandos en la carga de trabajo de destino. Las siguientes opciones están disponibles:
   - Cuenta de sistema (en macOS, esta es la cuenta raíz)
   - Cuenta con sesión iniciada actualmente
6. Especifique durante cuánto tiempo se puede ejecutar la secuencia de comandos en la carga de trabajo de destino.
   Si la secuencia de comandos no ha terminado de ejecutarse en ese periodo de tiempo, se producirá un error en la operación de secuencia de comandos cibernética.
   Puede usar valores entre 1 y 1440 minutos.

© Acronis International GmbH, 2003-2025

7. [Solo para secuencias de comandos de PowerShell] Configure la directiva de ejecución de PowerShell.

   Para obtener más información sobre esta política, consulte la documentación de Microsoft.
8. Haga clic en **Ejecutar ahora**.

© Acronis International GmbH, 2003-2025

Gestión de la copia de seguridad y recuperación de cargas de trabajo y archivos

El módulo de copia de seguridad permite realizar copias de seguridad y recuperar equipos físicos y virtuales, archivos y bases de datos en un almacenamiento local o en la nube.

Sistemas operativos y entornos compatibles para la copia de seguridad y la recuperación

La información que se presenta a continuación se aplica a la copia de seguridad y recuperación. Para obtener detalles acerca de las funciones de protección compatibles con el sistema operativo, consulte "Funciones de protección compatibles con el sistema operativo" (p. 28).

Agente para Windows

El modo compatible con FIPS es compatible con los sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de URL que admite un conjunto diferente de sistemas operativos. Consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Nota
La lista de sistemas operativos compatibles que se muestra a continuación se aplica a la copia de seguridad y recuperación.

- Windows 10 versión 1809 y posteriores (ediciones Home, Pro, Education, Enterprise y IoT Enterprise y LTSC, antes LTSB)
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- Windows Server 2025: todas las opciones de instalación, excepto Nano Server

© Acronis International GmbH, 2003-2025

Importante
Antes de actualizar el sistema operativo de una carga de trabajo protegida donde esté instalado un agente de protección o el servidor de administración, tenga en cuenta lo siguiente:

- En el caso de una actualización de versión importante (por ejemplo, de Windows 7 a Windows 10), debe reinstalar el agente o el servidor de administración después de la actualización para garantizar su correcto funcionamiento.
- En el caso de una actualización menor dentro de una versión principal (por ejemplo, de Windows 10 versión 20H2 a Windows 10 versión 21H1), no es necesario reinstalar el agente después de actualizar el sistema operativo.

Agente para Windows (heredado)

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de URL que admite un conjunto diferente de sistemas operativos. Consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Nota
La lista de sistemas operativos compatibles que se muestra a continuación se aplica a la copia de seguridad y recuperación.

- Windows XP Professional SP1 (x64), SP2 (x64) y SP3 (x86)

  Nota
  En los sistemas Windows XP, el Agente para Windows solo admite unidades con formato NTFS.

- Windows Server 2003 SP1/2003 R2 y posteriores (ediciones Standard y Enterprise [x86, x64])
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2*: ediciones Standard, Enterprise, Datacenter, Foundation y Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7: todas las ediciones

  Nota
  Para usar Cyber Protection con Windows 7, debe instalar las siguientes actualizaciones de Microsoft antes de instalar el agente de protección:
  - Actualizaciones de seguridad ampliadas de Windows 7 (ESU)
  - KB4474419
  - KB4490628

  Consulte este artículo de la base de conocimientos para obtener más información sobre las actualizaciones requeridas.

- Windows Server 2008 R2*: ediciones Standard, Enterprise, Datacenter, Foundation y Web

© Acronis International GmbH, 2003-2025

- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011*: todas las ediciones
- Windows 8/8.1: todas las ediciones (x86, x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 versión 1803 y anteriores (ediciones Home, Pro, Education, Enterprise y IoT Enterprise y LTSC, antes LTSB)
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server

Nota
* Para usar Cyber Protection con esta versión de Windows, debe instalar la actualización del soporte técnico de firma de código SHA2 de Microsoft (KB4474419) antes de instalar el agente de protección.

Consulte este artículo de la base de conocimiento para obtener más información sobre cuestiones relacionadas con la actualización del soporte de firma de código SHA2.

Importante
Antes de actualizar el sistema operativo de una carga de trabajo protegida donde esté instalado un agente de protección o el servidor de administración, tenga en cuenta lo siguiente:
- En el caso de una actualización de versión importante (por ejemplo, de Windows 7 a Windows 10), debe reinstalar el agente o el servidor de administración después de la actualización para garantizar su correcto funcionamiento.
- En el caso de una actualización menor dentro de una versión principal (por ejemplo, de Windows 10 versión 20H2 a Windows 10 versión 21H1), no es necesario reinstalar el agente después de actualizar el sistema operativo.

Agente para SQL, Agente para Active Directory y Agente para Exchange (para copia de seguridad de bases de datos y copias de seguridad compatibles con la aplicación)

Estos agentes se entregan como parte de Agente para Windows y Agente para Windows (heredado). Con Agente para Windows, el modo compatible con FIPS es compatible con sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

Cada uno de estos agentes es compatible con las mismas versiones de Windows que el Agente para Windows y el Agente para Windows (heredado) y pueden instalarse en un equipo que ejecute una versión compatible de la aplicación respectiva, con la siguiente excepción:

- Windows Server 2025 no es compatible.

© Acronis International GmbH, 2003-2025

Agente para la prevención de la pérdida de datos

Este agente se entregan como parte de Agente para Windows y Agente para Windows (heredado). Con Agente para Windows, el modo compatible con FIPS es compatible con sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

Control de dispositivos

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 – Windows Server 2022
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)

Nota
El Agente para la prevención de pérdida de datos para macOS solo es compatible con procesadores x64. Los procesadores basados en ARM de Apple Silicon no son compatibles.

Prevención de pérdida de datos

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 – Windows Server 2022

Nota
El Agente para la prevención de pérdida de datos podría estar instalado en sistemas macOS no compatibles porque es una parte integral del Agente para Mac. En ese caso, la consola de Cyber Protect mostrará que el Agente para la prevención de pérdida de datos está instalado en el ordenador, pero la función de control del dispositivos y de prevención de pérdida de datos no funcionará. La función de control de dispositivos solo funcionará en sistemas macOS compatibles con el Agente para la prevención de pérdida de datos.

Agente para File Sync & Share

Este agente se entrega como parte de Agente para Windows y Agente para Windows (heredado).

El Agente para File Sync & Share soporta un conjunto diferente de sistemas operativos que el Agente para Windows y el Agente para Windows (heredado).

Para verificar los sistemas operativos que el Agente para File Sync & Share soporta, consulte la documentación de Cyber Files Cloud.

© Acronis International GmbH, 2003-2025

Agente para Exchange (para la copia de seguridad de buzones de correo)

Este agente se entregan como parte de Agente para Windows y Agente para Windows (heredado). Con Agente para Windows, el modo compatible con FIPS es compatible con sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

- Windows Server 2008: ediciones Standard, Enterprise, Datacenter, Foundation y Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7: todas las ediciones
- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter, Foundation y Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (x86, x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10: ediciones Home, Pro, Education y Enterprise
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

Agente para Microsoft 365

Este agente se entregan como parte de Agente para Windows y Agente para Windows (heredado). Con Agente para Windows, el modo compatible con FIPS es compatible con sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

- Windows Server 2008: ediciones Standard, Enterprise, Datacenter, Foundation y Web (solo x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter, Foundation y Web
- Windows Home Server 2011
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (solo x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (solo x64)
- Windows 10: ediciones Home, Pro, Education y Enterprise (solo x64)

© Acronis International GmbH, 2003-2025

- Windows Server 2016: todas las opciones de instalación (solo x64), excepto Nano Server
- Windows Server 2019: todas las opciones de instalación (solo x64), excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

Agente para Oracle

Este agente se entrega como parte de Agente para Windows, Agente para Windows (heredado) y Agente para Linux (64 bits). Con Agente para Windows y Agente para Linux, el modo compatible con FIPS es compatible en sistemas operativos de 64 bits.

- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter y Web (x86, x64)
- Windows Server 2012 R2: ediciones Standard, Enterprise, Datacenter y Web (x86, x64)
- Linux: cualquier kernel y distribución compatibles con el Agente para Linux (se indican a continuación)

Agente para MySQL/MariaDB

Este agente se entrega como parte de Agente para Linux (64 bits).

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

- Linux: cualquier kernel y distribución compatibles con el Agente para Linux (se indican a continuación)

Agente para Linux

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de URL que admite un conjunto diferente de sistemas operativos. Consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Nota
La lista de sistemas operativos compatibles que se muestra a continuación se aplica a la copia de seguridad y recuperación.

Cyber Protect Cloud admite las distribuciones de Linux x86 y x86_64 que utilizan los siguientes componentes:

- Versión de kernel de 2.6.9 a 6.14
  Las versiones de kernel compatibles se enumeran según las versiones en www.kernel.org. Algunas distribuciones, como Red Hat Enterprise Linux, realizan el backport de las nuevas funciones a las versiones anteriores del kernel. Es posible que los kernel específicos de la distribución no sean compatibles, aunque su versión esté dentro del rango compatible.
- La biblioteca C de GNU (glibc) 2.3.4 o posterior

© Acronis International GmbH, 2003-2025

Se han probado específicamente las siguientes distribuciones. Sin embargo, incluso si su distribución de Linux o versión del kernel no se encuentra en la siguiente lista, podría funcionar correctamente en todos los escenarios requeridos, debido a las especificaciones de los sistemas operativos de Linux. Si encuentra problemas al utilizar Cyber Protect Cloud con su combinación de distribución y versión del kernel, póngase en contacto con el equipo de soporte para una investigación más detallada.

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*,8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*, 10*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04, 23.10, 24.04, 24.10, 25.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38, 39, 40, 41, 42

  Importante
  No se admiten configuraciones con Btrfs. Para obtener más información, consulte "Sistemas de archivos compatibles" (p. 525).

- SUSE Linux Enterprise Server 10, 11, 12, 15

  Importante
  No se admiten configuraciones con Btrfs. Para obtener más información, consulte "Sistemas de archivos compatibles" (p. 525).

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11, 12, 13
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*, 10*
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6* (tanto Unbreakable Enterprise Kernel como Red Hat Compatible Kernel)

  Nota
  Para instalar el agente de protección en Oracle Linux 8.6 y versiones posteriores, en las que se haya habilitado el arranque seguro, se deben firmar manualmente los módulos de kernel. Para obtener más información sobre cómo firmar un módulo de kernel, consulte este artículo de la base de conocimiento.

- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*,8.7*, 8.8*, 8.9*, 8.10*, 9.4*, 9.5*, 9.6*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*,8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*

© Acronis International GmbH, 2003-2025

- Rocky Linux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*,8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- ALT Linux 7.0

* A partir de la versión 8.4, solo se ofrece soporte con kernels de 4.18 y posteriores.

Importante
Antes de actualizar el sistema operativo de un recurso informático protegido donde esté instalado el agente Cyber Protection o un servidor de administración, tenga en cuenta lo siguiente.

- En el caso de una actualización de versión importante, debe reinstalar el agente o el servidor de administración después de la actualización para garantizar su correcto funcionamiento.
- Antes de instalar una nueva versión de kernel, consulte la sección "Agente para Linux" (p. 504) para verificar que la versión es compatible.

Agente para Mac

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de URL que admite un conjunto diferente de sistemas operativos. Consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Nota
La lista de sistemas operativos compatibles que se muestra a continuación se aplica a la copia de seguridad y recuperación.

Las arquitecturas x64 y ARM (utilizada en procesadores con Apple Silicon, como Apple M1, M2 y modelos posteriores) son compatibles.

Nota
No puede recuperar copias de seguridad a nivel de disco de equipos Mac basados en Intel en equipos Mac que usen procesadores Apple Silicon, ni viceversa. Puede recuperar archivos y carpetas.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14
- macOS Sequoia 15
- macOS Tahoe 26

© Acronis International GmbH, 2003-2025

Nota
El agente también es compatible con todas las versiones menores de los sistemas operativos enumerados anteriormente. Por ejemplo, macOS Sonoma 14.5.

Importante
A partir de la versión C23.07, Cyber Protect Cloud no es compatible con los siguientes sistemas operativos: OS X Yosemite 10.10, OS X El Capitan 10.11 y macOS Sierra 10.12.

A partir de la versión C25.07, Cyber Protect Monitor no es compatible con las versiones de macOS 10.x.

Le recomendamos encarecidamente que actualice su sistema operativo a una versión compatible para garantizar la compatibilidad y poder utilizar toda la funcionalidad de Cyber Protect Cloud.

Agente para VMware (dispositivo virtual)

Este agente se proporciona como un dispositivo virtual que se ejecuta en un host ESXi.

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

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

En el modo compatible con FIPS, solo VMware ESXi 8.0 es compatible.

Agente para VMware (Windows)

Este agente se entregan como parte de Agente para Windows y Agente para Windows (heredado). Con Agente para Windows, el modo compatible con FIPS es compatible con sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

Este agente es compatible con las mismas versiones de Windows que el Agente para Windows y el Agente para Windows (heredado) con las siguientes limitaciones:

- Los sistemas operativos de 32 bits no son compatibles.
- Windows XP, Windows Server 2003/2003 R2 y Windows Small Business Server 2003/2003 R2 no son compatibles.
- En el modo compatible con FIPS, solo VMware ESXi 8.0 es compatible.

Agente para Hyper-V

Este agente se entregan como parte de Agente para Windows y Agente para Windows (heredado). Con Agente para Windows, el modo compatible con FIPS es compatible con sistemas operativos de 64 bits. Consulte "Modo compatible con FIPS" (p. 60).

- Windows Server 2008 (solo x64) con el rol Hyper-V, incluido el modo de instalación de Server Core
- Windows Server 2008 R2 con el rol Hyper-V, incluido el modo de instalación de Server Core
- Microsoft Hyper-V Server 2008/2008 R2

© Acronis International GmbH, 2003-2025

- Windows Server 2012/2012 R2 con el rol Hyper-V, incluido el modo de instalación de Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (solo x64) con Hyper-V
- Windows 10: ediciones Pro, Education y Enterprise con Hyper-V
- Windows 11: ediciones Pro, Education y Enterprise con Hyper-V
- Windows Server 2016 con el rol Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 con el rol Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- Windows Server 2025: todas las opciones de instalación, excepto Nano Server

Agente para Virtuozzo

Este agente se entrega como parte de Agente para Linux (64 bits).

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

Agente para la Virtuozzo Hybrid Infrastructure

Este agente se entrega como un dispositivo virtual que se ejecuta en un host de Virtuozzo Hybrid Infrastructure.

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2, 6.3

Agent para Scale Computing HC3

Este agente se entrega como un dispositivo virtual que se ejecuta en un host de Scale Computing HC3.

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

Scale Computing HyperCore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4

Agente para oVirt

Este agente se entrega como un dispositivo virtual que se ejecuta en un host de hipervisor KVM gestionado por oVirt.

Admite el modo compatible con FIPS. Consulte "Modo compatible con FIPS" (p. 60).

© Acronis International GmbH, 2003-2025

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agente para Synology

Este agente se entrega como un dispositivo virtual que se ejecuta en un NAS de Synology.

DiskStation Manager 6.2.x, 7.x

El agente para Synology solo admite dispositivos NAS con procesadores x86_64. Los procesadores ARM no son compatibles. Consulte el centro de conocimientos de Synology.

Agente para Azure

Este agente se entrega como un dispositivo virtual que se ejecuta en su suscripción de Microsoft Azure.

Agente para Nutanix

Este agente se entrega como un dispositivo virtual que se ejecuta en un clúster Nutanix AHV.

Sistema operativo Nutanix Acropolis (AOS) 6.5, 6.6, 6.7, 6.8, 6.10

Cyber Protect Monitor

- Con Agente para Windows
  - Windows 10 versión 1809 y posteriores
  - Windows Server 2019 y versiones posteriores
- Con el agente para Windows (heredado)
  - Windows 7 y posterior
  - Windows Server 2008 R2 y posterior
- Con Agente para Mac
  - Todas las versiones de macOS compatibles con Agent for Mac, excepto macOS 10.x.

Versiones compatibles de Microsoft SQL Server

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2

© Acronis International GmbH, 2003-2025

- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Las ediciones de SQL Server Express de las versiones anteriores del servidor SQL también son compatibles.

Nota
La copia de seguridad de Microsoft SQL solo es compatible con las bases de datos que se ejecutan en sistemas de archivos NTFS, REFS y FAT32. ExFat no es compatible.

Versiones compatibles de Microsoft Exchange Server

- Microsoft Exchange Server Subscription Edition (SE)
- Microsoft Exchange Server 2019: todas las ediciones.
- Microsoft Exchange Server 2016: todas las ediciones.
- Microsoft Exchange Server 2013: todas las ediciones, actualización acumulativa 1 (CU1) y posteriores.
- Microsoft Exchange Server 2010: todas las ediciones, todos los Service Pack. Se admite la copia de seguridad de buzón de correo y la recuperación granular desde copias de seguridad de base de datos a partir del Service Pack 1 (SP1).
- Microsoft Exchange Server 2007: todas las ediciones, todos los Service Pack. No se admite la copia de seguridad de buzón de correo y la recuperación granular desde copias de seguridad de base de datos.

Versiones de Microsoft SharePoint compatibles

Cyber Protection es compatible con las siguientes versiones de Microsoft SharePoint:

- 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*

*Para utilizar SharePoint Explorer con estas versiones, es necesaria una granja de recuperación de SharePoint a la que conectar las bases de datos.

Las bases de datos o copias de seguridad desde las que se extraen los datos deben tener su origen en la misma versión de SharePoint que la versión en la que está instalado SharePoint Explorer.

© Acronis International GmbH, 2003-2025

Versiones de Oracle Database compatibles

- Oracle Database versión 11g, todas las ediciones
- Oracle Database versión 12c, todas las ediciones
- Oracle Database versión 19c, todas las ediciones
- Oracle Database versión 21c, todas las ediciones

Solo se admiten configuraciones de una instancia.

Versiones de SAP HANA compatibles

- HANA 2.0 SPS 03 instalado en RHEL 7.6 que se ejecuta en un equipo físico o en un equipo virtual VMware ESXi.
- HANA 2.0 SPS 03 instalado en SUSE 15 con sistema de archivos XFS.

Dado que SAP HANA no admite la recuperación de contenedores de bases de datos de múltiples inquilinos con el uso de instantáneas de almacenamiento, esta solución admite contenedores SAP HANA con base de datos de un solo inquilino.

Versiones de MySQL admitidas

- 5.5.x: ediciones Community Server, Enterprise, Standard y Classic
- 5.6.x: ediciones Community Server, Enterprise, Standard y Classic
- 5.7.x: ediciones Community Server, Enterprise, Standard y Classic
- 8.0.x: ediciones Community Server, Enterprise, Standard y Classic

Versiones de MariaDB admitidas

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

Plataformas de virtualización compatibles

En las tablas siguientes, se resume cómo se admiten las diferentes plataformas de virtualización.

© Acronis International GmbH, 2003-2025

Para obtener más información sobre las diferencias entre la copia de seguridad basada en agentes y la copia de seguridad sin agentes, consulte "Copia de seguridad basada en agente y sin agente" (p. 41).

Nota
Si utiliza una plataforma de virtualización o una versión que no se encuentra en la siguiente lista, el método de **copia de seguridad basada en agentes (copia de seguridad desde dentro de un sistema operativo invitado)** debería funcionar correctamente en todos los escenarios requeridos. Si encuentra problemas con la copia de seguridad basada en agentes, contacte con el equipo de soporte para una investigación más detallada.

VMware (Broadcom)

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Versiones de VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0 y 8.0 **Ediciones de VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Broadcom (VMware) ESXi** > **Agente para instalación en Windows** o **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Broadcom (VMware) ESXi** > **Dispositivo virtual (OVF)**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
VMware vSphere Hypervisor (Free ESXi)**	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

© Acronis International GmbH, 2003-2025

* En estas ediciones, el transporte HotAdd para unidades de disco virtual es compatible en vSphere 5.0 y versiones posteriores. Es posible que las copias de seguridad se ejecuten más lentamente en la versión 4.1.

** La copia de seguridad a nivel de hipervisor no es compatible para vSphere Hypervisor porque este producto restringe el acceso a la interfaz de la línea de comandos remota (RCLI) al modo de solo lectura. El agente funciona durante el periodo de evaluación de vSphere Hypervisor mientras no se introduzca ninguna clave. Una vez ingresada dicha clave, el agente deja de funcionar.

Nota
Cyber Protect Cloud admite oficialmente cualquier actualización dentro de la versión principal de vSphere compatible.

Por ejemplo, el soporte para vSphere 8.0 incluye soporte para cualquier actualización dentro de esta versión, a menos que se indique lo contrario. Es decir, vSphere 8.0 Update 1 también es compatible junto con la versión originalmente lanzada de vSphere 8.0.

La compatibilidad con una versión específica de VMware vSphere implica que vSAN de la versión correspondiente también es compatible. Por ejemplo, la compatibilidad con vSphere 8.0 implica que vSAN 8.0 también es compatible.

Limitaciones

- **Equipos tolerantes a errores**
  Agente para VMware realiza una copia de seguridad de un equipo tolerante a errores, solo si la tolerancia a errores está habilitada en vSphere 6.0 o versiones posteriores. Si ha actualizado desde una versión antigua de vSphere, solo es necesario que deshabilite y habilite la tolerancia a errores para cada equipo. Si está utilizando una versión de vSphere anterior, instale un agente en el sistema operativo invitado.
- **Discos independientes y RDM**
  Agente para VMware no puede realizar copias de seguridad de discos Raw Device Mapping (RDM) en modo de compatibilidad física ni de discos independientes. El agente omite estos discos y añade las advertencias al registro. Puede evitar las advertencias al excluir los discos independientes y RDM en el modo de compatibilidad física del plan de protección. Si desea realizar la copia de seguridad de estos discos o de los datos que estos contienen, instale un agente en el sistema operativo invitado.
- **Conexión iSCSI en invitado**
  Agente para VMware no realiza copias de seguridad de volúmenes de LUN conectados mediante un iniciador iSCSI que funciona en el sistema operativo invitado. Como el hipervisor ESXi no es compatible con tales volúmenes, estos no se incluyen en las instantáneas a nivel de hipervisor y se omiten de una copia de seguridad sin emitir ningún aviso. Si desea realizar la copia de seguridad de estos volúmenes o de los datos que estos contienen, instale un agente en el sistema operativo invitado.

© Acronis International GmbH, 2003-2025

- **Equipos virtuales cifrados** (presentados en VMware vSphere 6.5)
  - Los equipos virtuales cifrados se incluyen en la copia de seguridad en un estado cifrado. Si el cifrado es crucial en su caso, habilite las copias de seguridad al crear un plan de protección.
  - Los equipos virtuales recuperados nunca están cifrados. Puede habilitar el cifrado manualmente una vez se haya completado la recuperación.
  - Si realiza copias de seguridad de equipos virtuales cifrados, le recomendamos cifrar el equipo virtual en el que se está ejecutando Agente para VMware. En caso contrario, es posible que las operaciones realizadas con equipos cifrados sean más lentas de lo esperado. Aplique la **Directiva de cifrado de equipos virtuales** al equipo del agente mediante vSphere Web Client.
  - Los equipos virtuales cifrados se incluirán en la copia de seguridad mediante LAN, incluso si configura el modo de transporte SAN para el agente. El agente recurrirá al transporte NBD, pues VMware no es compatible con el transporte SAN para realizar copias de seguridad de discos virtuales cifrados.
- **Arranque seguro**
  - Equipos virtuales VMware: (introducidos en VMware vSphere 6.5) **Arranque seguro** está deshabilitado cuando un equipo virtual se ha recuperado como nuevo equipo virtual. Puede habilitar el cifrado manualmente una vez se haya completado la recuperación. Esta limitación se aplica a VMware.
  - Máquinas virtuales Hyper-V: en las máquinas virtuales de segunda generación, el arranque seguro se desactiva después de que el equipo se recupera tanto a una nueva máquina virtual como a una máquina virtual existente.
- **La copia de seguridad de configuración de ESXi** no es compatible con VMware vSphere 7.0 o versiones posteriores.
- **Los equipos virtuales con UUID de instancia vacíos no aparecen en la consola de Cyber Protect**

  Los equipos virtuales VMware con una propiedad vSphere `Instance UUID` vacía (`vc.uuid`) no aparecen en la consola de Cyber Protect. Para obtener más información sobre cómo resolver este problema, consulte este artículo de la base de conocimientos.
- **Configuración de red en el agente de protección**

  Una copia de seguridad de una máquina virtual VMware puede fallar si el agente de protección no puede resolver el nombre del host ESXi registrado en vCenter a una dirección IP, incluso si se puede resolver el nombre del host de vCenter. Se muestra el siguiente error: "No tiene derechos de acceso a este archivo".

  Para resolver el problema, edite la configuración de red del agente de protección, configurando el DNS o modificando el fichero `/etc/hosts`. Para verificar la solución, en el equipo con el agente de protección, ejecute el siguiente comando:

  ```
  ping <ESXi host name>
  ```
- **Operaciones admitidas para equipos con volúmenes lógicos**

© Acronis International GmbH, 2003-2025

La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

Nubes públicas

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Amazon EC2 instancias	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Microsoft Azure equipos virtuales	Compatible **Dispositivos** > **Agregar** > **Máquinas virtuales de Microsoft Azure**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Microsoft

Hyper-V máquinas virtuales que se ejecutan en un clúster hiperconvergente con Storage Spaces Direct (S2D). Storage Spaces Direct también es compatible como almacenamiento de copia de seguridad.

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Windows Server 2008 (x64) con Hyper-V Windows Server 2008 R2 con Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 con Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) con Hyper-V	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Microsoft Hyper-V**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

© Acronis International GmbH, 2003-2025

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Windows 10 con Hyper-V Windows 11 con Hyper-V Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server Windows Server 2025 con Hyper-V: todas las opciones de instalación, excepto Nano Server		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Microsoft Virtual Server 2005	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Nota
Se admiten los equipos virtuales Hyper-V que se ejecuten en un clúster hiperconvergente con Storage Spaces Direct (S2D). Storage Spaces Direct también es compatible como almacenamiento de copia de seguridad.

Limitaciones

- **Disco de paso a través**
  Agente para Hyper-V no realiza copias de seguridad de discos de paso a través. Durante la copia de seguridad, el agente omite estos discos y añade las advertencias al registro. Puede evitar las advertencias al excluir los discos de paso a través del plan de protección. Si desea realizar la

© Acronis International GmbH, 2003-2025

copia de seguridad de estos discos o de los datos que estos contienen, instale un agente en el sistema operativo invitado.

- **Agrupación de clústeres Hyper-V invitados**

  El agente para Hyper-V no es compatible con la copia de seguridad de los equipos virtuales de Hyper-V que son nodos de un clúster de conmutación por error de Windows Server. Una instantánea VSS al nivel del servidor puede desconectar temporalmente el disco de quórum externo del clúster. Si desea realizar la copia de seguridad de esos equipos, instale agentes en los sistemas operativos invitados.
- **Conexión iSCSI en invitado**

  Agente para Hyper-V no realiza copias de seguridad de volúmenes de LUN conectados mediante un iniciador iSCSI que funciona en el sistema operativo invitado. Como el hipervisor Hyper-V no es compatible con tales volúmenes, estos no se incluyen en las instantáneas a nivel de hipervisor y se omiten de una copia de seguridad sin emitir ningún aviso. Si desea realizar la copia de seguridad de estos volúmenes o de los datos que estos contienen, instale un agente en el sistema operativo invitado.
- **Nombres de archivos VHD/VHDX con el símbolo et (&)**

  En los servidores de Hyper-V que ejecutan Windows Server 2016 o una versión posterior, no puede hacer copias de seguridad de máquinas virtuales heredadas (versión 5.0) creadas originalmente con Hyper-V 2012 R2 o anterior si los nombres de los archivos VHD/VHDX contienen el símbolo et (&).

  Para poder hacer copias de seguridad de este tipo de equipos, vaya a Hyper-V Manager, desconecte el disco virtual correspondiente de la máquina virtual, elimine el símbolo et (&) del nombre del archivo VHD/VHDX y vuelva a conectar el disco a la máquina virtual.
- **Dependencia del subsistema WMI de Microsoft**

  Las copias de seguridad sin agente de equipos virtuales de Hyper-V dependen del subsistema WMI de Microsoft y, en particular, de la clase `Msvm_VirtualSystemManagementService`. Si las consultas WMI fallan, las copias de seguridad también fallarán. Para obtener más información sobre la clase `Msvm_VirtualSystemManagementService`, consulte la documentación de Microsoft.
- **Máquinas virtuales con discos PMEM**

  No se admite la copia de seguridad de máquinas virtuales Hyper-V que tienen discos de memoria persistente (PMEM).
- **Recuperación multiplataforma**

  Si el agente para Hyper-V recupera una copia de seguridad, creada por otro agente, como una nueva máquina virtual Hyper-V, la máquina resultante es de Generación 1.
- **Arranque seguro**

  Para garantizar el arranque de las máquinas virtuales Hyper-V de segunda generación que se recuperan, el arranque seguro se desactiva. Puede volver a activarlo manualmente en la herramienta de gestión Hyper-V. Para obtener más información sobre el arranque seguro y las máquinas virtuales de segunda generación, consulte la documentación de Microsoft.
- **Copias de seguridad de máquinas virtuales Linux resistentes a fallos**

© Acronis International GmbH, 2003-2025

Las copias de seguridad de máquinas virtuales Linux que se ejecutan en un host Hyper-V 2019 fallan en las instantáneas coherentes con fallos, debido a una limitación de Microsoft (incapacidad para crear puntos de control de producción para máquinas virtuales Linux). Para evitar advertencias durante una copia de seguridad, desactive la opción de copia de seguridad VSS para máquinas virtuales en el plan de protección.

- **Ejecución de un equipo virtual desde una copia de seguridad**
  La ejecución de una máquina virtual desde una copia de seguridad en un host Hyper-V falla si la copia de seguridad se encuentra en el mismo volumen que la ruta seleccionada para los discos VM montados. Para resolver el problema, seleccione un volumen diferente para la ruta de los discos VM montados. El espacio se utilizará solo para los cambios generados dentro de la máquina virtual montada, y no ocupará todo el tamaño del disco virtual.
- **Operaciones admitidas para equipos con volúmenes lógicos**
  La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

Scale Computing

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Scale Computing HyperCore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Scale Computing HyperCore**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Limitaciones

Operaciones admitidas para equipos con volúmenes lógicos

La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

© Acronis International GmbH, 2003-2025

Proxmox VE

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Proxmox VE 7.x, 8, and 8.1	No compatible	Solo admite invitados completamente virtualizados (HVM). No se admiten invitados paravirtualizados (PV). **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Proxmox VE 8.2, 8.3, 8.4, 9.0	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Proxmox VE**	Solo admite invitados completamente virtualizados (también denominados HVM). No se admiten invitados paravirtualizados (también denominados PV). **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Citrix Hypervisor/XenServer

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Citrix Hypervisor/XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2	No compatible	Solo admite invitados completamente virtualizados (también denominados HVM). No se admiten invitados paravirtualizados (también denominados PV). **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Citrix Hypervisor/XenServer** > **Windows** o **Linux**

© Acronis International GmbH, 2003-2025

Red Hat y Linux

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
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	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Red Hat Virtualization (gestionada por oVirt) 4.2, 4.3, 4.4 y 4.5	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Equipos virtuales basados en Kernel (KVM)	No compatible	Compatible **Dispositivos** > **Agregar** > **KVM** > **Windows** o **Linux**
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt 4.3 ejecutados en Red Hat Enterprise Linux 7.6, 7.7 o CentOS 7.6, 7.7	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt 4.4 ejecutados en Red Hat Enterprise Linux 8.x o CentOS Stream 8.x	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt 4.5 ejecutados en Red Hat Enterprise Linux 8.x o CentOS Stream 8.x	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Limitaciones

Operaciones admitidas para equipos con volúmenes lógicos

La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más

© Acronis International GmbH, 2003-2025

información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

Parallels

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Parallels Workstation	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Parallels Server 4 Bare Metal	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Oracle

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Oracle Linux Virtualization Manager (basado en oVirt)* 4.3	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Oracle LVM (oVirt)**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Oracle VM Server 3.0, 3.3, 3.4	No compatible	Solo admite invitados completamente virtualizados (también denominados HVM). No se admiten invitados paravirtualizados (también denominados PV). **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Oracle VM VirtualBox 4.x	No compatible	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

© Acronis International GmbH, 2003-2025

*Oracle Linux Virtualization Manager es compatible con Agent para oVirt .

Limitaciones

Operaciones admitidas para equipos con volúmenes lógicos

La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

Nutanix

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Sistema operativo Nutanix Acropolis (AOS) 6.5, 6.6, 6.7, 6.8, 6.10	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Nutanix AHV**	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Nutanix AHV** > **Windows** o **Linux**

Virtuozzo Hybrid Server

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Virtuozzo**	Compatible solo con máquinas virtuales. No se admiten contenedores. **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Virtuozzo 7.0.13, 7.0.14	Compatible solo con contenedores ploop. No se admiten equipos virtuales. **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Virtuozzo**	Compatible solo con máquinas virtuales. No se admiten contenedores. **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Virtuozzo Hybrid Server 7.5	Compatible	Compatible solo con máquinas

© Acronis International GmbH, 2003-2025

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
	Dispositivos > **Agregar** > **Hosts de virtualización** > **Virtuozzo**	virtuales. No se admiten contenedores. **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Limitaciones

Operaciones admitidas para equipos con volúmenes lógicos

La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

Virtuozzo Hybrid Infrastructure

Plataforma	Copia de seguridad sin agente (Copia de seguridad a nivel de hipervisor)	Copia de seguridad basada en agente (Copia de seguridad desde dentro de un SO invitado)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2, 6.3, 7.0	Compatible **Dispositivos** > **Agregar** > **Hosts de virtualización** > **Virtuozzo Hybrid infrastructure**	Compatible **Dispositivos** > **Agregar** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Limitaciones

- **Copia de seguridad sin agentes de máquinas virtuales con discos en un almacenamiento iSCSI externo**

  No puede ejecutar la copia de seguridad de las máquinas virtuales de Virtuozzo Hybrid Infrastructure si los discos de las máquinas virtuales se encuentran en volúmenes iSCSI externos (adjunto al clúster de VHI).
- **Operaciones admitidas para equipos con volúmenes lógicos**

  La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, se admiten con algunas limitaciones. Para obtener más información sobre las limitaciones, consulte "Operaciones admitidas con volúmenes lógicos" (p. 529).

© Acronis International GmbH, 2003-2025

Compatibilidad con almacenamientos Dell EMC Data Domain

Puede utilizar dispositivos Dell EMC Data Domain como almacenamiento de copia de seguridad.

Con este almacenamiento, recomendamos que utilice un esquema de copias de seguridad que cree regularmente copias de seguridad completas, por ejemplo **Siempre completo**. Para obtener más información sobre los esquemas de copias de seguridad disponibles, consulte "Esquemas de copia de seguridad" (p. 557).

Bloqueo de retención

Se admite el bloqueo de retención (modo de gobierno). Si el bloqueo de retención está habilitado en el almacenamiento Data Domain, debe añadir la variable de entorno `AR_RETENTION_LOCK_SUPPORT` al equipo con el agente de protección que utiliza este almacenamiento como destino de copia de seguridad. Para obtener más información, consulte "Añadir la variable AR_RETENTION_LOCK_SUPPORT" (p. 524).

Nota
Agente para Mac no admite almacenamiento Dell EMC Data Domain con el bloqueo de retención habilitado.

Si el bloqueo de retención está habilitado en el almacenamiento Data Domain, las copias de seguridad en el almacenamiento no serán eliminadas por las reglas de retención en el plan de protección. No se mostrará ningún error. Las copias de seguridad se eliminarán cuando expire el bloqueo de retención y se vuelvan a aplicar las reglas de retención.

Dependiendo de la configuración del plan de protección, las reglas de retención se aplican a un archivo antes o después de una copia de seguridad.

Añadir la variable AR_RETENTION_LOCK_SUPPORT

Si el bloqueo de retención está habilitado en el almacenamiento de Data Domain, debe añadir la variable de entorno `AR_RETENTION_LOCK_SUPPORT` a la máquina con el agente de protección que utiliza este almacenamiento como copia de seguridad.

Para añadir la variable de entorno `AR_RETENTION_LOCK_SUPPORT`

En Windows

1. Inicie sesión como administrador en el equipo con el agente de protección.
2. En **Panel de control**, vaya a **Sistema y seguridad** > **Sistema** > **Configuración avanzada del sistema**.
3. En la **pestaña Opciones avanzadas**, haga clic en **Variables de entorno**.
4. En el panel **Variables del sistema**, haga clic en **Nueva**.
5. En la ventana **Nueva variable del sistema**, añada la nueva variable tal como se indica:

© Acronis International GmbH, 2003-2025

- Nombre de la variable: `AR_RETENTION_LOCK_SUPPORT`
- Valor de la variable: `1`

6. Haga clic en **Aceptar**.
7. En la ventana **Variables de entorno**, haga clic en **Aceptar**.
8. Reinicie el equipo.

En Linux

1. Inicie sesión como administrador en el equipo con el agente de protección.
2. Vaya al directorio `/sbin` y abra el archivo `acronis_mms` para su edición.
3. Encima de la línea `export LD_LIBRARY_PATH`, añada la línea siguiente:

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. Guarde el archivo `acronis_mms`.
5. Reinicie el equipo.

En un dispositivo virtual

1. Inicie sesión como administrador en el dispositivo virtual.
2. Vaya al directorio `/bin` y abra el archivo `autostart` para su edición.
3. Debajo de la línea `export LD_LIBRARY_PATH`, añada la línea siguiente:

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. Guarde el archivo `autostart`.
5. Reiniciar el dispositivo virtual.

Sistemas de archivos compatibles

Un agente de protección puede realizar una copia de seguridad de cualquier sistema de archivos que sea accesible desde el sistema operativo en el que el agente está instalado. Por ejemplo, Agente para Windows puede realizar una copia de seguridad y recuperar un sistema de archivos ext4 si el controlador pertinente está instalado en Windows.

En la tabla siguiente se resumen los sistemas de archivos de los que se puede realizar una copia de seguridad y recuperar (los dispositivos de arranque solo son compatibles con la recuperación). Las limitaciones se aplican tanto a los agentes como a los dispositivos de arranque.

© Acronis International GmbH, 2003-2025

Sistema de archivos	Compatibilidad con			Limitaciones
	Agentes	Dispositivos de arranque para Windows y Linux	Dispositivos de arranque para Mac	
FAT16/32	Todos los agentes*	+	+	Sin limitaciones
NTFS	Todos los agentes	+	+	
ext2/ext3/ext4	Todos los agentes	+	-	
HFS+	Agente para Mac	-	+	
APFS	Agente para Mac	-	+	• Compatible a partir de macOS High Sierra 10.13 • La configuración del disco deberá volver a crearse manualmente cuando se recupera a un equipo no original o en una recuperación completa.
JFS	Agente para Linux	+	-	• Los filtros de archivo (Inclusiones/Exclusiones) no tienen soporte • No es posible habilitar la copia de seguridad diferencial incremental rápida
ReiserFS3	Agente para Linux	+	-	
ReiserFS4	Agente para Linux	+	-	• Los filtros de archivo (Inclusiones/Exclusiones) no tienen soporte • No es posible habilitar la copia de seguridad diferencial incremental rápida • No se puede cambiar el tamaño de los volúmenes durante la recuperación

© Acronis International GmbH, 2003-2025

Sistema de archivos	Compatibilidad con			Limitaciones
	Agentes	Dispositivos de arranque para Windows y Linux	Dispositivos de arranque para Mac	
ReFS	Todos los agentes	+	+	• Los filtros de archivo (Inclusiones/Exclusiones) no tienen soporte • No es posible habilitar la copia de seguridad diferencial incremental rápida • No se puede cambiar el tamaño de los volúmenes durante la recuperación • Durante la recuperación de un archivo desde una copia de seguridad ReFS, solo se recupera el contenido. Las listas de control de acceso (ACL) y los flujos alternativos no se recuperan. Los archivos dispersos se recuperan como archivos regulares.
XFS	Todos los agentes	+	+	• Los filtros de archivo (Inclusiones/Exclusiones) no tienen soporte • No es posible habilitar la copia de seguridad diferencial incremental rápida • No se puede cambiar el tamaño de los volúmenes durante la recuperación • El modo de copia de seguridad incremental rápida no es compatible con el sistema de archivos XFS. Las copias de seguridad

© Acronis International GmbH, 2003-2025

Sistema de archivos	Compatibilidad con			Limitaciones
	Agentes	Dispositivos de arranque para Windows y Linux	Dispositivos de arranque para Mac	
				diferenciales e incrementales de volúmenes XFS en la nube pueden ser mucho más lentas que unas copias de seguridad ext4 similares que usen el modo incremental rápido.
Linux swap	Agente para Linux	+	-	Sin limitaciones
exFAT	Todos los agentes	+ El dispositivo de arranque no se pueda usar para llevar a cabo la recuperación si la copia de seguridad *se almacena en* exFAT	+	• Solo son compatibles las copias de seguridad de disco o volumen • Los filtros de archivo (Inclusiones/Exclusiones) no tienen soporte • No se pueden recuperar archivos individuales desde una copia de seguridad

* En los sistemas Windows XP, el Agente para Windows solo es compatible con unidades formateadas en NTFS.

El software cambia automáticamente al modo sector por sector al hacer copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles (por ejemplo, Btrfs). Es posible realizar una copia de seguridad sector por sector para cualquier sistema de archivos que:

- esté basado en bloques
- abarque un único disco
- tenga un esquema de partición MBR/GPT estándar

Si el sistema de archivos no cumple estos requisitos, la copia de seguridad fallará.

© Acronis International GmbH, 2003-2025

Deduplicación de datos

En Windows Server 2012 y versiones posteriores, se puede activar la característica Deduplicación de datos para un volumen NTFS. La deduplicación de datos reduce el espacio utilizado en el volumen, ya que guarda una sola vez los fragmentos duplicados de los archivos del volumen.

Puede recuperar y realizar una copia de seguridad de un volumen donde esté activada la deduplicación de datos a nivel de discos sin ninguna limitación. Es posible hacer copias de seguridad a nivel de archivo excepto al usar Acronis VSS Provider. Para recuperar archivos a partir de una copia de seguridad del disco, ejecute un equipo virtual desde su copia de seguridad o monte la copia de seguridad en un equipo que ejecute Windows Server 2012 o una versión posterior, y luego copie los archivos desde el volumen montado.

La característica Deduplicación de datos de Windows Server no está relacionada con la característica Deduplicación de Acronis Backup.

Operaciones admitidas con volúmenes lógicos

La copia de seguridad y la recuperación de cargas de trabajo con volúmenes lógicos, como LDM en Windows (discos dinámicos) y LVM en Linux, son compatibles con las siguientes limitaciones.

Copia de seguridad

La copia de seguridad basada en agentes es una copia de seguridad creada por un agente de protección que se instala en la carga de trabajo o por un medio de arranque.

La copia de seguridad sin agente solo está disponible para máquinas virtuales. La copia de seguridad sin agente se realiza a nivel de hipervisor por un agente que puede respaldar y recuperar todas las máquinas virtuales en el entorno. No se instalan agentes individuales en las máquinas virtuales protegidas.

Para obtener más información sobre las diferencias entre la copia de seguridad basada en agentes y la copia de seguridad sin agentes, consulte "Copia de seguridad basada en agente y sin agente" (p. 41).

Copia de seguridad basada en agente	Copia de seguridad sin agente
• Las copias de seguridad de los volúmenes lógicos se llevan a cabo en función de cada volumen. • Se admiten filtros de archivos (Inclusiones/Exclusiones).	• Cuando se detecta un volumen lógico en un disco, el disco se respalda en el modo sector por sector (RAW). No se analiza la estructura de partición del disco y no se almacenan imágenes de volumen por separado. • No se pueden seleccionar volúmenes individuales LDM o LVM como fuente de la copia de seguridad, ni mediante selección directa ni mediante el uso de reglas de directiva. Solo **Todo el equipo** está disponible en la sección

© Acronis International GmbH, 2003-2025

Copia de seguridad basada en agente	Copia de seguridad sin agente
	Qué incorporar en la copia de seguridad de un plan de protección. • Los filtros de archivos (Inclusiones/Exclusiones) no se admiten. Cualquier inclusión o exclusión configurada será ignorada.

Recuperación

La recuperación basada en agentes es una recuperación realizada por un agente que está instalado en la carga de trabajo o por un medio de arranque.

La recuperación sin agente solo admite máquinas virtuales como objetivos. La recuperación sin agente se realiza a nivel de hipervisor por un agente que puede hacer copias de seguridad y recuperar todas las máquinas virtuales en el entorno. No tiene que crear manualmente un equipo objetivo en el que se recupere la copia de seguridad.

	Desde la copia de seguridad basada en agentes	Desde la copia de seguridad sin agente
Recuperación basada en agente	• La recuperación por volumen está disponible. • La recuperación de archivos y carpetas está disponible.	• La recuperación por volumen no está disponible. • La recuperación de archivos y carpetas está disponible.
Recuperación sin agente	• No se admite la migración de equipos (P2V, V2P y V2V). Para recuperar datos de una copia de seguridad basada en agentes, utilice un medio de arranque. • La operación **Ejecutar como máquina virtual** no se admite. • La recuperación de archivos y carpetas está disponible.	• La recuperación por volumen no está disponible. • La recuperación completa del equipo está disponible. • La recuperación de archivos y carpetas está disponible. • La operación **Ejecutar como máquina virtual** está admitida. Para hacer que la máquina virtual sea arrancable, es posible que necesite cambiar el orden de arranque. Para obtener más información, consulte este artículo de la base de conocimientos. • La conversión a los siguientes tipos de máquina virtual está admitida: ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

© Acronis International GmbH, 2003-2025

Compatibilidad con software de cifrado

No hay limitaciones en cuanto a las copias de seguridad y la recuperación de los datos que se hayan cifrado con el software de cifrado a *nivel de archivos*.

El software de cifrado a *nivel del disco* cifra los datos simultáneamente. Esta es la razón por la que los datos en la copia de seguridad no están cifrados. El software de cifrado a nivel del disco generalmente modifica áreas del sistema: registros de inicio, tablas de partición o tablas del sistema de archivos. Estos factores afectan a la copia de seguridad y recuperación a nivel del disco y la capacidad de un sistema de iniciar y acceder a Secure Zone.

Puede realizar una copia de seguridad de los datos cifrados con el software de cifrado a nivel del disco siguiente:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Para garantizar la fiabilidad de la recuperación a nivel del disco, siga las reglas comunes y las recomendaciones específicas del software.

Regla común de instalación

Es altamente recomendable instalar el software de cifrado antes que los agentes de protección.

Cómo utilizar Secure Zone

Secure Zone no debe estar cifrada con el cifrado a nivel del disco. Esta es la única forma de utilizar Secure Zone:

1. Instale el software de cifrado y, después, el agente.
2. Cree Secure Zone.
3. Excluya Secure Zone al cifrar el disco o sus volúmenes.

Regla común de copia de seguridad

Puede llevar a cabo una copia de seguridad a nivel del disco en el sistema operativo.

Procedimientos de recuperación específicos del software

Microsoft BitLocker Drive Encryption

Para recuperar un sistema cifrado con BitLocker:

1. Inicie desde el dispositivo de arranque.
2. Recupere el sistema. Los datos recuperados no estarán cifrados.

© Acronis International GmbH, 2003-2025

3. Reinicie el sistema recuperado.
4. Encienda BitLocker.

Si necesita recuperar solo una partición de un disco con múltiples particiones, hágalo en el sistema operativo. La recuperación en el dispositivo de arranque puede hacer que Windows no detecte la partición recuperada.

McAfee Endpoint Encryption y PGP Whole Disk Encryption

Puede recuperar una partición de sistema cifrada solo al utilizar un dispositivo de arranque.

Si el sistema recuperado no inicia, vuelva a crear el registro de inicio maestro según se describe en el siguiente artículo de la Microsoft Knowledge Base: https://support.microsoft.com/kb/2622803

Compatibilidad con discos duros de formato avanzado (sector de 4 K)

La copia de seguridad y la recuperación son compatibles con discos duros tradicionales con tamaño de sector de 512 bytes y con discos de formato avanzado con tamaño de sector de 4096 bytes.

Cuando recupera datos de un disco a otro, ambos discos deben tener el mismo tamaño de sector lógico (este es el tamaño que se presenta al sistema operativo). Los volúmenes en el disco se alinean automáticamente, si es necesario. Así, el inicio de un clúster en el sistema de archivos siempre coincide con el inicio de un sector físico en el disco.

La Asociación Internacional de Equipos y Materiales de Unidades de Disco (IDEMA) especifica dos tipos de discos de formato avanzado:

- discos de emulación de 512 bytes (512e)
  Estos discos tienen un tamaño de sector lógico de 512 bytes.
- discos nativos de 4K (4Kn)
  Estos discos tienen un tamaño de sector lógico de 4096 bytes.
  Los discos 4Kn se utilizan comúnmente como unidades externas con conexión USB. El arranque del sistema podría no ser compatible con estos discos.

Para más información sobre el formato avanzado, consulte https://idema.org/initiatives/advanced-format.

Pasos para comprobar el tamaño de sector lógico de un disco

Windows

1. Asegúrese de que el disco contiene un volumen NTFS.
2. Ejecute el siguiente comando como administrador, especificando la letra del dispositivo del volumen NTFS (por ejemplo, `D`):

```
fsutil fsinfo ntfsinfo D:
```


© Acronis International GmbH, 2003-2025

3. Compruebe el valor en la línea **Bytes Per Sector**.
   Por ejemplo:

```
Bytes Per Sector: 512
```

Linux

1. Compruebe el nombre del dispositivo del disco.
   Por ejemplo `/dev/sdb`.
2. Ejecute el siguiente comando como usuario root, especificando el nombre del dispositivo del disco:

```
parted /dev/sdb print
```

3. Compruebe el primer valor en la línea **Sector size (logical/physical)**.
   Por ejemplo:

```
Sector size (logical/physical): 512B/4096B
```

Copia de seguridad

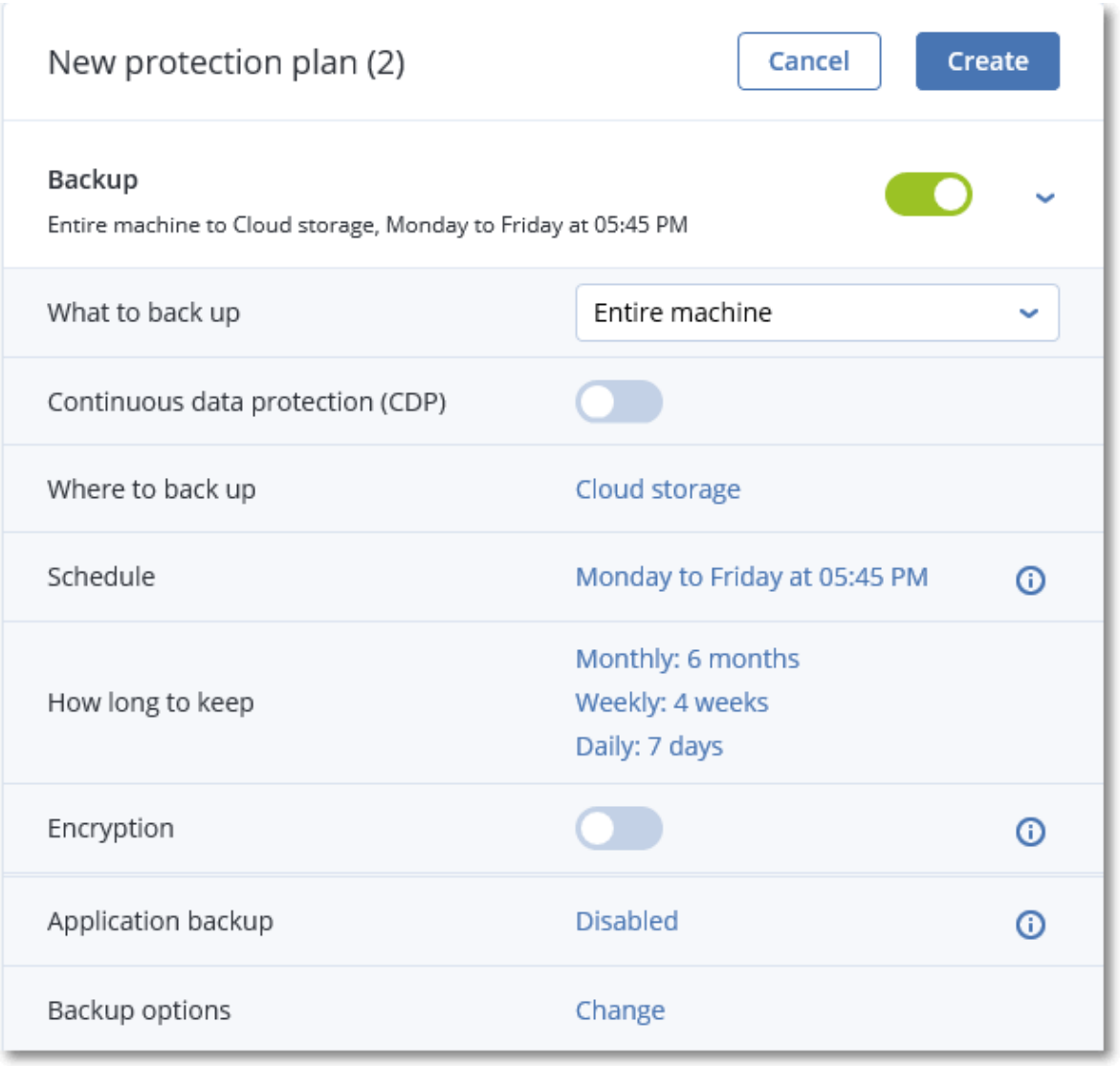
Un plan de protección con el módulo de copia de seguridad habilitado es un conjunto de reglas que especifican como se protegerán los datos de un equipo concreto.

Cuando cree un plan de protección, puede aplicarlo a múltiples equipos en ese momento o más adelante.

Pasos para crear el primer plan de protección con el módulo de copia de seguridad habilitado

1. Seleccione los equipos que desea incluir en la copia de seguridad.
2. Haga clic en **Proteger**.
   Se mostrarán los planes de protección que están aplicados al equipo. Si no hay ningún plan de protección asignado al equipo todavía, verá el plan de protección predeterminado que se puede aplicar. Puede cambiar la configuración según sea necesario y aplicar este plan, o crear uno nuevo.
3. Para crear un plan nuevo, haga clic en **Crear plan**. Habilite el módulo **Copia de seguridad** y despliegue la configuración.

© Acronis International GmbH, 2003-2025

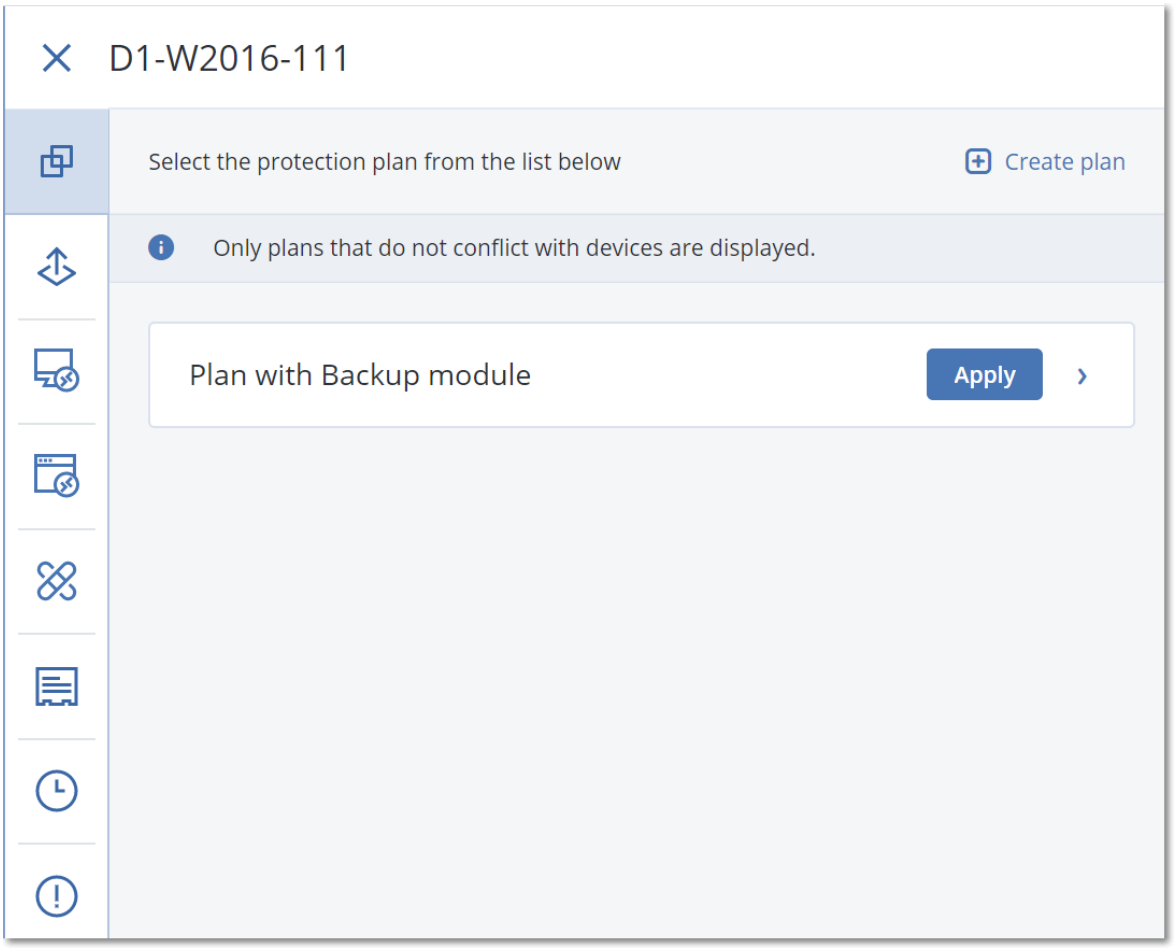


4. [Opcional] Para modificar el nombre del plan de protección, haga clic en el nombre predeterminado.
5. [Opcional] Para modificar los parámetros del módulo de copia de seguridad, haga clic en la configuración correspondiente del panel del plan de protección.
6. [Opcional] Para modificar las opciones de copia de seguridad, haga clic en **Modificar**, que se encuentra junto a **Opciones de copia de seguridad**.
7. Haga clic en **Crear**.

Pasos para aplicar un plan de protección existente

1. Seleccione los equipos que desea incluir en la copia de seguridad.
2. Haga clic en **Proteger**. Si ya se aplica un plan de protección común a los equipos seleccionados, haga clic en **Agregar plan**.
   El software muestra planes de protección creados previamente.

© Acronis International GmbH, 2003-2025



3. Seleccione el plan de protección que desea aplicar.
4. Haga clic en **Aplicar**.

Hoja de referencia de la copia de seguridad

En la siguiente tabla se resumen los parámetros más comunes de la copia de seguridad.

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	ELEMENTOS QUE SE INCLUIRÁN EN LA COPIA DE SEGURIDAD Métodos de selección	DÓNDE GUARDAR LAS COPIAS DE SEGURIDAD	PLANIFICAR Esquemas de copia de seguridad
Discos/volúmenes (equipos físicos[1])	Selección directa Normas de directiva Filtros de archivo	Nube Carpeta local Carpeta de red	Siempre incremental (un archivo) Siempre completa

[1]Un equipo que tiene una copia de seguridad realizada por un agente instalado en el sistema operativo.

© Acronis International GmbH, 2003-2025

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	ELEMENTOS QUE SE INCLUIRÁN EN LA COPIA DE SEGURIDAD Métodos de selección	DÓNDE GUARDAR LAS COPIAS DE SEGURIDAD	PLANIFICAR Esquemas de copia de seguridad
		NFS* Secure Zone**	Completa semanal, incremental diaria Completa mensual, diferencial semanal, incremental diaria (GFS) Personalizadas (F-D-I)
Discos/volúmenes (equipos virtuales[1])	Normas de directiva Filtros de archivo	Nube Carpeta local Carpeta de red NFS*	
Archivos (solo equipos físicos[2])	Selección directa Normas de directiva Filtros de archivo	Nube Carpeta local Carpeta de red NFS* Secure Zone**	Siempre incremental (un archivo) Siempre completa Completa semanal, incremental diaria Completa mensual, diferencial semanal, incremental diaria (GFS) Personalizadas (F-D-I)
Configuración de ESXi	Selección directa	Carpeta local Carpeta de red NFS*	
Sitios web (archivos y bases de datos MySQL)	Selección directa	Nube	—
Estado del sistema	Selección directa	Nube Carpeta local Carpeta de red	Siempre completa Completa semanal, incremental diaria Personalizadas (F-I) Siempre incremental (un archivo): solo para base de datos SQL
Bases de datos SQL	Selección directa		
Bases de datos de Exchange	Selección directa		

[1]Un equipo virtual que tiene una copia de seguridad a nivel de hipervisor realizada por un agente externo como Agente para VMware o Agente para Hyper-V. Un equipo virtual con un agente dentro se considera un equipo físico desde la perspectiva de la copia de seguridad.
[2]Un equipo que tiene una copia de seguridad realizada por un agente instalado en el sistema operativo.

© Acronis International GmbH, 2003-2025

DE QUÉ REALIZAR COPIAS DE SEGURIDAD		ELEMENTOS QUE SE INCLUIRÁN EN LA COPIA DE SEGURIDAD Métodos de selección	DÓNDE GUARDAR LAS COPIAS DE SEGURIDAD	PLANIFICAR Esquemas de copia de seguridad
Microsoft 365	Buzones de correo (Agente local para Microsoft 365)	Selección directa	Nube Carpeta local Carpeta de red	Siempre incremental (un archivo)
	Buzones de correo (Agente en la nube para Microsoft 365)	Selección directa	Nube	Hasta 6 copias de seguridad al día
	Carpetas públicas	Selección directa		
	Teams	Selección directa		
	Archivos de OneDrive	Selección directa Normas de directiva		
	Datos de SharePoint Online	Selección directa Normas de directiva		
Google Workspace	Buzones de correo de Gmail	Selección directa	Nube	Hasta 6 copias de seguridad al día
	Archivos de Google Drive	Selección directa Normas de directiva		
	Archivos de unidades compartidas	Selección directa Normas de directiva		

* En Windows no se pueden hacer copias de seguridad en NFS compartidos.

** Secure Zone no se puede crear en un Mac.

Nota
Las copias de seguridad en la nube pública requieren una cuota de almacenamiento en **Copia de seguridad local**.

¿Cuánto tiempo se conservarán las copias de seguridad?

Puede conservar sus copias de seguridad para siempre o configurar un período de retención según los siguientes criterios:

© Acronis International GmbH, 2003-2025

- Por antigüedad de las copias de seguridad (regla única/por conjunto de copias de seguridad)
- Por número de copias de seguridad
- Por tamaño total de las copias de seguridad

Nota
La regla de retención **Por tamaño total de las copias de seguridad** no está disponible con el esquema de copias de seguridad **Siempre incremental (un archivo)** o al guardar las copias de seguridad en el almacenamiento en la nube.

Consulte Reglas de retención.

Seleccionar los datos que se incluirán en la copia de seguridad

Selección de todo el equipo

La copia de seguridad de un equipo entero es una copia de seguridad de todos sus discos no extraíbles. Para obtener más información sobre la copia de seguridad del disco, consulte "Seleccionar discos o volúmenes" (p. 538).

Limitaciones

- Las copias de seguridad a nivel de disco no son compatibles con los volúmenes APFS bloqueados. Durante una copia de seguridad de un equipo entero, esos volúmenes se omiten.
- No puede recuperar el contenido de la carpeta raíz de OneDrive desde **Todo el equipo** o una copia de seguridad de **discos/volumen**, aunque la carpeta de OneDrive se muestre al navegar por el archivo comprimido de copia de seguridad en una aplicación de administrador de archivos, como Explorador de archivos. Al navegar por el archivo comprimido de copia de seguridad en la consola de Cyber Protect, no se muestra la carpeta de OneDrive. Al navegar por el archivo comprimido de copia de seguridad en la consola de Web Restore, se muestra la carpeta de OneDrive como un archivo, pero no es posible la recuperación desde esta copia de seguridad.
  Para poder recuperar el contenido de la carpeta de OneDrive, cree una copia de seguridad de **archivos/carpetas**. Los archivos que no estén disponibles en el dispositivo se mostrarán en el archivo comprimido, pero no se podrán recuperar.

Seleccionar discos o volúmenes

Una copia de seguridad a nivel de discos contiene una copia de un disco o un volumen en forma compacta. Puede recuperar discos, volúmenes, carpetas y archivos desde una copia de seguridad de nivel de disco.

Puede seleccionar los discos o volúmenes que se van a incluir en la copia de seguridad de cada carga de trabajo individual del plan de protección (selección directa) o configurar reglas de directiva

© Acronis International GmbH, 2003-2025

para varias cargas de trabajo. Asimismo, puede excluir determinados archivos de una copia de seguridad o incluir solo archivos específicos en ella mediante la configuración de filtros de archivo. Para obtener más información, consulte "Filtros de archivo (inclusiones y exclusiones)" (p. 607).

Pasos para seleccionar discos o volúmenes

Selección directa

La selección directa está disponible únicamente para los equipos físicos.

1. En **Qué incorporar en la copia de seguridad**, seleccione **Discos/volúmenes**.
2. Haga clic en **Elementos que se incluirán en la copia de seguridad**.
3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Directamente**.
4. Para cada una de las cargas de trabajo que se incluyen en el plan de protección, seleccione las casillas de verificación que se encuentran al lado de los discos o volúmenes que se van a incluir en la copia de seguridad.
5. Haga clic en **Listo**.

Por reglas de directiva

1. En **Qué incorporar en la copia de seguridad**, seleccione **Discos/volúmenes**.
2. Haga clic en **Elementos que se incluirán en la copia de seguridad**.
3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Usar las normas de directiva**.
4. Seleccione cualquiera de las normas predefinidas, escriba sus propias normas o combine las dos.

   Para obtener más información sobre las reglas de directiva disponibles, consulte "Reglas de directiva para discos y volúmenes" (p. 541).

   Las reglas de directiva se aplicarán a todas las cargas de trabajo incluidas en el plan de protección.

   Si ninguna de las reglas especificadas puede aplicarse a una carga de trabajo, la copia de seguridad de dicha carga de trabajo fallará.
5. Haga clic en **Listo**.

Limitaciones

- Las copias de seguridad a nivel de disco no son compatibles con los volúmenes APFS bloqueados. Durante una copia de seguridad de un equipo entero, esos volúmenes se omiten.
- No puede recuperar el contenido de la carpeta raíz de OneDrive desde **Todo el equipo** o una copia de seguridad de **discos/volumen**, aunque la carpeta de OneDrive se muestre al navegar por el archivo comprimido de copia de seguridad en una aplicación de administrador de archivos, como Explorador de archivos. Al navegar por el archivo comprimido de copia de seguridad en la consola de Cyber Protect, no se muestra la carpeta de OneDrive. Al navegar por el archivo comprimido de copia de seguridad en la consola de Web Restore, se muestra la carpeta de

© Acronis International GmbH, 2003-2025

OneDrive como un archivo, pero no es posible la recuperación desde esta copia de seguridad. Para poder recuperar el contenido de la carpeta de OneDrive, cree una copia de seguridad de **archivos/carpetas**. Los archivos que no estén disponibles en el dispositivo se mostrarán en el archivo comprimido, pero no se podrán recuperar.

- Puede hacer una copia de seguridad de los discos conectados mediante el protocolo iSCSI a un equipo físico. Sin embargo, se aplican limitaciones si usa Agente para VMware o Agente para Hyper-V para realizar la copia de seguridad de los discos conectados mediante iSCSI. Para obtener más información, consulte "Limitaciones" (p. 513).

¿Qué almacena una copia de seguridad de un disco o volumen?

Una copia de seguridad de disco o volumen almacena un **sistema de archivos** de discos o volúmenes de forma completa e incluye toda la información necesaria para que el sistema operativo se inicie. Es posible recuperar discos o volúmenes de forma completa a partir de estas copias de seguridad, así como carpetas o archivos individuales.

Con la opción de copia de seguridad **sector por sector (modo sin procesar)** habilitada, una copia de seguridad del disco almacena todos los sectores del disco. La copia de seguridad sector por sector se puede utilizar para realizar copias de seguridad de discos con sistemas de archivos no reconocidos o incompatibles, o formatos de datos de terceros.

Windows

Una copia de seguridad de volumen almacena todos los archivos y las carpetas del volumen seleccionado, independientemente de sus atributos (incluidos los archivos ocultos y del sistema), el registro de inicio, la tabla de asignación de archivos (FAT) si existe, la raíz y la pista cero del disco duro con el registro de inicio maestro (MBR).

Una copia de seguridad del disco almacena todos los volúmenes del disco seleccionado (incluidos volúmenes ocultos como las particiones de mantenimiento del proveedor) y la ísta cero con el registro de inicio maestro.

Los siguientes elementos *no* se incluyen en una copia de seguridad de disco o volumen (así como en una copia de seguridad a nivel de archivo):

- El archivo de intercambio (pagefile.sys) ni el archivo que mantiene el contenido de la memoria RAM cuando el equipo ingresa al estado de hibernación (hiberfil.sys). Después de la recuperación, los archivos se pueden volver a crear en el lugar apropiado con el tamaño cero.
- Si la copia de seguridad se realiza bajo el sistema operativo (a diferencia de dispositivos de arranque o la copia de seguridad de equipos virtuales en un nivel de hipervisor):
  - Almacenamiento de instantáneas de Windows. La ruta se determina en el valor de registro **Proveedor predeterminado de VSS** que puede encontrarse en la clave de registro **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Esto significa que no se les realizan copias de seguridad en los sistemas operativos Windows Vista, puntos de restauración de Windows.

© Acronis International GmbH, 2003-2025

- Si se habilita la opción de copia de seguridad **Servicio de instantáneas de volumen (VSS)**, los archivos y carpetas especificados en la clave de registro **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**.

Linux

Una copia de seguridad de volumen almacena todos los archivos y directorios del volumen seleccionado, independientemente de sus atributos, un registro de inicio y el superbloque del sistema de archivos.

Una copia de seguridad del disco almacena todos los volúmenes del disco y también el registro cero junto con el registro de inicio maestro.

Mac

Un disco o copia de seguridad de volumen almacena todos los archivos y directorios del disco o volumen seleccionado, junto con una descripción de la distribución del volumen.

Los siguientes elementos están excluidos:

- Metadatos del sistema, como el diario del sistema de archivos y el índice de Spotlight
- Papelera de reciclaje
- Copias de seguridad de Time Machine

Físicamente, las copias de seguridad de los discos y volúmenes de un Mac se realizan a nivel de archivo. Es posible la recuperación completa desde copias de seguridad de disco y de volumen, pero el modo de copia de seguridad sector por sector no está disponible.

Reglas de directiva para discos y volúmenes

Cuando selecciona discos o volúmenes para hacer una copia de seguridad, puede utilizar las siguientes reglas de directiva, según el sistema operativo de la carga de trabajo protegida.

Windows

- `[All Volumes]` selecciona todos los volúmenes del equipo.
- La letra de unidad (por ejemplo, `C:\`) selecciona el volumen con la letra de la unidad especificada.
- `[Fixed Volumes (physical machines)]` selecciona todos los volúmenes de un equipo físico, además de los dispositivos extraíbles. Los volúmenes fijos incluyen aquellos en dispositivos iSCSI, SCSI, ATAPI, ATA, SSA, SAS y SATA, y conjuntos RAID.
- `[BOOT+SYSTEM]` selecciona los volúmenes de arranque y del sistema. Esta es la combinación mínima desde la que puede recuperar un sistema operativo.
- `[Disk 1]` selecciona el primer disco del equipo, incluidos todos los volúmenes de ese disco. Para seleccionar otro disco, escriba el número correspondiente.

Linux

© Acronis International GmbH, 2003-2025

- `[All Volumes]` selecciona todos los volúmenes montados del equipo.
- `/dev/hda1` selecciona el primer volumen en el primer disco rígido IDE.
- `/dev/sda1` selecciona el primer volumen en el primer disco rígido SCSI.
- `/dev/md1` selecciona el primer disco rígido de software RAID.
- Para seleccionar otros volúmenes básicos, especifique `/dev/xdyN`, donde:
  - «x» corresponde al tipo de disco
  - «y» corresponde al número de disco (a para el primer disco, b para el segundo disco y así sucesivamente)
  - «N» es el número de volumen.
- Para seleccionar un volumen lógico, especifique su ruta tal y como aparece después de ejecutar el comando `ls /dev/mapper` en su cuenta raíz.

  Por ejemplo:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Este resultado muestra dos volúmenes lógicos, `lv1` y `lv2`, que pertenecen al grupo de volúmenes `vg_1`. Para hacer una copia de seguridad de estos volúmenes, especifique:

  `/dev/mapper/vg_1-lv1`

  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` selecciona todos los volúmenes montados del equipo.
- `[Disk 1]` selecciona el primer disco del equipo, incluidos todos los volúmenes de ese disco. Para seleccionar otro disco, especifique el número correspondiente.

Seleccionar archivos o carpetas

Utilice la copia de seguridad a nivel de archivo para proteger solo datos específicos, por ejemplo, los archivos de su proyecto actual. Las copias de seguridad a nivel de archivo son más pequeñas que las de nivel disco y ahorran espacio de almacenamiento.

Importante
No puede recuperar un sistema operativo desde una copia de seguridad a nivel de archivos.

Puede seleccionar los archivos y carpetas que se van a incluir en la copia de seguridad de cada carga de trabajo individual del plan de protección (selección directa) o configurar reglas de directiva para varias cargas de trabajo. Asimismo, puede excluir determinados archivos de una copia de seguridad o incluir solo archivos específicos en ella mediante la configuración de filtros. Para obtener más información, consulte "Filtros de archivo (inclusiones y exclusiones)" (p. 607).

Pasos para seleccionar archivos o carpetas

Selección directa

 © Acronis International GmbH, 2003-2025

1. En **Qué incorporar en la copia de seguridad**, seleccione **Archivos/carpetas**.
2. En **Elementos que se incluirán en la copia de seguridad** haga clic en **Especificar**.
3. En **Seleccionar elementos que se incluirán en la copia de seguridad**, seleccione **Directamente**.
4. Especifique los archivos y carpetas que se van a incluir en la copia de seguridad de cada carga de trabajo del plan de protección.
   a. Haga clic en **Seleccionar archivos y carpetas**.
   b. Haga clic en **Carpeta local** o **Carpeta de red**.
      Las carpetas de red deben estar accesibles desde el equipo seleccionado.
      Si selecciona **Carpeta de red** como fuente, podrá realizar copias de seguridad de los datos de los almacenes conectados a la red (NAS), como los dispositivos de NetApp. Los dispositivos NAS de todos los proveedores son compatibles.
   c. Seleccione los archivos y las carpetas a los que desea realizarles copias de seguridad.
      Puede seleccionar una combinación de hasta 1000 archivos y carpetas.
      Alternativamente, puede especificar la ruta a un archivo o carpeta y luego hacer clic en el botón de flecha.
   d. [Para carpetas compartidas] Especifique el nombre de usuario y la contraseña de la carpeta compartida.
      No se admite la copia de seguridad de carpetas con acceso anónimo.
   e. Haga clic en **Listo**.

Por reglas de directiva

1. En **Qué incorporar en la copia de seguridad**, seleccione **Archivos/carpetas**.
2. En **Elementos que se incluirán en la copia de seguridad** haga clic en **Especificar**.
3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Usar las normas de directiva**.
4. Seleccione cualquiera de las normas predefinidas, escriba sus propias normas o combine las dos.
   Para obtener más información sobre las reglas de directiva disponibles, consulte "Reglas de directiva para los archivos y las carpetas" (p. 544).
   Las reglas de directiva se aplicarán a todas las cargas de trabajo incluidas en el plan de protección.
   Si ninguna de las reglas especificadas puede aplicarse a una carga de trabajo, la copia de seguridad de dicha carga de trabajo fallará.
5. Haga clic en **Listo**.

Limitaciones

- Puede seleccionar archivos y carpetas cuando haga copias de seguridad de los equipos físicos o las máquinas virtuales en los que esté instalado un agente (copia de seguridad basada en

© Acronis International GmbH, 2003-2025

agente). La copia de seguridad a nivel de archivo no está disponible para máquinas virtuales de las que realizó la copia de seguridad en el modo sin agente. Para obtener más información acerca de las diferencias entre estos tipos de copia de seguridad, consulte "Copia de seguridad basada en agente y sin agente" (p. 41).

- No puede recuperar el contenido de la carpeta raíz de OneDrive desde **Todo el equipo** o una copia de seguridad de **discos/volumen**, aunque la carpeta de OneDrive se muestre al navegar por el archivo comprimido de copia de seguridad en una aplicación de administrador de archivos, como Explorador de archivos. Al navegar por el archivo comprimido de copia de seguridad en la consola de Cyber Protect, no se muestra la carpeta de OneDrive. Al navegar por el archivo comprimido de copia de seguridad en la consola de Web Restore, se muestra la carpeta de OneDrive como un archivo, pero no es posible la recuperación desde esta copia de seguridad.

  Para poder recuperar el contenido de la carpeta de OneDrive, cree una copia de seguridad de **archivos/carpetas**. Los archivos que no estén disponibles en el dispositivo se mostrarán en el archivo comprimido, pero no se podrán recuperar.
- Puede hacer una copia de seguridad de los archivos y carpetas ubicados en discos conectados mediante el protocolo iSCSI a un equipo físico. Se aplican algunas limitaciones si usa Agente para VMware o Agente para Hyper-V para realizar la copia de seguridad de los datos de los discos conectados mediante iSCSI.

Reglas de directiva para los archivos y las carpetas

Cuando selecciona archivos o carpetas para hacer una copia de seguridad, puede utilizar las siguientes reglas de directiva, según el sistema operativo de la carga de trabajo protegida.

Windows

- Ruta completa a un archivo o carpeta. Por ejemplo `D:\Work\Text.doc` o `C:\Windows`.
- Reglas predefinidas:
  - `[All Files]` selecciona todos los archivos que hay en los volúmenes del equipo.
  - `[All Profiles Folder]` selecciona la carpeta en la que se encuentran todos los perfiles de usuario. Por ejemplo, `C:\Users` o `C:\Documents and Settings`.
- Variables de entorno:
  - `%ALLUSERSPROFILE%` selecciona la carpeta en la que se encuentran los datos habituales de todos los perfiles de usuario. Por ejemplo, `C:\ProgramData` o `C:\Documents and Settings\All Users`.
  - `%PROGRAMFILES%` selecciona la carpeta `Program Files`. Por ejemplo, `C:\Program Files`.
  - `%WINDIR%` selecciona la carpeta `Windows`. Por ejemplo, `C:\Windows`.

  Puede utilizar otras variables de entorno o una combinación de variables de entorno y texto. Por ejemplo, para seleccionar la carpeta Java en la carpeta archivos de programa, especifique: `%PROGRAMFILES%\Java`.

Linux

© Acronis International GmbH, 2003-2025

- Ruta completa a un archivo o directorio.

  Por ejemplo, para realizar una copia de seguridad del archivo `file.txt` en el volumen `/dev/hda3` incorporado en `/home/usr/docs`, especifique `/dev/hda3/file.txt` o `/home/usr/docs/file.txt`.
- Reglas predefinidas:
  - `[All Profiles Folder]` selecciona `/home`. De forma predeterminada, todos los perfiles de usuario se almacenan en esta carpeta.
  - `/home` selecciona el directorio de inicio de los usuarios habituales.
  - `/root` selecciona el directorio de inicio de los usuarios raíz.
  - `/usr` selecciona el directorio para todos los programas relacionados con los usuarios.
  - `/etc` selecciona el directorio para los archivos de configuración del sistema.

macOS

- Ruta completa a un archivo o directorio.

  Por ejemplo:
  - Para realizar una copia de seguridad `file.txt` en el escritorio de un usuario, especifique `/Users/<user name>/Desktop/file.txt`.
  - Para realizar una copia de seguridad de las carpetas `Desktop`, `Documents` y `Downloads` de un usuario, especifique `/Users/<user name>/Desktop`, `/Users/<user name>/Documents` y `/Users/<user name>/Downloads`, respectivamente.
  - Para realizar una copia de las carpetas de inicio de todos los usuarios con una cuenta en este equipo, especifique `/Users`.
  - Para hacer copias de seguridad de la carpeta donde están instaladas las aplicaciones, especifique `/Applications`.
- Reglas predefinidas
  - `[All Profiles Folder]` selecciona `/Users`. De forma predeterminada, todos los perfiles de usuario se almacenan en esta carpeta.

Seleccionar un estado del sistema

Nota
La copia de seguridad del estado del sistema está disponible para los equipos que ejecutan de Windows 7 en adelante en los que el Agente para Windows está instalado. La copia de seguridad del estado del sistema no está disponible para las máquinas virtuales de las que se hace una copia de seguridad a nivel del hipervisor (copia de seguridad sin agente).

Para realizar copias de seguridad del estado del sistema, en **Qué incorporar en la copia de seguridad**, seleccione **Estado del sistema**.

La copia de seguridad de un estado del sistema está formada por los siguientes archivos:

- Configuración del programador de tareas
- Almacenamiento de metadatos de VSS

© Acronis International GmbH, 2003-2025

- Información de configuración del contador de rendimiento
- Servicio MSSearch
- Servicio de transferencia inteligente en segundo plano (BITS)
- El registro
- Windows Management Instrumentation (WMI)
- Base de datos del registro de Component Services Class

Selección de la configuración de ESXi

Una copia de seguridad de una configuración de servidor ESXi permite recuperar un servidor ESXi desde cero. La recuperación se lleva a cabo con un dispositivo de arranque.

Los equipos virtuales que se ejecutan en el servidor no se incluyen en la copia de seguridad. Se puede hacer una copia de seguridad de ellos y se pueden recuperar por separado.

Una copia de seguridad de una configuración de servidor ESXi incluye:

- Las particiones del cargador de arranque y el banco de arranque del servidor.
- El estado del servidor (configuración del almacenamiento y las redes virtuales, claves SSL, ajustes de la red del servidor e información del usuario local).
- Extensiones o parches instalados o montados en el servidor.
- Archivos de registro.

Requisitos previos

- SSH debe estar habilitado en el **Perfil de seguridad** de la configuración del servidor ESXi.
- Tiene que conocer la contraseña de la cuenta "raíz" alojada en el servidor ESXi.

Limitaciones

- La copia de seguridad de configuración de ESXi no es compatible con hosts que ejecutan VMware ESXi 7.0 y versiones posteriores.
- No se puede realizar una copia de seguridad en el almacenamiento en la nube de una configuración de ESXi.

Para seleccionar una configuración de ESXi

1. Haga clic en **Dispositivos** > **Todos los dispositivos** y seleccione los servidores ESXi de los que desea hacer una copia de seguridad.
2. Haga clic en **Proteger**.
3. En **Qué incorporar en la copia de seguridad**, seleccione **Configuración de ESXi**.
4. En **Contraseña "raíz" de ESXi**, indique una contraseña para la cuenta "raíz" de cada uno de los servidores seleccionados o aplique la misma contraseña a todos los servidores.

© Acronis International GmbH, 2003-2025

Seleccionar un destino

Haga clic en **Dónde guardar las copias de seguridad** y seleccione una de las siguientes opciones:

- **Almacenamiento en la nube**

  Las copias de seguridad se almacenarán en el centro de datos de la cloud.

  Nota
  Las copias de seguridad en la nube pública requieren una cuota de almacenamiento en **Copia de seguridad local**.

- **Carpetas locales**

  Si se selecciona un único equipo, busque una carpeta en el equipo seleccionado o escriba la ruta de la carpeta.

  Si se seleccionan varios equipos, escriba la ruta de la carpeta. Las copias de seguridad se almacenarán en esta carpeta en cada uno de los equipos seleccionados o en el equipo en el que está instalado el Agente para equipos virtuales. Si la carpeta no existe, se creará.

- **Carpeta de red**

  Esta carpeta se comparte a través de SMB/CIFS/DFS.

  Navegue hasta la carpeta compartida requerida o introduzca la ruta en el siguiente formato, donde <host> es un nombre de dominio DNS completo o una dirección IPv4:

  - Para recursos compartidos SMB/CIFS:
    - \\<host>\<path>\
    - smb://<host>/<path>/
  - Para recursos compartidos DFS:
    - \\<host>\<DFS root>\<path>

  Luego haga clic en el botón de la flecha. Si se le pide, especifique el nombre de usuario y la contraseña de la carpeta compartida. Puede modificar estas credenciales en cualquier momento al hacer clic en el icono de llave que se encuentra junto al nombre de la carpeta.

  No se admite la copia de seguridad a una carpeta con acceso anónimo.

- **Nube pública**

  Esta opción está disponible como parte del paquete Advanced Backup.

  Le permite configurar una copia de seguridad directa en un almacenamiento compatible en la nube pública sin necesidad de desplegar componentes adicionales (como Microsoft Azure u otras máquinas virtuales como puertas de enlace). Seleccione la nube pública correspondiente y conéctese a ella si es necesario.

  Nota
  Las copias de seguridad en la nube pública requieren una cuota de almacenamiento en **Copia de seguridad local**.

© Acronis International GmbH, 2003-2025

Para obtener más información, consulte "Hacer copias de seguridad de cargas de trabajo en nubes públicas" (p. 734).

- **Carpeta NFS** (disponible para equipos que ejecutan Linux o macOS)

  Compruebe que el paquete nfs-utils esté instalado en el servidor Linux en el que está instalado el agente para Linux.

  Navegue hasta la carpeta NFS requerida o introduzca la ruta en el siguiente formato, donde <host> es un nombre de dominio DNS completo o una dirección IPv4:

  nfs://<host>/<exported folder>:/<subfolder>

  Luego haga clic en el botón de la flecha.

  Nota
  No se puede realizar una copia de seguridad en una carpeta NFS protegida con contraseña.

- **Secure Zone** (disponible si está en todos los equipos seleccionados)

  Secure Zone es una partición segura que está en un disco del equipo incluido en la copia de seguridad. Esta partición debe crearse manualmente antes de configurar una copia de seguridad. Para obtener información sobre cómo crear Secure Zone y sus ventajas y limitaciones, consulte "Acerca de Secure Zone" (p. 549).

Opción de almacenamiento avanzada

Nota
Esta función está disponible únicamente en la edición Advanced del servicio Cyber Protection.

Definido por una secuencia de comandos (disponible en equipos Windows)

Puede almacenar las copias de seguridad de cada equipo en una carpeta definida por un script. El software es compatible con comandos escritos en JScript, VBScript o Python 3.5. Al implementar el plan de protección, el software ejecuta el comando en todos los equipos. El resultado del script para cada equipo debería ser una ruta de carpeta local o de red. Si una carpeta no existe, se creará (limitación: los comandos escritos en Python no pueden crear carpetas en redes compartidas). En la pestaña **Almacenamiento de la copia de seguridad**, cada carpeta aparece como una ubicación de copia de seguridad independiente.

En **Tipo de secuencia de comandos**, seleccione el tipo de script (**JScript**, **VBScript** o **Python**), e importe el script, o cópielo y péguelo. Con carpetas de red, especifique las credenciales de acceso con permiso de lectura y escritura.

Ejemplos:

- El siguiente comando JScript devuelve la ubicación de la copia de seguridad para un equipo con el formato `\\bkpsrv\<machine name>`:

```
WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
```


© Acronis International GmbH, 2003-2025

De ese modo, las copias de seguridad de cada equipo se guardarán en una carpeta con el mismo nombre en el servidor **bkpsrv**.

- El siguiente comando JScript da salida a la ubicación de la copia de seguridad en una carpeta del equipo en el que se ejecuta dicho comando:

```
WScript.Echo("C:\\Backup");
```

Como resultado, las copias de seguridad de este equipo se guardarán en la carpeta `C:\Backup` del mismo equipo.

Nota
La ruta de la ubicación de estos comandos distingue entre mayúsculas y minúsculas. Por lo tanto, `C:\Backup` y `C:\backup` se muestran como distintas ubicaciones en la consola de Cyber Protect. Use mayúsculas para la letra de unidad.

Acerca de Secure Zone

Secure Zone es una partición segura que está en un disco del equipo incluido en la copia de seguridad. La partición puede almacenar copias de seguridad de discos o archivos de este equipo.

Si el disco presenta un error físico, las copias de seguridad almacenadas en Secure Zone podrían perderse. Esa es la razón por la que Secure Zone no debe ser la única ubicación donde se almacene una copia de seguridad. En entornos empresariales, se puede pensar en Secure Zone como una ubicación intermedia utilizada para realizar copias de seguridad cuando una ubicación normal no está disponible temporalmente o se conecta a partir de un canal lento u ocupado.

¿Por qué se debe usar Secure Zone?

Secure Zone:

- Permite la recuperación de un disco en el mismo disco en donde reside la copia de seguridad del disco.
- Constituye un método rentable y práctico para la protección de datos ante un funcionamiento defectuoso del software, ataques de virus o errores humanos.
- Elimina la necesidad de medios o conexiones de red diferentes para realizar copias de seguridad o recuperar los datos. Esto es muy útil para los usuarios itinerantes.
- Puede funcionar como destino primario cuando se usa la replicación de copias de seguridad.

Limitaciones

- Secure Zone no se puede organizar en un Mac.
- Secure Zone es una partición en un disco básico. No puede organizarse en un disco dinámico ni crearse como volumen lógico (administrado por LVM).
- Secure Zone tiene el formato de sistema de archivos FAT32. Como FAT32 tiene un límite de tamaño de archivos de 4 GB, las copias de seguridad de mayor tamaño se dividen al guardarse en Secure Zone. Esto no afecta al procedimiento de recuperación ni a la velocidad.

© Acronis International GmbH, 2003-2025

Cómo la creación de Secure Zone transforma el disco

- Secure Zone siempre se crea al final del disco rígido.
- Si no hay espacio sin asignar suficiente o no hay al final del disco, pero sí hay espacio sin asignar entre volúmenes, estos últimos se moverán para agregar más espacio sin asignar al final del disco.
- Cuando se recopile todo el espacio sin asignar y el mismo siga siendo insuficiente, el software sacará espacio libre de los volúmenes que seleccione, de forma proporcional, reduciendo el tamaño de los volúmenes.
- Sin embargo, debería haber espacio libre en un volumen para que el sistema operativo y las aplicaciones puedan funcionar; por ejemplo, para crear archivos temporales. El software no reducirá un volumen en el que el espacio libre ocupe el 25 % o menos del tamaño total del volumen. El software continuará reduciendo los volúmenes de forma proporcional únicamente cuando todos los volúmenes del disco tengan el 25 % o menos espacio libre.

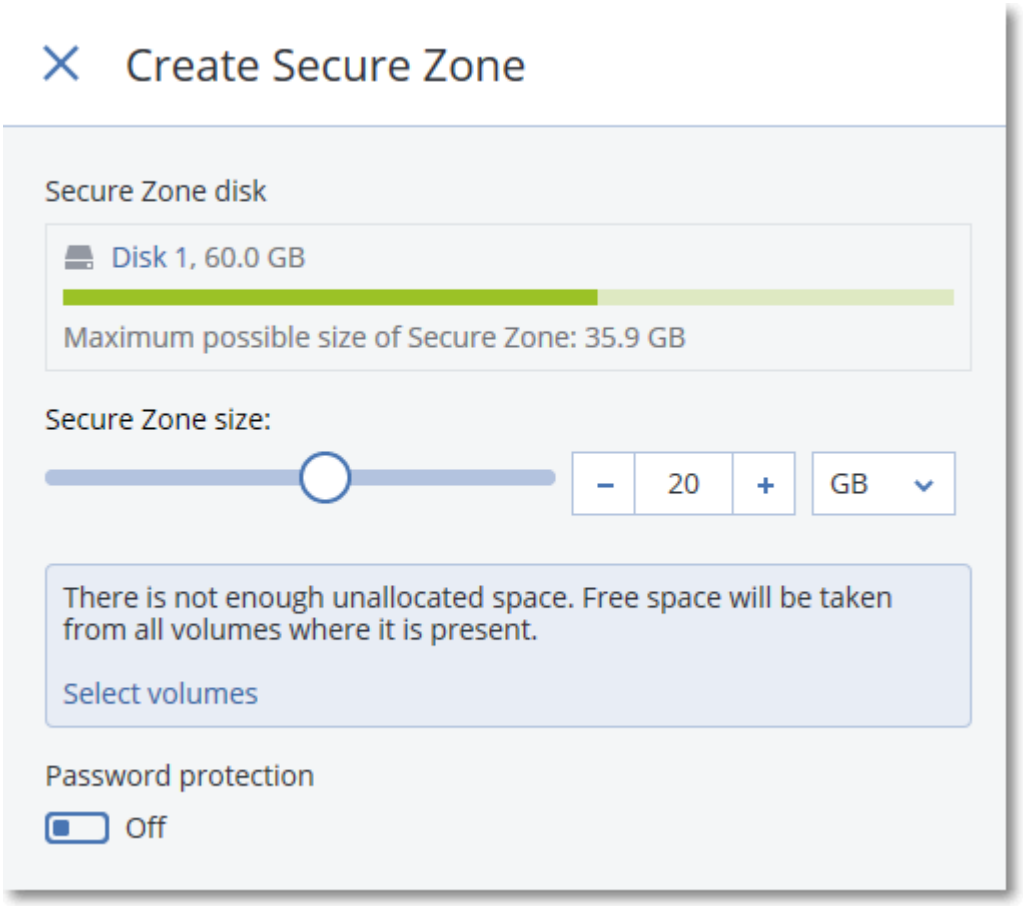
Como se deduce de esto, no es recomendable especificar el tamaño máximo posible para Secure Zone. Acabará sin espacio libre en ningún volumen, lo que puede hacer que el sistema operativo o las aplicaciones funcionen de forma inestable e incluso que no puedan iniciarse.

Importante
Para mover o cambiar el tamaño del volumen desde el que se arranca el sistema actualmente, es necesario reiniciar.

Cómo crear Secure Zone

1. Seleccione el equipo en el que desea crear Secure Zone.
2. Haga clic en **Detalles** > **Crear Secure Zone**.
3. En el **disco Secure Zone**, haga clic en **Seleccionar** y, a continuación, elija el disco rígido (si hay más de uno) en el que desea crear la zona.
   El software calcula el tamaño máximo posible de Secure Zone.
4. Introduzca el tamaño de Secure Zone o arrastre el deslizador para seleccionar cualquier tamaño entre los mínimos y los máximos.
   El tamaño mínimo es de aproximadamente 50 MB, de acuerdo con la geometría del disco duro.
   El tamaño máximo es igual al espacio sin asignar del disco más el espacio libre total de todos los volúmenes del disco.
5. Si el espacio sin asignar no es suficiente para el tamaño que ha indicado, el software obtendrá el espacio libre de los volúmenes existentes. De manera predeterminada, se seleccionan todos los volúmenes. Si desea excluir algunos volúmenes, haga clic en **Seleccionar volúmenes**. De lo contrario, omita este paso.

© Acronis International GmbH, 2003-2025



6. [Opcional] Habilite el conmutador **Protección por contraseña** y especifique una contraseña.
   La contraseña es obligatoria para acceder a las copias de seguridad ubicadas en Secure Zone. No se necesita contraseña para realizar una copia de seguridad en Secure Zone, salvo que dicha copia de seguridad se haga en un soporte de arranque.
7. Haga clic en **Crear**.
   El software muestra la distribución esperada de la partición. Haga clic en **Aceptar**.
8. Espere mientras el software crea Secure Zone.

Ahora puede escoger Secure Zone en **Dónde guardar las copias de seguridad** al crear un plan de protección.

Cómo eliminar Secure Zone

1. Seleccione un equipo con Secure Zone.
2. Haga clic en **Detalles**.
3. Haga clic en el ícono de engranaje situado junto a **Secure Zone** y después haga clic en **Eliminar**.
4. [Opcional] Seleccione los volúmenes a los que desea agregar el espacio liberado de la zona. De manera predeterminada, se seleccionan todos los volúmenes.
   El espacio se distribuirá a partes iguales entre los volúmenes seleccionados. Si no selecciona ningún volumen, el espacio liberado se convertirá en espacio sin asignar.

© Acronis International GmbH, 2003-2025

Para cambiar el tamaño del volumen desde el que se arranca el sistema, es necesario reiniciar.

5. Haga clic en **Eliminar**.

Como resultado, se eliminan Secure Zone y todas las copias de seguridad almacenadas en ella.

Protección continua de datos (CDP)

La protección continua de datos (CDP) es parte del paquete de Advanced Backup. Crea copias de seguridad de datos esenciales justo después de que se modifiquen, lo que garantiza que no se perderán cambios si se produce un error en su sistema entre dos copias de seguridad planificadas. Puede configurar la Protección continua de datos para los siguientes datos:

- Archivos y carpetas en ubicaciones específicas
- Archivos modificados por aplicaciones específicas

La Protección continua de datos solo es compatible con el sistema de archivos NTFS y los siguientes sistemas operativos:

- Escritorio: Windows 7 y posterior
- Servidor: Windows Server 2008 R2 y posterior

Solo son compatibles las carpetas locales. No pueden seleccionarse carpetas de red para la Protección continua de datos.

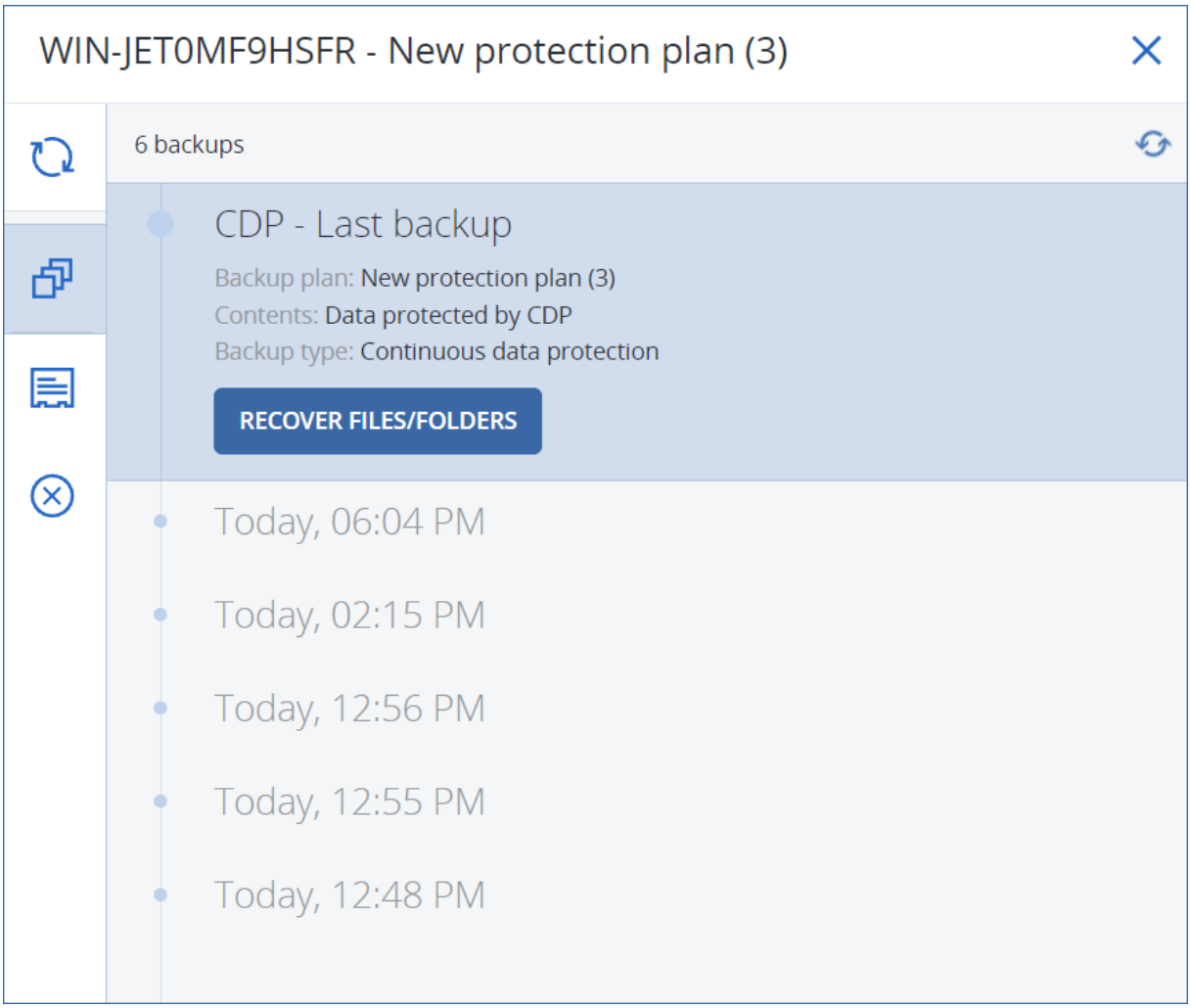
La Protección continua de datos no es compatible con la opción **Copia de seguridad de aplicación**.

Nota
La protección continua de datos (CDP) evita la eliminación de archivos de copia de seguridad. Si desea eliminar manualmente una copia de seguridad que se crea con la CDP habilitada, debe revocar o eliminar el plan de protección correspondiente.

Cómo funciona

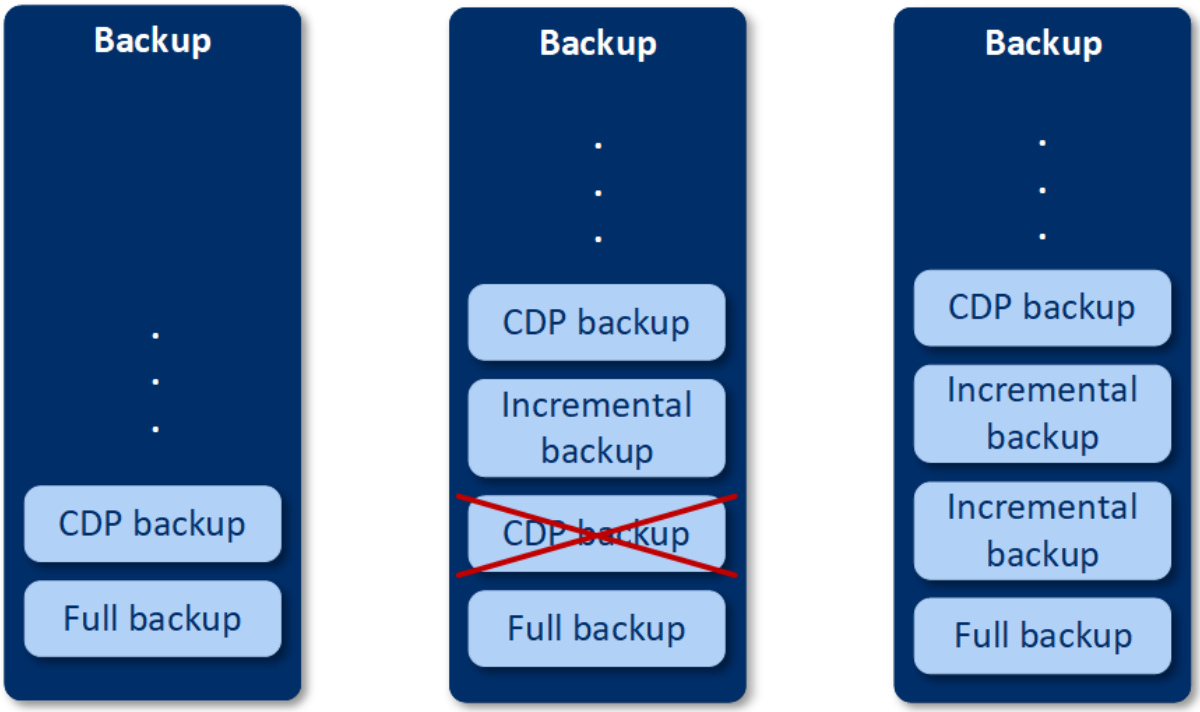
Los cambios en los archivos y carpetas para los que se realiza un seguimiento mediante la Protección continua de datos se guardan inmediatamente en una carpeta especial de CDP. Solo hay una copia de seguridad de CDP en un conjunto de copias de seguridad, y siempre es la más reciente.

© Acronis International GmbH, 2003-2025



Cuando se inicia una copia de seguridad regular planificada, la Protección continua de datos se pausa porque los últimos datos no se incluyen en la copia de seguridad planificada. Cuando finaliza la copia de seguridad planificada, se reanuda la Protección continua de datos, se elimina la antigua copia de seguridad de CDP y se crea una nueva. Por tanto, la copia de seguridad de CDP siempre es la más reciente en el conjunto de copias de seguridad y solo almacena el último estado de las carpetas y archivos para los que se realiza un seguimiento.

© Acronis International GmbH, 2003-2025



Si su equipo se bloquea durante una copia de seguridad regular, la Protección continua de datos se reanudará automáticamente después de que el equipo se reinicie y creará una copia de seguridad de CDP sobre la última copia de seguridad planificada realizada correctamente.

La Protección continua de datos requiere que se cree al menos una copia de seguridad regular antes de la copia de seguridad de CDP. Ese es el motivo por el que, cuando ejecuta un plan de protección con la Protección continua de datos por primera vez, se crea una copia de seguridad completa y la copia de seguridad de CDP se añade inmediatamente sobre ella. Si habilita la opción de **Protección continua de datos** para un plan de protección existente, la copia de seguridad de CDP se añade al conjunto de copias de seguridad existente.

Nota
La protección continua de datos está habilitada de forma predeterminada para los planes de protección que creó desde la pestaña **Dispositivos** si tiene habilitada la funcionalidad de Advanced Backup y no utiliza otras funciones de Advanced Backup para los equipos seleccionados. Si ya tiene un plan con protección continua de datos para un equipo seleccionado, no se habilitará la protección continua de datos de forma predeterminada para ese equipo en los planes recién creados.
La protección continua de datos no está habilitada de forma predeterminada para los planes creados para grupos de dispositivos.

Fuentes de datos compatibles

Puede configurar la Protección continua de datos para las siguientes fuentes de datos:

© Acronis International GmbH, 2003-2025

- Todo el equipo
- Discos/volúmenes
- Archivos/carpetas

Después de seleccionar la fuente de datos en la sección **Qué incorporar en la copia de seguridad** del plan de protección, en la sección **Elementos que proteger de forma continua** seleccione los archivos, carpetas o aplicaciones para la Protección continua de datos. Para obtener más información sobre cómo configurar la Protección continua de datos, consulte "Configuración de una copia de seguridad de CDP" (p. 555).

Destinos compatibles

Puede configurar la Protección continua de datos con los siguientes destinos:

- Carpeta local
- Carpeta de red
- Almacenamiento en la nube
- Acronis Cyber Infrastructure
- Ubicación definida por secuencia de comandos

Nota
Puede definir por una secuencia de comandos solo las ubicaciones indicadas arriba.

Configuración de una copia de seguridad de CDP

Puede configurar la Protección continua de datos del módulo **Copia de seguridad** de un plan de protección. Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 250).

Configuración de la protección continua de datos

1. En el módulo **Copia de seguridad** de un plan de protección, active el control deslizante **Protección continua de datos (CDP)**.
   Este control deslizante solo está disponible para los siguientes orígenes de datos:
   - Todo el equipo
   - Discos/volúmenes
   - Archivos/carpetas
2. En **Elementos que proteger de forma continua**, configure la protección continua de datos para **Aplicaciones** o **Archivos/carpetas**, o ambos.
   - Haga clic en **Aplicaciones** para configurar la copia de seguridad de CDP para archivos modificados por aplicaciones específicas.
     Puede seleccionar las aplicaciones de las categorías predefinidas y añadir otras especificando la ruta que lleva al archivo ejecutable de la aplicación, por ejemplo:

© Acronis International GmbH, 2003-2025

- `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
- `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

- Haga clic en **Archivos/carpetas** para configurar la copia de seguridad de CDP para archivos en ubicaciones específicas.

  Puede definir las ubicaciones mediante reglas de selección, o puede seleccionar directamente los archivos y carpetas.
  - [Para todos los equipos] Para crear una regla de selección, use el cuadro de texto.

    Puede utilizar las rutas completas a los archivos o las rutas mediante los caracteres comodín (* y ?). El asterisco coincide con cero o más caracteres. El signo de interrogación sustituye a un solo carácter.

    Importante
    Para crear una copia de seguridad de CDP de una carpeta, debe especificar su contenido mediante el carácter comodín asterisco:

    Ruta correcta: `D:\Data\*`

    Ruta incorrecta: `D:\Data\`
  - [Para equipos en línea] Para seleccionar archivos y carpetas directamente:
    - En **Equipo desde el cual examinar**, seleccione el equipo en el que residan los archivos o carpetas.
    - Haga clic en **Seleccionar archivos y carpetas** para examinar el equipo seleccionado.

      Su selección directa crea una regla de selección. Si aplica el plan de protección a múltiples equipos y una regla de selección no es válida para un equipo, se omitirá en él.

3. En el panel del plan de protección, haga clic en **Crear**.

Como resultado, se creará una copia de seguridad de los datos que especificó de forma continua entre las copias de seguridad planificadas.

Programación de copia de seguridad

Para configurar una copia de seguridad automáticamente en un momento específico, en intervalos específicos o en un evento específico.

Las copias de seguridad planificadas para recursos que no son de nube a nube se ejecutan según la configuración de la zona horaria de la carga de trabajo en la que está instalado el agente de protección. Por ejemplo, si aplica el mismo plan de protección a cargas de trabajo con diferente configuración de zonas horarias, las copias de seguridad se iniciarán según la zona horaria local de cada carga de trabajo.

Planificar una copia de seguridad incluye las siguientes acciones:

- Selección de un esquema de copia de seguridad
- Configuración de la hora o selección del evento que activa la copia de seguridad
- Configuración de los ajustes opcionales y las condiciones de inicio

© Acronis International GmbH, 2003-2025

Esquemas de copia de seguridad

Un esquema de copias de seguridad es parte de la planificación del plan de protección que define qué tipo de copia de seguridad (completa, diferencial o incremental) se crea y cuándo. Puede seleccionar uno de los esquemas de copias de seguridad predefinidos o crear un esquema personalizado.

Los esquemas y los tipos de copias de seguridad disponibles dependen de la ubicación y el origen de la copia de seguridad. Por ejemplo, una copia de seguridad diferencial no está disponible cuando realiza una copia de seguridad de datos SQL, de datos de Exchange o del estado del sistema.

Esquema de copias de seguridad	Descripción	Elementos configurables
Siempre incremental (un archivo)	La primera copia de seguridad está llena y podría requerir mucho tiempo. Las copias posteriores son incrementales y mucho más rápidas. Las copias de seguridad usan el formato de copia de seguridad de archivo único[1]*. De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes. Le recomendamos que utilice este esquema cuando almacene sus copias de seguridad en el almacenamiento de la nube porque las copias de seguridad incrementales son rápidas y conllevan menos tráfico de red.	• Tipo de planificación: mensual, semanal, diaria u horaria • Iniciador de copia de seguridad: evento u hora • Hora de inicio • Condiciones de inicio • Otras opciones
Siempre completa	Todas las copias de seguridad del conjunto de copias de seguridad son completas. De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes.	• Tipo de planificación: mensual, semanal, diaria u horaria • Iniciador de copia de seguridad: evento u hora • Hora de inicio • Condiciones de inicio • Otras opciones
Completa semanal,	Se crea una copia de seguridad completa una vez a	• Iniciador de copia de

[1]Es un formato de copia de seguridad en el que las copias de seguridad iniciales completas e incrementales subsiguientes se guardan en un único archivo .tibx. Este formato aprovecha la velocidad del método de copia de seguridad incremental, al mismo tiempo que se evita la desventaja principal: la eliminación compleja de copias de seguridad desactualizadas. El software marca los bloques que usan las copias de seguridad desactualizadas como "libres" y escribe nuevas copias de seguridad en esos bloques. Con este formato, la limpieza es extremadamente rápida, y el consumo de recursos es mínimo. El formato de copia de seguridad de archivo único no está disponible cuando se realiza la copia en ubicaciones que no son compatibles con los accesos de lectura y escritura aleatorios.

© Acronis International GmbH, 2003-2025

Esquema de copias de seguridad	Descripción	Elementos configurables
incremental diaria	la semana y el resto de copias de seguridad son incrementales. La primera copia de seguridad es completa y el resto de copias de seguridad de la semana son incrementales. A continuación, el ciclo se repite. Para seleccionar el día de creación de la copia de seguridad completa semanal, en el plan de protección, haga clic en el ícono de engranaje y vaya a **Opciones de copia de seguridad** > **Copia de seguridad semanal**. De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes.	seguridad: evento u hora • Hora de inicio • Condiciones de inicio • Otras opciones
Completa mensual, diferencial semanal, incremental diaria (GFS)	De forma predeterminada, las copias de seguridad incrementales se realizan a diario, de lunes a viernes. Las copias de seguridad diferenciales se realizan los sábados. Las copias de seguridad completas se realizan el primer día de cada mes. **Nota** Este es un esquema personalizado predefinido. En el plan de protección, se muestra como **Personalizado**.	• Cambie el esquema existente por tipo de copia de seguridad: ◦ Tipo de planificación: mensual, semanal, diaria u horaria ◦ Iniciador de copia de seguridad: evento u hora ◦ Hora de inicio ◦ Condiciones de inicio ◦ Otras opciones • Añada nuevos esquemas por tipo de copia de seguridad
Personalizado	Debe seleccionar los tipos de copia de seguridad (completa, diferencial e incremental) y configurar un esquema independiente para cada uno de ellos*.	• Cambie el esquema existente por tipo de copia de seguridad: ◦ Tipo de planificación: mensual, semanal, diaria u horaria ◦ Iniciador de copia de seguridad: evento u hora ◦ Hora de inicio ◦ Condiciones de

© Acronis International GmbH, 2003-2025

Esquema de copias de seguridad	Descripción	Elementos configurables
		inicio ◦ Otras opciones • Añada nuevos esquemas por tipo de copia de seguridad

* Después de crear un plan de protección, no puede cambiar entre **Siempre incremental (un archivo)** y el resto de esquemas de copia de seguridad, y viceversa. **Siempre incremental (un archivo)** es un esquema de formato de archivo único, y los demás esquemas son de archivos múltiples. Si quiere cambiar de formato, cree un nuevo plan de protección.

Tipos de copia de seguridad

Los tipos de copia de seguridad disponibles son los siguientes:

- Completa: una copia de seguridad completa contiene todos los datos de origen. Esta copia de seguridad es autosuficiente. No necesita acceso a ninguna otra copia de seguridad para recuperar los datos.

  Nota
  La primera copia de seguridad creada por un plan de protección siempre es completa.

- Incremental: una copia de seguridad incremental almacena todos los cambios desde la última copia de seguridad, independientemente de es completa, diferencial o incremental. Para recuperar los datos, necesita que la cadena completa de copias de seguridad de la que depende la copia de seguridad incremental vuelva a la copia de seguridad completa inicial.
- Diferencial: una copia de seguridad diferencial almacena todos los cambios desde la última copia de seguridad completa. Para recuperar los datos, necesita tanto la copia de seguridad diferencial como la copia de seguridad completa correspondiente de la que depende la copia de seguridad diferencial.

Ejecutar una copia de seguridad en una planificación

Para ejecutar una copia de seguridad automáticamente en un momento o evento específico, habilite una planificación en el plan de protección.

Pasos para habilitar una planificación

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. Haga clic en **Planificación**.
3. Habilite el conmutador de planificación.
4. Seleccione el esquema de copias de seguridad.

© Acronis International GmbH, 2003-2025

5. Configure la planificación según sea necesario y haga clic en **Listo**.
   Para obtener más información sobre las opciones planificadas disponibles, consulte "Planificar por hora" (p. 560) y "Planificación por eventos" (p. 562).
6. [Opcional] Configure las condiciones de inicio o las opciones de planificación adicionales.
7. Guarde el plan de protección.

Como resultado, se inicia una operación de copia de seguridad cada vez que se cumplen las condiciones de planificación.

Pasos para deshabilitar una planificación

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. Haga clic en **Planificación**.
3. Deshabilite el conmutador de planificación.
4. Guarde el plan de protección.

Como resultado, la copia de seguridad se ejecuta sola si la inicia manualmente.

Nota
Si la planificación está deshabilitada, no se aplican las reglas de retención automáticamente. Para aplicarlas, ejecute la copia de seguridad manualmente.

Planificar por hora

La tabla siguiente resume las opciones de planificación según el tiempo. La disponibilidad de estas opciones depende del esquema de copias de seguridad. Para obtener más información, consulte "Esquemas de copia de seguridad" (p. 557).

Opción	Descripción	Ejemplos
Mensualmente	Seleccione los meses, los días del mes o los días de la semana y luego la hora de inicio de la copia de seguridad.	Ejecutar una copia de seguridad el 1 de enero y el 3 de febrero a las 00:00. Ejecutar una copia de seguridad el primer día de cada mes a las 10:00. Ejecutar una copia de seguridad el 1 de marzo, el 5 de abril, el 1 de abril y el 5 de abril a las 09:00. Ejecutar una copia de seguridad el segundo y el tercer viernes de cada mes a las 11:00. Ejecutar una copia de seguridad el último miércoles de cada mes a las 22:30.
Semanalmente	Seleccione los días de la semana y luego la	Ejecutar una copia de seguridad de lunes

© Acronis International GmbH, 2003-2025

Opción	Descripción	Ejemplos
	hora de inicio de la copia de seguridad.	a viernes, a las 10:00. Ejecutar una copia de seguridad los lunes a las 23:00. Ejecutar una copia de seguridad los martes y los sábados a las 08:00.
Diariamente	Seleccione los días (todos los días o solo los fines de semana) y luego la hora de inicio de la copia de seguridad.	Ejecutar una copia de seguridad todos los días a las 11:45. Ejecutar una copia de seguridad de lunes a viernes, a las 21:30.
Cada hora	Seleccione los días de la semana, un intervalo de tiempo entre dos copias de seguridad consecutivas y el intervalo de tiempo en el que se ejecutan las copias de seguridad. Si configura el intervalo en minutos, puede seleccionar un intervalo sugerido entre 10 y 60 minutos o especificar uno personalizado, por ejemplo, 45 o 75 minutos.	Ejecutar una copia de seguridad cada hora entre las 08:00 y las 18:00 de lunes a viernes. Ejecutar una copia de seguridad cada tres horas entre la 01:00 y las 18:00 los sábados y los domingos.

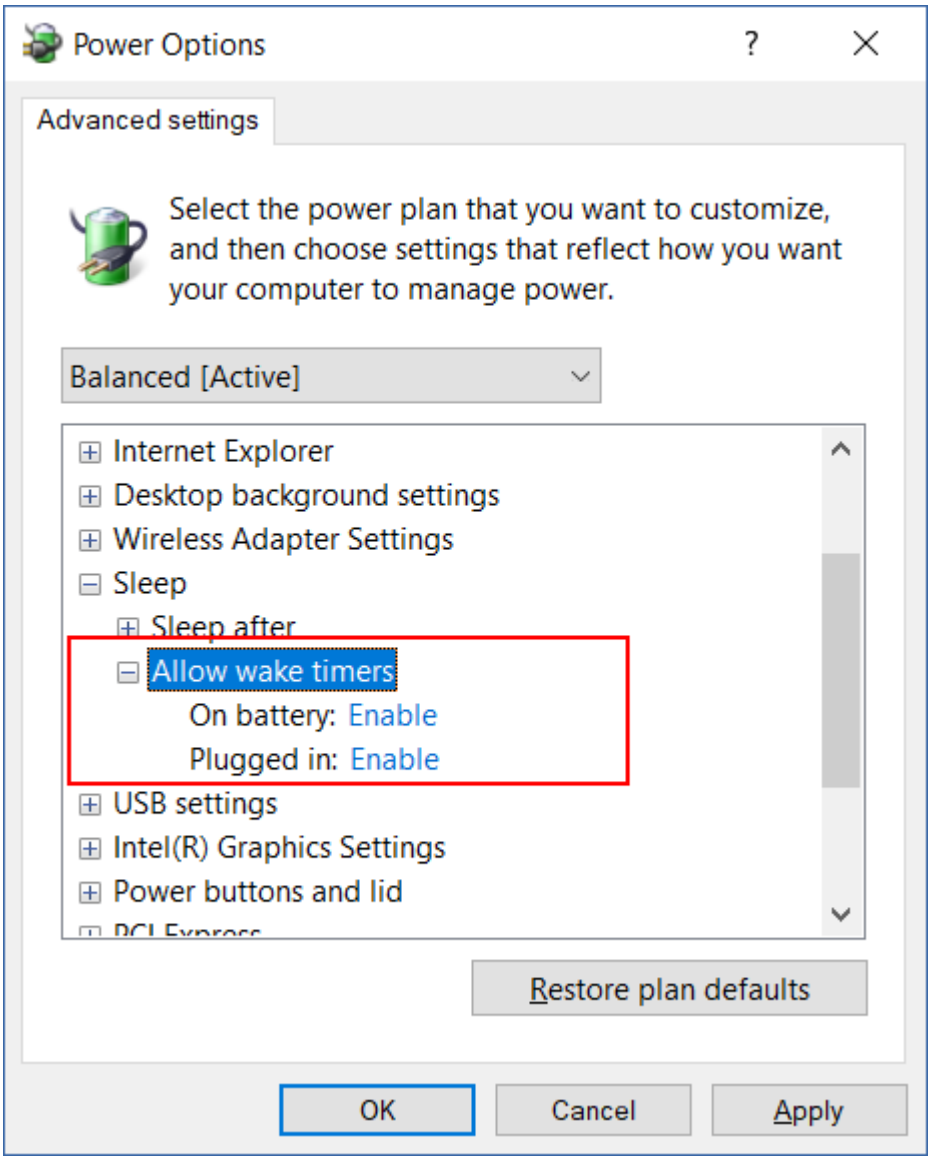
Otras opciones

Cuando planifica una copia de seguridad por hora, están disponibles las siguientes opciones de planificación adicionales.

Para acceder a ellas, en el panel **Planificación**, haga clic en **Mostrar más**.

- **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo**
  Configuración predeterminada: Deshabilitado.
- **Evitar el modo de suspensión o hibernación durante una copia de seguridad**
  Esta opción solo se aplica a los equipos que ejecutan Windows.
  Configuración predeterminada: Habilitado.
- **Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada**
  Esta opción solo se aplica a los equipos que ejecutan Windows, en los planes de energía que tienen la opción **Permitir temporizadores de reactivación** habilitada.

© Acronis International GmbH, 2003-2025



Esta opción no utiliza la funcionalidad Wake-On-LAN y no se aplica a los equipos apagados.

Configuración predeterminada: Deshabilitado.

Planificación por eventos

Para configurar una copia de seguridad que se ejecuta en un evento específico, seleccione una de las siguientes opciones:

Opción	Descripción	Ejemplos
En el momento en que se realizó la última copia de seguridad	Una copia de seguridad se inicia tras un periodo especificado después de la última copia de seguridad que se haya realizado correctamente.	Ejecute una copia de seguridad un día después de la última copia de seguridad que se haya realizado correctamente. Ejecute una copia de seguridad cuatro horas después de la última copia de seguridad que se haya realizado

© Acronis International GmbH, 2003-2025

Opción	Descripción	Ejemplos
	Nota Esta opción depende de cómo se completó la anterior copia de seguridad. Si una copia de seguridad falla, la siguiente se iniciará automáticamente. En este caso, debe ejecutar la copia de seguridad manualmente y garantizar que se completa correctamente para restablecer la planificación.	correctamente.
Cuando un usuario inicia sesión en el sistema	Una copia de seguridad se inicia cuando un usuario inicia sesión en el equipo. Puede configurar esta opción para cualquier inicio de sesión o para un inicio de sesión de un usuario específico. **Nota** Al iniciar sesión con un perfil de usuario temporal no se iniciará una copia de seguridad.	Ejecutar una copia de seguridad cuando el usuario John Doe inicie sesión.
Cuando un usuario cierra sesión en el sistema	Una copia de seguridad se inicia cuando un usuario cierra sesión en el equipo. Puede configurar esta opción para cualquier cierre de sesión o para un cierre de sesión de un usuario específico. **Nota** Al cerrar sesión en un perfil de usuario temporal no se iniciará una copia de seguridad. Al apagar un equipo no se iniciará una copia de seguridad.	Ejecutar una copia de seguridad cuando todos los usuarios cierren sesión.
Al iniciarse el sistema	Una copia de seguridad se ejecuta cuando se inicia el equipo protegido.	Ejecutar una copia de seguridad cuando un usuario inicia el equipo.
Al apagarse el sistema	Una copia de seguridad se ejecuta cuando se apaga el equipo protegido.	Ejecutar una copia de seguridad cuando un usuario apaga el equipo.
Al ocurrir un evento en el registro de eventos de Windows	Una copia de seguridad se ejecuta cuando ocurre un evento de Windows que especifica.	Ejecutar una copia de seguridad cuando el evento 7 del tipo error y el disco de origen se registran en el registro del sistema de Windows.

© Acronis International GmbH, 2003-2025

La disponibilidad de estas opciones depende del origen de la copia de seguridad y del sistema operativo de las cargas de trabajo protegidas. La siguiente tabla resume las opciones disponibles para Windows, Linux y macOS.

Evento	Origen de la copia de seguridad (Qué incorporar en la copia de seguridad)					
	Todo el equipo, Discos/volúmenes o Archivos/carpetas (equipos físicos)	**Todo el equipo o Discos/volúmenes (equipos virtuales)**	**Configuración de ESXi**	**Buzones de correo de Microsoft 365**	**Bases de datos y buzones de Exchange**	**Bases de datos SQL**
En el momento en que se realizó la última copia de seguridad	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Cuando un usuario inicia sesión en el sistema	Windows	N/D	N/D	N/D	N/D	N/D
Cuando un usuario cierra sesión en el sistema	Windows	N/D	N/D	N/D	N/D	N/D
Al iniciarse el sistema	Windows, Linux, macOS	N/D	N/D	N/D	N/D	N/D
Al apagarse el sistema	Windows	N/D	N/D	N/D	N/D	N/D

© Acronis International GmbH, 2003-2025

Evento	Origen de la copia de seguridad (Qué incorporar en la copia de seguridad)					
	Todo el equipo, Discos/volúmenes o Archivos/carpetas (equipos físicos)	**Todo el equipo o Discos/volúmenes (equipos virtuales)**	**Configuración de ESXi**	**Buzones de correo de Microsoft 365**	**Bases de datos y buzones de Exchange**	**Bases de datos SQL**
Al ocurrir un evento en el registro de eventos de Windows	Windows	N/D	N/D	Windows	Windows	Windows

Al ocurrir un evento en el registro de eventos de Windows

Puede ejecutar automáticamente una copia de seguridad cuando un evento específico se registre en un registro de eventos de Windows, como el registro de aplicaciones, el de seguridad y el del sistema.

Nota
Puede explorar los eventos y ver sus propiedades en **Administración del ordenador** > **Visor de sucesos** en Windows. Para abrir el Registro de seguridad, necesita derechos de administrador.

Parámetros del evento

La siguiente tabla resume los parámetros que debe especificar a la hora de configurar la opción **Al ocurrir un evento en el registro de eventos de Windows**.

Parámetro	Descripción
Nombre del registro	El nombre del registro. Seleccione el nombre de un registro estándar (Aplicación, Seguridad o Sistema) o especifique otro nombre de registro. Por ejemplo, Sesiones de Microsoft Office.
Origen del evento	El origen del evento indica qué programa o componente del sistema generó el suceso. Por ejemplo, disco. Todos los orígenes de eventos que incluyan la cadena de texto especificada activarán la copia de seguridad planificada. Esta opción no distingue mayúsculas de minúsculas. Por ejemplo, si especifica `service`,

© Acronis International GmbH, 2003-2025

Parámetro	Descripción
	los orígenes de evento Administrador de control del servicio y Tiempo-servicio activarán una copia de seguridad.
Tipo de evento	Tipo de evento: Error, Advertencia, Información, Auditoría correcta o Error en auditoría.
ID del evento	El ID de evento identifica un tipo de evento específico dentro de un origen del evento. Por ejemplo, un evento Error con Origen del evento disco e ID del evento 7 ocurre cuando Windows detecta un bloque dañado en un disco, mientras que un evento Error con Origen del evento disco e ID del evento 15 ocurre cuando no se puede obtener acceso a un disco porque no está preparado.

Ejemplo: Copia de seguridad de emergencia en case de bloques dañados en el disco duro

Uno o más bloques dañados en un disco duro podrían indicar un error inminente. Por ello, es posible que quiera crear una copia de seguridad cuando se detecte un bloque dañado.

Cuando Windows detecta un bloque dañado en el disco, registra un suceso en el disco de origen del evento y el número de suceso 7 en el registro del sistema. En el plan de protección, configure la siguiente planificación:

- Programación: Al ocurrir un evento en el registro de eventos de Windows
- Nombre del registro: Sistema
- Origen del evento: Disco
- Tipo de suceso: Error
- Id. suceso: 7

Importante
Para garantizar que la copia de seguridad se completa a pesar de los bloques dañados, en **Opciones de copia de seguridad**, vaya a **Control de errores** y marque la casilla de verificación **Ignorar los sectores defectuosos**.

Condiciones de inicio

Para ejecutar una copia de seguridad solo si se cumplen las condiciones específicas, configure una o más condiciones de inicio. Si configura varias condiciones, deben cumplirse todas simultáneamente para que se inicie la copia de seguridad. Puede especificar un periodo después del que se ejecutarán las copias de seguridad, independientemente de si se cumplen las condiciones. Para obtener más información sobre esta opción de copia de seguridad, consulte "Condiciones de inicio de la tarea" (p. 647).

Las condiciones de inicio no son aplicables cuando inicia una copia de seguridad manualmente.

© Acronis International GmbH, 2003-2025

En la siguiente tabla se muestran las condiciones de inicio disponibles para diversos datos en Windows, Linux y macOS.

Condición de inicio	Origen de la copia de seguridad (Qué incorporar en la copia de seguridad)					
	Todo el equipo, Discos/volúmenes o Archivos/carpetas (equipos físicos)	**Todo el equipo o Discos/volúmenes (equipos virtuales)**	**Configuración de ESXi**	**Buzones de correo de Microsoft 365**	**Bases de datos y buzones de Exchange**	**Bases de datos SQL**
El usuario está inactivo	Windows	N/D	N/D	N/D	N/D	N/D
El servidor de la ubicación de copia de seguridad está disponible	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Los usuarios cerraron la sesión	Windows	N/D	N/D	N/D	N/D	N/D
Se adapta al intervalo de tiempo	Windows, Linux, macOS	Windows, Linux	N/D	N/D	N/D	N/D
Ahorrar batería	Windows	N/D	N/D	N/D	N/D	N/D
No iniciar con conexiones de uso medido	Windows	N/D	N/D	N/D	N/D	N/D
No iniciar con conexiones a las siguientes redes Wi-Fi	Windows	N/D	N/D	N/D	N/D	N/D

© Acronis International GmbH, 2003-2025

Condición de inicio	Origen de la copia de seguridad (Qué incorporar en la copia de seguridad)					
	Todo el equipo, Discos/volúmenes o Archivos/carpetas (equipos físicos)	Todo el equipo o Discos/volúmenes (equipos virtuales)	Configuración de ESXi	Buzones de correo de Microsoft 365	Bases de datos y buzones de Exchange	Bases de datos SQL
Comprobar dirección IP del dispositivo	Windows	N/D	N/D	N/D	N/D	N/D

El usuario está inactivo

"El usuario está inactivo" significa que se está ejecutando el protector de pantalla en el equipo o que el equipo está bloqueado.

Ejemplo

Ejecutar una copia de seguridad todos los días a las 21:00, preferiblemente cuando el usuario esté inactivo. Si el usuario sigue activo a las 23:00, ejecutar la copia de seguridad de todos modos.

- Programación: **Cada día**, **Ejecutar cada día**. Iniciar a las: **21:00**.
- Condición: **El usuario está inactivo**.
- Condiciones de inicio de la copia de seguridad: **Esperar hasta que se cumplan las condiciones**, **Iniciar la tarea de todos modos después de 2** horas.

Como resultado:

- Si el usuario queda inactivo antes de las 21:00, la copia de seguridad se inicia a las 21:00.
- Si el usuario queda inactivo entre las 21:00 y las 23:00, la copia de seguridad se inicia inmediatamente.
- Si el usuario sigue activo a las 23:00, la copia de seguridad se inicia a las 23:00.

El servidor de la ubicación de copia de seguridad está disponible

"El servidor de ubicación de copia de seguridad está disponible" significa que el equipo que alberga la ubicación de las copias de seguridad está disponible a través de la red.

Esta condición se aplica a las carpetas de red, al almacenamiento en la nube y a las ubicaciones gestionadas por un nodo de almacenamiento.

Esta condición no cubre la disponibilidad de la ubicación en sí misma, solo la disponibilidad del servidor. Por ejemplo, si el servidor está disponible, pero la carpeta de red en este servidor no está

© Acronis International GmbH, 2003-2025

compartida o las credenciales de la carpeta ya no son válidas, se sigue considerando que se cumple la condición.

Ejemplo

Realice copias de seguridad en una carpeta de red cada día hábil a las 21:00. Si el equipo donde se encuentra la carpeta no estuviera disponible en ese momento (por ejemplo, debido a mantenimiento), la copia de seguridad se omite y se espera al siguiente día hábil para iniciar la tarea planificada.

- Programación: **Cada día**, **Ejecutar de lunes a viernes**. Iniciar a las: **21:00**.
- Condición: **El servidor de la ubicación de copia de seguridad está disponible**.
- Condiciones de inicio de la copia de seguridad: **Omita la copia de seguridad planificada**.

Como resultado:

- Si el host está disponible a las 21:00, la copia de seguridad se inicia inmediatamente.
- Si el host no está disponible a las 21:00, la copia de seguridad se iniciará el siguiente día hábil (si el host está disponible a las 21:00 ese día).
- Si es imposible que el host esté disponible en días hábiles a las 21:00, la copia de seguridad nunca se iniciará.

Los usuarios cerraron la sesión

Utilice esta condición de inicio para posponer una copia de seguridad hasta que todos los usuarios cierren sesión en un equipo Windows.

Ejemplo

Ejecute la copia de seguridad a las 20:00 cada viernes, preferentemente cuando todos los usuarios hayan cerrado la sesión. Si alguno de los usuarios todavía no hubiera cerrado la sesión a las 23:00, ejecute la copia de seguridad de todos modos.

- Programación: **Semanal**, los viernes. Iniciar a las: **20:00**.
- Condición: **Los usuarios cerraron la sesión**.
- Condiciones de inicio de la copia de seguridad: **Esperar hasta que se cumplan las condiciones**, **Iniciar la copia de seguridad de todos modos después de 3** horas.

Como resultado:

- Si, para las 20:00, todos los usuarios han cerrado la sesión, la copia de seguridad se iniciará a las 20:00.
- Si el último usuario cierra sesión entre las 20:00 y las 23:00, la copia de seguridad se iniciará inmediatamente.
- Si a las 23:00 todavía hay usuarios que no han cerrado sesión, la copia de seguridad se iniciará a las 23:00.

© Acronis International GmbH, 2003-2025

Se adapta al intervalo de tiempo

Utilice esta condición de inicio para restringir el inicio de la copia de seguridad a un intervalo concreto.

Ejemplo

Una empresa usa distintas ubicaciones en el mismo dispositivo de almacenamiento conectado a la red para realizar copias de seguridad de servidores y datos de usuarios.

El día hábil empieza a las 8:00 y termina a las 17:00. Los datos de los usuarios deben incluirse en una copia de seguridad en cuanto los usuarios cierren la sesión, pero nunca antes de las 16:30.

Todos los días a las 23:00 se realiza la copia de seguridad de los servidores de la empresa. Es preferible que las copias de seguridad de los datos de los usuarios se realicen antes de las 23:00, para liberar ancho de banda de la red de las copias de seguridad de los servidores..

Realizar la copia de seguridad de los datos de los usuarios no lleva más de una hora, por lo tanto, la hora límite para iniciar una copia de seguridad son las 22:00. Si un usuario todavía no hubiera cerrado sesión después del intervalo especificado, o si cierra la sesión en cualquier otro momento, se debe omitir la copia de seguridad de los datos de los usuarios.

- Suceso: **Cuando un usuario cierra sesión en el sistema**. Especifique la cuenta de usuario: **Cualquier usuario**.
- Condición: **Se encuentra dentro del intervalo de tiempo** de **16:30** a **22:00**.
- Condiciones de inicio de la copia de seguridad: **Omita la copia de seguridad planificada**.

Como resultado:

- Si el usuario cierra sesión entre las 16:30 y las 22:00, la copia de seguridad se iniciará inmediatamente.
- Si el usuario cierra la sesión en cualquier otro momento, la copia de seguridad se omitirá.

Ahorrar batería

Utilice esta condición de inicio para evitar una copia de seguridad si un equipo (por ejemplo, un portátil o tableta) no está conectado a una fuente de alimentación. En función del valor de la opción Condiciones de inicio de la copia de seguridad, la copia de seguridad omitida se iniciará o no después de que el equipo se conecte a una fuente de alimentación.

Las siguientes opciones están disponibles:

- **No iniciar con alimentación por batería**
  Una copia de seguridad se iniciará únicamente si el equipo está conectado a una fuente de alimentación.
- **Iniciar con alimentación por batería si su nivel es superior a**
  Una copia de seguridad se iniciará si el equipo está conectado a una fuente de alimentación o si el nivel de la batería es superior a un valor especificado.

© Acronis International GmbH, 2003-2025

Ejemplo

Realice una copia de seguridad de sus datos todos los días hábiles a las 21:00. Si su equipo no está conectado a una fuente de alimentación, deberá omitir la copia de seguridad para ahorrar batería y esperar a que conecte el equipo a una fuente de alimentación.

- Programación: **Cada día**, **Ejecutar de lunes a viernes**. Iniciar a las: **21:00**.
- Condición: **Ahorrar batería**, **No iniciar con alimentación por batería**.
- Condiciones de inicio de la copia de seguridad: **Esperar hasta que se cumplan las condiciones**.

Como resultado:

- Si son las 21:00 y el equipo está conectado a una fuente de alimentación, la copia de seguridad se inicia inmediatamente.
- Si son las 21:00 y el equipo está conectado a una batería, la copia de seguridad se inicia cuando conecte el equipo a una fuente de alimentación.

No iniciar con conexiones de uso medido

Utilice esta condición de inicio para evitar una copia de seguridad (incluida la copia de seguridad a un disco local) si el equipo está conectado a Internet mediante una conexión definida como de uso medido en Windows. Para obtener más información sobre conexiones de uso medido en Windows, consulte https://support.microsoft.com/es-es/help/17452/windows-metered-internet-connections-faq.

La condición de inicio adicional **No iniciar con conexiones a las siguientes redes Wi-Fi** se habilita automáticamente cuando habilita la condición **No iniciar con conexiones de uso medido**. Esta es una medida adicional para evitar copias de seguridad en puntos de conexión móviles. Los siguientes nombres de red están especificados de forma predeterminada: android, phone, mobile y modem.

Para eliminar estos nombres de la lista, haga clic en el signo X. Para añadir un nuevo nombre, escríbalo en el campo vacío.

Ejemplo

Realice una copia de seguridad de sus datos todos los días hábiles a las 21:00. Si el equipo está conectado a Internet mediante una conexión de uso medido, debe omitir la copia de seguridad para ahorrar el tráfico de red y esperar al inicio planificado en el siguiente día hábil.

- Programación: **Cada día**, **Ejecutar de lunes a viernes**. Iniciar a las: **21:00**.
- Condición: **No iniciar con conexiones de uso medido**.
- Condiciones de inicio de la copia de seguridad: **Omita la copia de seguridad planificada**.

Como resultado:

© Acronis International GmbH, 2003-2025

- Si son las 21:00 y el dispositivo está conectado a Internet mediante una conexión de uso medido, la copia de seguridad se iniciará inmediatamente.
- Si son las 21:00 y el dispositivo está conectado a Internet mediante una conexión de uso medido, la copia de seguridad se iniciará el siguiente día hábil.
- Si el equipo siempre está conectado a Internet mediante una conexión de uso medido a las 21:00 en días hábiles, la copia de seguridad nunca se iniciará.

No iniciar con conexiones a las siguientes redes Wi-Fi

Utilice esta condición de inicio para evitar una copia de seguridad (incluida la copia de seguridad a un disco local) si el dispositivo está conectado a alguna de las redes inalámbricas especificadas (por ejemplo, si desea restringir copias de seguridad mediante un punto de conexión móvil).

Puede especificar los nombres de red Wi-Fi, también conocidos como identificadores de conjunto de servicios (SSID). La restricción se aplica a todas las redes de contengan el nombre especificado como una subcadena en su nombre, sin distinción de mayúsculas y minúsculas. Por ejemplo, si especifica `phone` como nombre de red, la copia de seguridad no se iniciará cuando el equipo esté conectado a alguna de las siguientes redes: `John's iPhone`, `phone_wifi` o `my_PHONE_wifi`.

La condición de inicio **No iniciar con conexiones a las siguientes redes Wi-Fi** se habilita automáticamente cuando habilita la condición **No iniciar con conexiones de uso medido**. Los siguientes nombres de red están especificados de forma predeterminada: android, `phone`, `mobile` y modem.

Para eliminar estos nombres de la lista, haga clic en el signo X. Para añadir un nuevo nombre, escríbalo en el campo vacío.

Ejemplo

Realice una copia de seguridad de sus datos todos los días hábiles a las 21:00. Si el equipo está conectado a Internet mediante un punto de conexión móvil (por ejemplo, un portátil conectado en modo de anclaje a red), debe omitir la copia de seguridad y esperar al inicio planificado en el siguiente día hábil.

- Programación: **Cada día**, **Ejecutar de lunes a viernes**. Iniciar a las: **21:00**.
- Condición: **No iniciar con conexiones a las siguientes redes Wi-Fi**, **Nombre de la red**: `<SSID of the hotspot network>`.
- Condiciones de inicio de la copia de seguridad: **Omita la copia de seguridad planificada**.

Como resultado:

- Si son las 21:00 y el equipo no está conectado a la red especificada, la copia de seguridad se inicia inmediatamente.
- Si son las 21:00 y el equipo no está conectado a la red especificada, la copia de seguridad se inicia en el siguiente día hábil.
- Si el equipo siempre está conectado a la red especificada a las 21:00 en días hábiles, la copia de seguridad nunca se iniciará.

© Acronis International GmbH, 2003-2025

Comprobar dirección IP del dispositivo

Utilice esta condición de inicio para evitar una copia de seguridad (incluida la copia de seguridad a un disco local) si cualquiera de las direcciones IP de los equipos quedan dentro o fuera del intervalo de direcciones IP especificado. Así, por ejemplo, puede evitar grandes cargos por tráfico de datos al realizar copias de seguridad de los equipos de usuarios que se encuentran en el extranjero, o puede evitar las copias de seguridad a través de una conexión de red privada virtual (VPN).

Las siguientes opciones están disponibles:

- **Iniciar si queda fuera del intervalo IP**
- **Iniciar si queda dentro del intervalo IP**

Puede especificar varios intervalos en cualquiera de esas opciones. Solo se admiten direcciones IPv4.

Ejemplo

Realice una copia de seguridad de sus datos todos los días hábiles a las 21:00. Si el equipo está conectado a la red corporativa mediante un túnel de VPN, deberá omitir la copia de seguridad.

- Programación: **Cada día**, **Ejecutar de lunes a viernes**. Iniciar a las **21:00**.
- Condición: **Comprobar dirección IP del dispositivo**, **Iniciar si queda fuera del intervalo IP**, **De**: `<beginning of the VPN IP address range>`, **A**: `<end of the VPN IP address range>`.
- Condiciones de inicio de la copia de seguridad: **Esperar hasta que se cumplan las condiciones**.

Como resultado:

- Si son las 21:00 y la dirección IP del equipo no está en el intervalo especificado, la copia de seguridad se inicia inmediatamente.
- Si son las 21:00 y la dirección IP del equipo no está en el intervalo especificado, la copia de seguridad se inicia cuando el equipo obtiene una dirección IP que no sea VPN.
- Si la dirección IP del equipo siempre está dentro del intervalo especificado en días hábiles a las 21:00, la copia de seguridad nunca se iniciará.

Opciones de planificación adicionales

Puede configurar las copias de seguridad para que se ejecuten solo cuando se cumplan unas condiciones específicas, durante un periodo determinado o con un retraso respecto a la planificación.

Pasos para configurar las condiciones de inicio

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. Haga clic en **Planificación**.
3. En el panel **Planificación**, haga clic en **Mostrar más**.

© Acronis International GmbH, 2003-2025

4. Seleccione las casillas de verificación junto a las condiciones de inicio que quiere incluir y, a continuación, haga clic en **Listo**.
   Para obtener más información sobre las condiciones de inicio disponibles y cómo configurarlas, consulte "Condiciones de inicio" (p. 566).
5. Guarde el plan de protección.

Pasos para configurar un intervalo de tiempo

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. Haga clic en **Planificación**.
3. Seleccione la casilla de verificación **Ejecutar el plan en un rango de fechas**.
4. Especifique el periodo según sus necesidades y, a continuación, haga clic en **Listo**.
5. Guarde el plan de protección.

Como resultado, las copias de seguridad solo se ejecutarán durante el periodo especificado.

Pasos para configurar un retraso

Para evitar una carga excesiva de la red al ejecutar la copia de seguridad de varias cargas de trabajo en una ubicación de red, se configura una pequeña demora aleatoria como una opción de copia de seguridad. Puede deshabilitarla o cambiar su configuración.

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. Haga clic en **Opciones de copia de seguridad** y, a continuación, seleccione **Planificación**.
   El valor de demora de cada carga de trabajo se selecciona de forma aleatoria entre cero y el valor máximo que especifique. De forma predeterminada, el valor máximo es 30 minutos.
   Para obtener más información sobre esta opción de copia de seguridad, consulte "Planificación" (p. 645)
   El valor de demora de cada carga de trabajo se calcula cuando se aplica el plan de protección a esa carga de trabajo y permanece igual hasta que se edita el valor máximo de demora.
3. Especifique el periodo según sus necesidades y, a continuación, haga clic en **Listo**.
4. Guarde el plan de protección.

Ejecutar una copia de seguridad manualmente

Puede ejecutar manualmente las copias de seguridad planificadas y sin planificar.

Pasos para ejecutar una copia de seguridad manualmente

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Seleccione la carga de trabajo de la que desea ejecutar una copia de seguridad y haga clic en **Proteger**.
3. Seleccione el plan de protección del que desea crear la copia de seguridad.

© Acronis International GmbH, 2003-2025

Si no se aplica ningún plan de protección a la carga de trabajo, aplique un plan existente o cree uno nuevo.

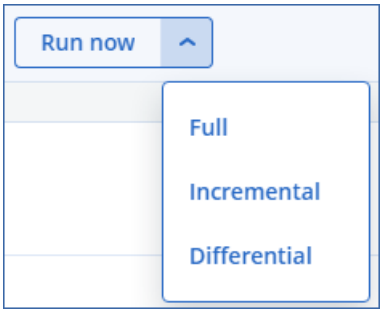
Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 250).

4. [Para crear el tipo de copia de seguridad predeterminado] En el plan de protección, haga clic en el icono **Ejecutar ahora**.



De forma alternativa, en el plan de protección, expanda el módulo **Copia de seguridad** y haga clic en el botón **Ejecutar ahora**.

5. [Para crear un tipo específico de copia de seguridad] En el plan de protección, expanda el módulo **Copia de seguridad** y haga clic en la flecha junto al botón **Ejecutar ahora** y, a continuación, seleccione el tipo de copia de seguridad.



Nota
La selección del tipo no está disponible para los esquemas de copias de seguridad que utiliza solo un método de copia de seguridad, por ejemplo, **Siempre incremental (un archivo)** o **Siempre completa**.

Como resultado, la operación de copia de seguridad se inicia. Puede consultar su progreso y su resultado en la pestaña **Dispositivos**, en la columna **Estado**.

Normas de retención

Para eliminar las copias de seguridad más antiguas automáticamente, configure las reglas de retención de copias de seguridad en el plan de protección.

Puede basar las reglas de retención en cualquiera de la siguientes propiedades de copia de seguridad:

- Número
- Edad

© Acronis International GmbH, 2003-2025

- Tamaño

Las reglas de retención disponibles y sus opciones dependen del esquema de copias de seguridad. Las reglas también son relevantes para los agentes, cargas de trabajo y copias de seguridad de la nube a la nube. Para obtener más información, consulte "Reglas de retención según el esquema de copias de seguridad" (p. 577).

Dependiendo de la configuración del plan de protección, las reglas de retención se aplican a un archivo antes o después de una copia de seguridad.

Puede deshabilitar la eliminación automática de las copias de seguridad antiguas. Para ello, seleccione la opción **Conservar las copias de seguridad indefinidamente** al configurar las reglas de retención. Esto podría dar como resultado un mayor uso del almacenamiento y tendría que eliminar las copias de seguridad antiguas innecesarias de forma manual.

Consejos importantes

- Las reglas de retención son parte del plan de protección. Si revoca o elimina un plan, las reglas de retención de dicho plan ya no se aplicarán. Consulte "Eliminación de copias de seguridad" (p. 727) para obtener más información sobre cómo eliminar copias de seguridad que ya no necesita.
- Puede configurar una regla de retención para que se ejecute antes o después de la operación de copia de seguridad, lo que da como resultado un número o tamaño diferente de las copias de seguridad retenidas.

  Por ejemplo, en **Cuántas se conservarán** > **Por número de copias de seguridad**, selecciona 2. La siguiente tabla compara los resultados de aplicar las reglas de retención antes o después de la copia de seguridad.

Antes de la copia de seguridad	Después de la copia de seguridad
◦ Se ejecuta una operación de limpieza. Se conservan dos copias de seguridad. ◦ Se ejecuta una operación de copia de seguridad. Se crea una nueva copia de seguridad. Resultado: Hay tres copias de seguridad disponibles.	◦ Se ejecuta una operación de copia de seguridad. Se crea una nueva copia de seguridad. ◦ Se ejecuta una operación de limpieza. Se conservan dos copias de seguridad. Resultado: Hay dos copias de seguridad disponibles.

- Si, de acuerdo con el esquema y el formato de copia de seguridad, cada copia de seguridad se almacena como un archivo independiente, no podrá eliminar aquellas de las que dependan otras copias de seguridad incrementales o diferenciales. Esta copia de seguridad se eliminará según las reglas de retención aplicadas a las copias de seguridad dependientes. Esta configuración podría dar como resultado un aumento del uso del almacenamiento porque se pospone la eliminación de algunas copias de seguridad. Además, la antigüedad, la cantidad o el tamaño de las copias de seguridad pueden superar los valores que especifique. Para obtener más información sobre cómo cambiar este comportamiento, consulte "Consolidación de la copia de seguridad" (p. 595).
- De forma predeterminada, la última copia de seguridad creada por un plan de protección nunca se elimina. Sin embargo, si configura una regla de retención para limpiar copias de seguridad

© Acronis International GmbH, 2003-2025

antes de iniciar una nueva operación de copia de seguridad y establecer que el número de copias de seguridad que se deben mantener sea cero, la última copia de seguridad también se eliminará.

Advertencia.
Si aplica esta regla de retención a un conjunto de copias de seguridad con una sola copia de seguridad y la operación de copia de seguridad falla, no podrá recuperar sus datos, ya que la copia de seguridad existente se eliminará antes de que se cree una nueva.

Reglas de retención según el esquema de copias de seguridad

Las reglas de retención disponibles y su configuración dependen del esquema de copia de seguridad que utilice en el plan de protección. Para obtener más información sobre los esquemas de copias de seguridad, consulte "Esquemas de copia de seguridad" (p. 557).

La tabla siguiente resume las reglas de retención disponibles y su configuración.

Esquema de copias de seguridad	Planificación	Reglas de retención y configuración disponibles
Siempre incremental (un archivo)	Mensualmente Semanalmente Diariamente Cada hora Copias de seguridad activadas por eventos	Por número de copias de seguridad Por antigüedad de la copia de seguridad (configuración independiente para las copias de seguridad mensuales, semanales, diarias y horarias) Mantener las copias de seguridad indefinidamente
Siempre completa	Mensualmente Semanalmente Diariamente Cada hora Copias de seguridad activadas por eventos	Por número de copias de seguridad Por antigüedad de la copia de seguridad (configuración independiente para las copias de seguridad mensuales, semanales, diarias y horarias) Por tamaño total de las copias de seguridad Mantener las copias de seguridad indefinidamente
Completa semanal, incremental diaria	Diariamente Copias de seguridad activadas por eventos	Por número de copias de seguridad Por antigüedad de la copia de seguridad (configuración independiente para las copias de seguridad semanales y diarias) Por tamaño total de las copias de seguridad Mantener las copias de seguridad indefinidamente
Completa mensual, diferencial semanal,	Mensualmente	Por número de copias de seguridad

© Acronis International GmbH, 2003-2025

Esquema de copias de seguridad	Planificación	Reglas de retención y configuración disponibles
incremental diaria	Semanalmente Diariamente Cada hora Copias de seguridad activadas por eventos	Por antigüedad de la copia de seguridad (configuración independiente para las copias de seguridad completas, diferenciales e incrementales) Por tamaño total de las copias de seguridad Mantener las copias de seguridad indefinidamente
Personalizado	Mensualmente Semanalmente Diariamente Cada hora Copias de seguridad activadas por eventos	Por número de copias de seguridad Por antigüedad de la copia de seguridad (configuración independiente para las copias de seguridad completas, diferenciales e incrementales) Por tamaño total de las copias de seguridad Mantener las copias de seguridad indefinidamente

¿Por qué hay copias de seguridad mensuales con un esquema horario?

Según el esquema de las copias de seguridad, puede configurar la opción **Por antigüedad de la copia de seguridad** para una de las siguientes copias de seguridad:

- Copias de seguridad mensuales, semanales, diarias y horarias.

  Estas configuraciones están disponibles con todos los esquemas de copia de seguridad no personalizados y se basan en el tiempo. Están disponibles todas estas copias de seguridad (mensuales, semanales, diarias y horarias), incluso si las configura para que se ejecuten de forma horaria. Consulte el siguiente ejemplo.

Copia de seguridad	Descripción
Mensualmente	Una copia de seguridad mensual es la primera copia de seguridad de cada mes.
Semanalmente	Una copia de seguridad semanal es la primera copia de seguridad que se crea el día de la semana que especifique en la opción Copia de seguridad semanal. Este día se considera como el principio de la semana en términos de reglas de retención. Si una copia de seguridad semanal es también la primera copia de seguridad del mes, se considerará una copia de seguridad mensual. En ese caso, se creará una copia de seguridad semanal el día seleccionado de la semana siguiente.
Diariamente	Una copia de seguridad diaria es la primera copia de seguridad del día, excepto si puede considerarse mensual o semanal. En ese caso, se creará una copia de seguridad diaria al día siguiente.

© Acronis International GmbH, 2003-2025

Copia de seguridad	Descripción
Cada hora	Una copia de seguridad de cada hora es la primera copia de seguridad que se crea en una hora, excepto si puede considerarse mensual, semanal o diaria. En ese caso, se creará una copia de seguridad por hora en la siguiente hora.

- Copias de seguridad completas, diferenciales e incrementales.

  Estas configuraciones están disponibles con todos el esquema de copia de seguridad **personalizado** y se basan en el método de la copia de seguridad. El esquema **Completa mensual, diferencial semanal, incremental diaria** es un esquema personalizado y preconfigurado.

Ejemplo

Utilice el esquema de copias de seguridad **Siempre incremental (un archivo)** con la configuración predeterminada para las copias de seguridad por hora:

- Planificada por hora.
- Las copias de seguridad se ejecutan por hora: De lunes a viernes, cada hora, de 8:00 a 18:00.
- La opción **Copia de seguridad semanal** está configurada para los lunes.

En la sección **Cuánto tiempo se conservarán** del plan de protección, puede aplicar las reglas de retención a las copias de seguridad mensuales, semanales, diarias y por hora.

La siguiente tabla resume los tipos de copia de seguridad creados durante un periodo de ocho días.

Fecha	Día de la semana	Descripción
1 de julio	Lunes	La primera copia de seguridad de cada mes es mensual, por lo que la primera copia de seguridad de hoy es mensual. El resto de copias de seguridad creadas a lo largo de hoy son por hora. Esta semana, la primera copia de seguridad se considera mensual. Por eso no hay una copia de seguridad semanal. La primera copia de seguridad de la próxima semana será semanal.
2 de julio	Martes	La primera copia de seguridad es diaria, las demás copias de seguridad del día se realizan cada hora.
3 de julio	Miércoles	La primera copia de seguridad es diaria, las demás copias de seguridad del día se realizan cada hora.
4 de julio	Jueves	La primera copia de seguridad es diaria, las demás copias de seguridad del día se realizan cada hora.
5 de julio	Viernes	La primera copia de seguridad es diaria, las demás copias de seguridad del día se realizan cada hora.

© Acronis International GmbH, 2003-2025

Fecha	Día de la semana	Descripción
6 de julio	Sábado	La primera copia de seguridad es diaria, las demás copias de seguridad del día se realizan cada hora.
7 de julio	Domingo	La primera copia de seguridad es diaria, las demás copias de seguridad del día se realizan cada hora.
8 de julio	Lunes	La primera copia de seguridad es semanal, las demás copias de seguridad del día se realizan cada hora.

Configuración de reglas de retención

Las reglas de retención son parte del plan de protección, y su disponibilidad y opciones dependen del esquema de copias de seguridad. Para obtener más información, consulte "Reglas de retención según el esquema de copias de seguridad" (p. 577).

Pasos para configurar las reglas de retención

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. Haga clic en **Cuántas se conservarán**.
3. Seleccione una de las siguientes opciones:
   - **Por número de copias de seguridad**
   - **Por antigüedad de la copia de seguridad**

     Hay disponible una configuración independiente para las copias de seguridad mensuales, semanales, diarias y horarias. El valor máximo para todos los tipos es 9999.

     También puede utilizar una única configuración para todas las copias de seguridad.
   - **Por tamaño total de las copias de seguridad**

     Este ajuste no está disponible con el esquema de copias de seguridad **Siempre incremental (un archivo)**.
   - **Mantener las copias de seguridad indefinidamente**
4. [Si no ha seleccionado **Mantener las copias de seguridad indefinidamente**] Configure los valores para la opción seleccionada.
5. [Si no ha seleccionado **Mantener las copias de seguridad indefinidamente**] Seleccione cuándo se aplican las reglas de retención.
   - Después de la copia de seguridad
   - Antes de la copia de seguridad

     Esta opción no está disponible cuando se hacen copias de seguridad de los clústeres de Microsoft SQL Server o Microsoft Exchange Server.
6. Haga clic en **Listo**.
7. Guarde el plan de protección.

© Acronis International GmbH, 2003-2025

Replicación

Con la replicación, cada nueva copia de seguridad se copia automáticamente en una ubicación de replicación. Las copias de seguridad en la ubicación de replicación no dependen de las copias de seguridad en la ubicación de origen, y viceversa.

Solo se replica la última copia de seguridad en la ubicación de origen. Sin embargo, si las copias de seguridad anteriores no pudieran replicarse (por ejemplo, debido a un problema de conexión de red), la operación de replicación incluirá todas las copias de seguridad que se hubieran creado después de la última replicación realizada correctamente.

Si se interrumpe una operación de replicación, la siguiente operación de replicación utilizará los datos ya procesados.

Nota
Este tema describe la replicación como parte de un plan de protección. También puede crear un plan de replicación de copias de seguridad independiente. Para obtener más información, consulte "Réplica de copia de seguridad" (p. 261).

Ejemplos de uso

- Garantizar la recuperación fiable

  Almacene sus copias de seguridad tanto de forma local (para una recuperación inmediata) como externa (para garantizar que las copias de seguridad permanezcan seguras incluso en caso de que se produzca un error en el almacenamiento o de que ocurra un desastre natural que afecte a la ubicación primaria).
- Utilice el almacenamiento en la nube para proteger los datos de cualquier posible desastre natural

  Replique las copias de seguridad en el almacenamiento en la cloud transfiriendo solo los cambios realizados en los datos.
- Mantenimiento de solo los últimos puntos de recuperación

  Configure reglas de retención para eliminar las copias de seguridad más antiguas de un almacenamiento rápido con el fin de ahorrar en costes de almacenamiento.

Ubicaciones compatibles

Ubicación	Como ubicación de origen	Como ubicación de replicación
Carpeta local	+	+
Carpeta de red	+	+
Almacenamiento en la nube	-*	+
Secure Zone	+	+

© Acronis International GmbH, 2003-2025

Ubicación	Como ubicación de origen	Como ubicación de replicación
Nube pública	- *	+

* La replicación desde la nube pública solo está disponible en planes de procesamiento de datos fuera del host. Consulte "Ubicaciones admitidas para el procesamiento de datos fuera del host" (p. 264).

Cómo activar la replicación

1. En un plan de protección, amplíe el módulo **Copia de seguridad** y, a continuación, haga clic en **Añadir ubicación**.

   Nota
   La opción **Añadir ubicación** no está disponible cuando se selecciona el almacenamiento en la nube en **Dónde guardar la copia de seguridad**.

2. En la lista de ubicaciones disponibles, seleccione la ubicación de replicación.
   La ubicación aparece en el plan de protección como **2.ª ubicación**, **3.ª ubicación**, **4.ª ubicación** o **5.ª ubicación**, según el número de ubicaciones que añada para la replicación.
3. [Opcional] Haga clic en el icono de engranaje para configurar las opciones de la ubicación de replicación.
   - **Ventana de copia de seguridad y rendimiento**: establezca la ventana de copia de seguridad para la ubicación seleccionada, como se describe en "Ventana de copia de seguridad y rendimiento" (p. 633). Estos ajustes definen el rendimiento de la replicación.
   - **Eliminar ubicación**: elimine la ubicación de replicación seleccionada.
   - [Solo para el almacenamiento en la nube] **Envío de datos físicos**: guarde la copia de seguridad inicial en un dispositivo de almacenamiento extraíble y envíelo para cargarlo en el almacenamiento en la nube, en lugar de replicarlo a través de internet.
     Esta opción es adecuada para ubicaciones con una conexión de red lenta o cuando se desee ahorrar ancho de banda en transferencias de archivos grandes a través de la red. Activar la opción no requiere cuotas de servicio avanzadas de Cyber Protect, pero necesitará una cuota de servicio de envío físico para crear una orden de envío y realizar su seguimiento. Consulte "Envío de datos físicos" (p. 637).

     Nota
     Esta opción es compatible con el agente de protección a partir de la versión C21.06 o posterior.

4. [Opcional] En la fila **Cuántas se conservarán** debajo de la ubicación de replicación, configure las reglas de retención para esa ubicación, como se describe en "Normas de retención" (p. 575).
5. [Opcional] Repita los pasos 1–4 para añadir más ubicaciones de replicación.
   Puede configurar hasta cuatro ubicaciones de replicación (**2.ª ubicación**, **3.ª ubicación**, **4.ª ubicación** y **5.ª ubicación**). Si selecciona **Almacenamiento en la nube**, no podrá añadir más ubicaciones de replicación.

© Acronis International GmbH, 2003-2025

Importante
Si habilita la copia de seguridad y la replicación en el mismo plan de protección, asegúrese de que la replicación se completa antes de la siguiente copia de seguridad programada. Si todavía se está realizando la replicación, no se iniciará la copia de seguridad: por ejemplo, una copia de seguridad programada que se ejecuta cada 24 horas no se iniciará si la replicación tarda 26 horas en completarse.

Para evitar esta dependencia, use un plan independiente para la replicación de copia de seguridad. Para obtener más información sobre este plan específico, consulte "Réplica de copia de seguridad" (p. 261).

Cifrado

Cyber Protect utiliza dos niveles de seguridad para proteger los datos respaldados del acceso no autorizado.

Los datos respaldados se cifran con una clave de 256 bits, que a su vez se cifra utilizando el hash SHA-2 (256 bits) de una contraseña de cifrado proporcionada por el usuario como clave, de la siguiente manera:

1. Al crear un plan de protección con cifrado habilitado, el usuario especifica una contraseña de cifrado.

   Advertencia.
   Cyber Protect no almacena esta contraseña. No es posible recuperar una contraseña perdida.

2. La función de derivación de claves basada en contraseña 2 (PBKDF2) se aplica a la contraseña de cifrado proporcionada por el usuario 1 048 576 veces (2 elevado a 20). Como resultado, se crea un hash SHA-2 (256 bits). Esta es la primera clave, que se utiliza para cifrar la segunda clave.
3. Se crea una clave aleatoria de 256 bits mediante OpenSSL. Esta es la segunda clave, que se utiliza para cifrar los datos respaldados.
4. La segunda clave se cifra mediante Advanced Encryption Standard (AES-256) y el hash que se deriva de la contraseña de cifrado proporcionada por el usuario.
5. La segunda clave cifrada se añade al archivo de la copia de seguridad.
6. Los datos respaldados se cifran mediante Advanced Encryption Standard con el modo Galois/Counter (AES-256 GCM) y la segunda clave.
7. Al recuperar datos, el usuario debe proporcionar la contraseña de cifrado. El hash de esa contraseña es la primera clave de cifrado. Esta clave se utiliza para descifrar la segunda clave. Con la segunda clave, se puede descifrar y recuperar el archivo de la copia de seguridad.

Nota
Usar el algoritmo AES-256 con una contraseña fuerte proporciona un cifrado resistente al cuántico. Es seguro contra ataques criptoanalíticos que dependen de la computación cuántica.

© Acronis International GmbH, 2003-2025

Se recomienda que cifre todas las copias de seguridad que estén almacenadas en el almacenamiento en la cloud, sobre todo si su empresa está sujeta al cumplimiento de reglamentaciones.

Puede configurar el cifrado de las siguientes maneras:

- En el plan de protección
- Como propiedad del equipo, utilizando la interfaz de Cyber Protect Monitor o de línea de comandos

Configurar el cifrado en el plan de protección

En un plan de protección, el cifrado está habilitado por defecto. Se utiliza el algoritmo AES-256.

Con una contraseña fuerte, el algoritmo AES-256 proporciona un cifrado resistente a la cuántica.

Para cuentas en el modo de cumplimiento, no puede configurar el cifrado en el plan de protección. Para obtener más información sobre cómo configurar el cifrado en el dispositivo protegido, consulte "Configurar el cifrado como una propiedad del equipo" (p. 584).

Para configurar el cifrado

1. En un plan de protección, expanda el módulo **Copia de seguridad**.
2. En **Cifrado**, haga clic en **Especificar contraseña**.
3. Especifique y confirme la contraseña de cifrado.
4. Haga clic en **Aceptar**.

Advertencia.
No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.

No puede cambiar la configuración de cifrado después de aplicar el plan de protección. Para usar diferentes configuraciones de cifrado, cree un plan.

Configurar el cifrado como una propiedad del equipo

Puede configurar el cifrado de la copia de seguridad como una propiedad del equipo. En este caso, el cifrado de la copia de seguridad no se configura en el plan de protección, sino en la carga de trabajo protegida. El cifrado como propiedad del equipo utiliza el algoritmo AES con una clave de 256 bits (AES-256).

Nota
Usar el algoritmo AES-256 con una contraseña fuerte proporciona un cifrado resistente al cuántico. Es seguro contra ataques criptoanalíticos que dependen de la computación cuántica.

Configurar el cifrado como una propiedad del equipo afecta a los planes de protección de la forma siguiente:

© Acronis International GmbH, 2003-2025

- **Planes de protección que ya se han aplicado al equipo.** Si la configuración de cifrado de un plan de protección es diferente, las copias de seguridad fallarán.
- **Planes de protección que se aplicarán al equipo más tarde.** La configuración de cifrado guardada en el equipo anulará la configuración de cifrado en el plan de protección. Cualquier copia de seguridad se cifrará, incluso si el cifrado está deshabilitado en la configuración del módulo de copia de seguridad.

Para cuentas en el modo de cumplimiento, solo está disponible el cifrado como una propiedad del equipo.

Si tiene más de un agente de VMware conectado al mismo vCenter Server y configura el cifrado como una propiedad del equipo, deberá usar la misma contraseña de cifrado en todos los equipos con agente de VMware, debido al equilibrio de carga entre los agentes.

Puede configurar el cifrado como una propiedad del equipo de las formas siguientes:

- En la línea de comando
- En Cyber Protect Monitor (Disponible para Windows y macOS)

Advertencia.
No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.

Para configurar el cifrado como una propiedad del equipo

En la línea de comando

1. Inicie sesión como administrador en Windows o usuario root en Linux.
2. Navegue hasta la herramienta **acropsh** de la siguiente manera:
   - Para Windows:

     ```
     <installation_path>\PyShell\bin\
     ```

     Donde `<installation_path>` es `%ProgramFiles%\BackupClient`.
   - Para Linux:

     ```
     /usr/sbin/
     ```

   - Para un dispositivo virtual:

     ```
     /./sbin/
     ```

3. [Para especificar la contraseña en la interfaz de línea de comandos]
   - Ejecute el siguiente comando:
     - Para Windows

       ```
       acropsh.exe -m manage_creds --set-password
       ```


© Acronis International GmbH, 2003-2025

- Para Linux y dispositivo virtual

```
acropsh -m manage_creds --set-password
```

- En la entrada interactiva, especifique la contraseña de cifrado.

4. [Para especificar la contraseña mediante un archivo]
   - Prepare un archivo de texto en el que especifique la contraseña de cifrado.
     El archivo debe tener el siguiente contenido:

     ```
     --set-password <password>
     ```

     Donde `<password>` es la contraseña de cifrado.

     Advertencia.
     Por motivos de seguridad, asegúrese de que solo usted puede acceder a este archivo. Elimine el archivo después de terminar este procedimiento.

   - En la línea de comando, ejecute el siguiente comando:
     - Para Windows

       ```
       acropsh.exe -m manage_creds @<file_path>
       ```

     - Para Linux y dispositivo virtual

       ```
       acropsh -m manage_creds @<file_path>
       ```

     Donde `<file_path>` es la ruta completa al archivo en el que se especifica la contraseña.
     Por ejemplo, `/home/JohnDoe/MyFile.txt` o `C:\Users\JohnDoe\MyFile.txt`.

En Cyber Protect Monitor

1. Inicie sesión como administrador.
2. Haga clic en el icono de Cyber Protect Monitor del área de notificaciones (en Windows) o en la barra de menús (en macOS).
3. Haga clic en el icono de engranaje y, luego, en **Configuración** > **Cifrado**.
4. Seleccione **Establecer una contraseña para este equipo**. Especifique y confirme la contraseña de cifrado.
5. Haga clic en **Guardar**.

Advertencia.
No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.

Para restablecer la configuración de cifrado

1. Inicie sesión como administrador en Windows o usuario root en Linux.
2. Navegue hasta la herramienta **acropsh** de la siguiente manera:

© Acronis International GmbH, 2003-2025

- Para Windows:

```
<installation_path>\PyShell\bin\
```

  Donde `<installation_path>` es `%ProgramFiles%\BackupClient`.

- Para Linux:

```
/usr/sbin/
```

- Para un dispositivo virtual:

```
 /./sbin/
```

3. Ejecute el siguiente comando:
   - Para Windows

```
acropsh.exe -m manage_creds --reset
```

   - Para Linux y dispositivo virtual

```
acropsh -m manage_creds --reset
```

Importante
Si restablece el cifrado como una propiedad del equipo o cambia la contraseña de cifrado después de que un plan de protección cree una copia de seguridad, la próxima operación de copia de seguridad fallará. Para continuar con la copia de seguridad de la carga de trabajo, cree un plan de protección.

Notarización

Nota
Esta función está disponible con el paquete Advanced Backup.

La notarización permite demostrar que un archivo es auténtico y que no ha cambiado desde su copia de seguridad. Se recomienda habilitar la notarización cuando realice la copia de seguridad de documentos legales u otros archivos cuya autenticidad se desee demostrar.

La Notarización está disponible solo para copias de seguridad a nivel de archivo. Se omiten los archivos con firma digital, ya que no se requiere su notarización.

La notarización *no* está disponible:

- Si el formato de copia de seguridad está establecido en la **Versión 11**
- Si el destino de la copia de seguridad es Secure Zone

© Acronis International GmbH, 2003-2025

Cómo utilizar la notarización

Para habilitar la certificación de todos los archivos seleccionados para su copia de seguridad (excepto los archivos con firma digital), active la opción **Notarización** cuando cree un plan de protección.

Al configurar la recuperación, los archivos notarizados se marcarán con un icono especial y podrá verificar la autenticidad del archivo.

Cómo funciona

Durante una copia de seguridad, el agente calcula los códigos de cifrado de los archivos de los que se ha realizado la copia de seguridad, crea un árbol de cifrado (en función de la estructura de carpetas), guarda el árbol en la copia de seguridad y envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización guarda la raíz del árbol de cifrado en la base de datos de cadenas de bloques de Ethereum para garantizar que este valor no cambie.

Al verificar la autenticidad del archivo, el agente calcula su cifrado y lo compara con el almacenado en el árbol de cifrado de la copia de seguridad. Si los cifrados no coinciden, se considerará que el archivo no es auténtico. De lo contrario, la autenticidad del archivo queda garantizada por el árbol de cifrado.

Para verificar que el propio árbol de cifrado no se haya visto alterado, el agente envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización lo compara con el almacenado en la base de datos de cadenas de bloques. Si los cifrados coinciden, se garantiza que el archivo seleccionado es auténtico. De lo contrario, el software muestra un mensaje para indicar que el archivo no es auténtico.

Opciones de copia de seguridad predeterminadas

Los valores predeterminados de las opciones de copia de seguridad existen a nivel de empresa, unidad y usuario. Cuando se crea una unidad o una cuenta de usuario dentro de una empresa o dentro de una unidad, se heredan los valores predeterminados establecidos para la empresa o la unidad.

Los administradores de empresa y de unidad, junto con los usuarios sin derechos de administrador, pueden cambiar un valor de opción predeterminado en comparación con el predefinido. El nuevo valor se utilizará de forma predeterminada en todos los planes de protección creados en el nivel correspondiente cuando se produzca el cambio.

Al crear un plan de protección, un usuario puede anular un valor predeterminado con un valor personalizado que será específico del plan en cuestión únicamente.

Para cambiar el valor de la opción predeterminada

© Acronis International GmbH, 2003-2025

1. Realice uno de los siguientes procedimientos:
   - Para cambiar el valor predeterminado de la empresa, inicie sesión en la consola de Cyber Protect como administrador de la empresa.
   - Para cambiar el valor predeterminado de una unidad, inicie sesión en la consola de Cyber Protect como administrador de la unidad.
   - Para cambiar el valor predeterminado por su cuenta, inicie sesión en la consola de Cyber Protect con una cuenta que no tenga derechos de administrador.
2. Haga clic en **Configuración** > **Configuración del sistema**.
3. Amplíe la sección **Opciones de copia de seguridad predeterminadas**.
4. Seleccione la opción y, a continuación, realice los cambios necesarios.
5. Haga clic en **Guardar**.

Opciones de copia de seguridad

Para modificar las opciones de copia de seguridad de un plan de protección, en el módulo **Copia de seguridad**, en el campo **Opciones de copia de seguridad**, haga clic en **Modificar**.

Disponibilidad de las opciones de copia de seguridad

El conjunto de opciones de copia de seguridad disponible depende de:

- El entorno en el que opera el agente (Windows, Linux o macOS).
- El tipo de datos que se está incluyendo en la copia de seguridad (discos, archivos, equipos virtuales, datos de aplicación).
- El destino de la copia de seguridad (el almacenamiento en la cloud o la carpeta local o de red).

La siguiente tabla resume la disponibilidad de las opciones de copia de seguridad.

	Copia de seguridad a nivel de discos			**Copia de seguridad a nivel de archivos**			**Equipos virtuales**				**SQL y Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Azure**	**Windows**
Alertas	+	+	+	+	+	+	+	+	+	-	+
Puntos de restauración de Azure: Retención	-	-	-	-	-	-	-	-	-	+	-
Puntos de restauración de Azure: Nivel de coherencia	-	-	-	-	-	-	-	-	-	+	-

© Acronis International GmbH, 2003-2025

Puntos de restauración de Azure: Gestión de discos no compatibles	-	-	-	-	-	-	-	-	-	+	-
Consolidación de la copia de seguridad	+	+	+	+	+	+	+	+	+	-	-
Nombre del archivo de la copia de seguridad	+	+	+	+	+	+	+	+	+	+	+
Formato de la copia de seguridad	+	+	+	+	+	+	+	+	+	-	+
Validación de la copia de seguridad	+	+	+	+	+	+	+	+	+	-	+
Seguimiento de bloques modificados (CBT)	+	-	-	-	-	-	+	+	-	-	-
Modo de copia de seguridad de clústeres	-	-	-	-	-	-	-	-	-	-	+
Tasa de compresión	+	+	+	+	+	+	+	+	+	+	+
Control de errores											
Reintentar si se produce un error	+	+	+	+	+	+	+	+	+	+	+
No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)	+	+	+	+	+	+	+	+	+	+	+
Ignorar los sectores defectuosos	+	-	+	+	-	+	+	+	+	+	-
Reintentar si se produce un error durante la	-	-	-	-	-	-	+	+	+	+	-

© Acronis International GmbH, 2003-2025

creación de instantáneas de VM											
Copias de seguridad incrementales/diferenciales rápidas	+	+	+	-	-	-	-	-	-	-	-
Instantánea de la copia de seguridad a nivel de archivo	-	-	-	+	+	+	-	-	-	-	-
Filtros de archivo	+	+	+	+	+	+	+	+	+	+	-
Datos forenses	+	-	-	-	-	-	-	-	-	-	-
Truncamiento de registros	-	-	-	-	-	-	+	+	-	-	Solo SQL
Toma de instantáneas de LVM	-	+	-	-	-	-	-	-	-	-	-
Puntos de montaje	-	-	-	+	-	-	-	-	-	-	-
Instantánea multivolumen	+	+	-	+	+	-	-	-	-	-	-
Recuperación con un clic	+	+	-	-	-	-	-	-	-	-	-
Ventana de copia de seguridad y rendimiento	+	+	+	+	+	+	+	+	+	-	+
Envío de datos físicos	+	+	+	+	+	+	+	+	+	-	-
Comandos previos/posteriores	+	+	+	+	+	+	+	+	+	-	+
Comandos previos o posteriores a la captura de datos	+	+	+	+	+	+	-	-	-	-	+
Planificación											
Distribuir las	+	+	+	+	+	+	+	+	+	-	+

© Acronis International GmbH, 2003-2025

horas de inicio en una ventana de tiempo											
Limite el número de copias de seguridad que se ejecutan simultáneamente	-	-	-	-	-	-	+	+	+	-	-
Copia de seguridad sector por sector	+	+	-	-	-	-	+	+	+	+	-
División	+	+	+	+	+	+	+	+	+	-	+
Manejo de fallos de la tarea	+	+	+	+	+	+	+	+	+	-	+
Condiciones de inicio de la tarea	+	+	-	+	+	-	+	+	+	-	+
Servicio de instantáneas de volumen (VSS)	+	-	-	+	-	-	-	+	-	-	+
Servicio de instantáneas de volumen (VSS) para equipos virtuales	-	-	-	-	-	-	+	+	-	-	-
Copia de seguridad semanal	+	+	+	+	+	+	+	+	+	+	+
Registro de eventos de Windows	+	-	-	+	-	-	+	+	-	-	+

Alertas

No se realizan copias de seguridad correctamente durante un número especificado de días

El valor predeterminado es el siguiente: **Deshabilitado**.

Esta opción determina si se debe crear una alerta cuando el plan de protección no ha realizado una copia de seguridad correcta en un periodo de tiempo determinado. Además de las copias de

© Acronis International GmbH, 2003-2025

seguridad fallidas, el software también hace un recuento de las copias de seguridad que no se han realizado según la planificación (copias de seguridad perdidas).

Las alertas se generan por equipo y se muestran en la pestaña **Alertas**.

Puede especificar el número de días consecutivos sin realizar copias de seguridad tras los que se generará la alerta.

Puntos de restauración de Azure

Hay tres opciones de copia de seguridad de Microsoft Azure disponibles al configurar la copia de seguridad sin agente de máquinas virtuales de Microsoft Azure:

- Puntos de restauración de Azure: Retención
- Puntos de restauración de Azure: Nivel de coherencia
- Puntos de restauración de Azure: Gestión de discos no compatibles

Puntos de restauración de Azure: Retención

Esta opción le permite definir cuántos puntos de restauración de Microsoft Azure desea conservar después de una copia de seguridad (el valor predeterminado es 3). Estos puntos de restauración mejoran el rendimiento de las copias de seguridad incrementales, que utilizan la función Changed Block Tracking (CBT).

El número máximo de puntos de restauración de Azure que puede mantener es 200 (como lo recomienda Microsoft), y solo debe haber una colección de puntos de restauración creada para cada máquina virtual.

Al realizar la recuperación en la máquina virtual original de Microsoft Azure, desde una copia de seguridad que tiene el punto de restauración de Azure correspondiente aún disponible en Microsoft Azure, el proceso de recuperación utiliza este punto de restauración para revertir automáticamente el estado de la máquina virtual, en lugar de recuperar datos del archivo de copia de seguridad. Esto ayuda a optimizar el tráfico y el rendimiento de la recuperación.

Tenga en cuenta que la lógica de rotación de los puntos de restauración es gestionada por el plan de protección. Si hay dos planes aplicados a la misma máquina virtual, entonces cada plan trata todos los puntos de restauración dentro de la colección como propios y rota las copias de seguridad de acuerdo con el valor definido de **Puntos de restauración**.

Puntos de restauración de Azure: Nivel de coherencia

Esto le permite seleccionar el nivel de coherencia de los puntos de restauración, como los puntos de restauración coherentes con la aplicación o los puntos de restauración coherentes con el sistema de archivos.

Nota
Esta opción se aplica únicamente a las máquinas virtuales que están encendidas.

© Acronis International GmbH, 2003-2025

Puede seleccionar una de las siguientes opciones:

- **Exigir puntos de restauración coherentes con la aplicación**: Si el punto de restauración no es coherente con la aplicación, no se realizará correctamente la copia de seguridad.

  Tenga en cuenta que los puntos de restauración de máquinas virtuales admiten la coherencia de aplicaciones para máquinas virtuales que ejecutan sistemas operativos Windows, y la coherencia del sistema de archivos para máquinas virtuales que ejecutan sistemas operativos Linux. Los puntos de restauración coherentes con la aplicación utilizan escritores de VSS (o secuencias de comandos previas/posteriores para Linux) para garantizar la coherencia de los datos de la aplicación antes de que se cree un punto de restauración.
- **Alertar sobre puntos de restauración coherentes con el sistema de archivos o con bloqueos**: Si el punto de restauración es coherente con el sistema de archivos o con bloqueos, la copia de seguridad se completa con un aviso.

  Esta opción añade un aviso al registro y marca la actividad con un aviso si el nivel de coherencia de la instantánea es coherente con el sistema de archivos y está por debajo (coherente con el bloqueo).
- **Alertar sobre puntos de restauración coherentes con fallos**: Si el punto de restauración es consistente con bloqueos, la copia de seguridad se completa con un aviso. Los puntos de restauración consistentes con el sistema de archivos y la aplicación no generan avisos. Esta opción está seleccionada de manera predeterminada.

  Esta opción añade un aviso al registro y marca la actividad con un aviso.
- **Ignorar nivel de coherencia**: Independientemente del nivel de coherencia del punto de restauración, la copia de seguridad se completará correctamente.

  Esta opción añade un mensaje de información al registro y ejecuta el plan de protección correctamente.

Puntos de restauración de Azure: Gestión de discos no compatibles

Esta opción le permite determinar qué hacer si se está realizando una copia de seguridad de una máquina virtual con un disco sin gestionar, compartido o efímero. Tenga en cuenta que estos tipos de discos no son compatibles con los puntos de restauración de Microsoft Azure y no se pueden copiar en el modo sin agente. Si necesita copiar los datos de estos discos, instale el agente de protección dentro del sistema operativo invitado de la máquina virtual.

Puede seleccionar una de las siguientes opciones:

- **Ignorar discos no compatibles**: La copia de seguridad se completa correctamente y se omiten los discos no compatibles.
- **Avisar en caso de discos no compatibles**: La copia de seguridad se completa con un aviso sobre el disco no compatible. Esta opción está seleccionada de manera predeterminada.
- **Fallar en caso de discos no admitidos**: La copia de seguridad falla si se está realizando la copia de seguridad de una máquina virtual con un disco no admitido.

© Acronis International GmbH, 2003-2025

Consolidación de la copia de seguridad

Esta opción define si se consolidarán las copias de seguridad durante la limpieza o si se eliminarán cadenas de copia de seguridad completas.

El valor predeterminado es el siguiente: **Deshabilitado**.

La consolidación es el proceso de combinar dos o más copias de seguridad subsiguientes en una sola.

Si esta opción está habilitada, una copia de seguridad que debería eliminarse durante la limpieza se consolida con la siguiente copia de seguridad dependiente (incremental o diferencial).

Si no, la copia de seguridad se retiene hasta que se puedan eliminar todas las dependientes. Esto ayuda a evitar una consolidación que requeriría mucho tiempo, pero necesita espacio extra para almacenar copias de seguridad cuya eliminación se ha postergado. El número de copias de seguridad o su antigüedad puede superar los valores indicados en las reglas de retención.

Importante
Tenga en cuenta que la consolidación es solo un método para eliminar y no una alternativa a la eliminación. La copia de seguridad resultante no tendrá los datos que estaban en la copia de seguridad eliminada y que no estaban en la copia de seguridad incremental o diferencial retenida.

Esta opción *no* es eficaz si sucede algo de lo que se indica a continuación:

- El destino de la copia de seguridad es el almacenamiento en la cloud.
- El esquema de copias de seguridad está configurado como **Siempre incremental (un archivo)**.
- El formato de copia de seguridad se configura en la **Versión 12**.

Las copias de seguridad almacenadas en el almacenamiento en la cloud, con el formato tanto de la versión 11 como de la 12, y las copias de seguridad de archivo único, siempre se consolidan ya que la estructura interna permite realizar una consolidación rápida y sencilla.

Sin embargo, si se usa el formato de la versión 12 y hay varias cadenas de copias de seguridad (cada cadena almacenada en un archivo .tibx independiente), la consolidación solo funciona en la última cadena. El resto de cadenas se eliminan como un todo, excepto la primera, que se reduce al mínimo tamaño para conservar la metainformación (~12 KB). Esta metainformación es necesaria para garantizar la consistencia de los datos cuando se lleven a cabo operaciones de lectura y escritura simultáneas. Las copias de seguridad incluidas en estas cadenas desaparecen de la GUI en cuanto se aplica la regla de retención, aunque existan físicamente hasta que se elimine toda la cadena.

En el resto de los casos, las copias de seguridad cuya eliminación se posponga se marcan con el icono de la papelera () en el GUI. Si hace clic en el signo de X para eliminar una copia de seguridad, se llevará a cabo la consolidación.

© Acronis International GmbH, 2003-2025

Nombre del archivo de copia de seguridad.

Esta opción define los nombres de los archivos de copia de seguridad creados por el plan de protección o por el plan de copias de seguridad de aplicaciones de la nube.

Para los archivos de copia de seguridad creados por planes de protección, puede ver estos nombres en un administrador de archivos cuando explore la ubicación de copias de seguridad.

¿Qué es un archivo de copia de seguridad?

Cada plan de protección crea un archivo o varios en la ubicación de la copia de seguridad, dependiendo de qué esquema de copias de seguridad y qué formato de copia de seguridad se utilice. La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

	Siempre incremental (un archivo)	**Otros esquemas de copia de seguridad**
Formato de copia de seguridad **Versión 11**	Un archivo TIB y otro archivo de metadatos XML	Varios archivos TIB y un archivo de metadatos XML
Formato de copia de seguridad **Versión 12**	Un archivo TIBX por cadena de copia de seguridad (una copia de seguridad completa o diferencial y todas las copias de seguridad incrementales que dependan de ella). Si el tamaño de un archivo almacenado en una carpeta local o de red (SMB) sobrepasa los 200 GB, este se divide en archivos de 200 GB de manera predeterminada.	

Todos los archivos tienen el mismo nombre, con o sin marca horaria o número de secuencia. Puede definir este nombre (denominado nombre de archivo de copia de seguridad) al crear o modificar un plan de protección o un plan de copias de seguridad de aplicaciones de la nube.

Nota
La marca de fecha y hora se añade al nombre del archivo de copia de seguridad solo en el formato de copia de seguridad de la versión 11.

Si cambia el nombre de un archivo de copia de seguridad en un plan de protección o un plan de copias de seguridad de aplicaciones de la nube, la siguiente copia de seguridad será completa.

Si especifica el nombre de archivo de una copia de seguridad que ya existe en el mismo equipo, se creará una copia de seguridad completa, incremental o diferencial según la programación del plan.

Nota
Si mueve los archivos de las copias de seguridad (.tibx) desde su almacenamiento original, no les cambie el nombre. Los archivos renombrados aparecerán dañados y no podrá recuperar los datos de estos.

© Acronis International GmbH, 2003-2025

Es posible configurar nombres de archivos de copia de seguridad para ubicaciones que un administrador de archivos no puede buscar (como el almacenamiento en la nube). En ese caso, verá los nombres personalizados en la pestaña **Almacenamiento de la copia de seguridad**.

¿Dónde se ven los nombres del archivo de copia de seguridad?

Para planes de protección, en la pestaña **Almacenamiento de la copia de seguridad**, seleccione la ubicación y luego seleccione el archivo de copia de seguridad.

- El nombre del archivo de copia de seguridad predeterminado aparece en el panel **Detalles**.
- Si configura un nombre de archivo de copia de seguridad no predeterminado, aparecerá directamente en la pestaña **Almacenamiento de la copia de seguridad**, en la columna **Nombre**.

Para planes de copias de seguridad de aplicaciones en la nube, en la pestaña **Almacenamiento de la copia de seguridad**, seleccione la ubicación, seleccione el archivo de copia de seguridad y haga clic en el icono del engranaje.

Limitaciones de los nombres de archivos de copia de seguridad

- Los nombres de archivo de copia de seguridad no pueden acabar en un dígito.
  Con el fin de impedir que el nombre termine con un dígito, se añade la letra "A" al nombre de copia de seguridad predeterminado. Al crear un nombre personalizado, asegúrese siempre de que no termine en un dígito. Al usar variables, el nombre no puede acabar con una variable, ya que la variable podría finalizar a su vez en un dígito.
- Un nombre de archivo de copia de seguridad no puede contener los símbolos siguientes: **()&?*$<>":\|/#**, finalizaciones de línea (**\n**) ni pestañas (**\t**).

Nota
Elija nombres de archivo de copia de seguridad fáciles de usar. Esto le ayudará a distinguir fácilmente copias de seguridad al buscar su ubicación con un administrador de archivos.

Nombre de archivo de copia de seguridad predeterminado

El nombre de archivo de copias de seguridad predeterminado para copias de seguridad de equipo virtuales y físicos completos, discos, volúmenes, archivos, carpetas, bases de datos de Microsoft SQL Server, bases de datos de Microsoft Exchange Server y configuración ESXi es `[Machine Name]-[Plan ID]-[Unique ID]A`.

El nombre predeterminado para copias de seguridad de buzón de correo de Exchange y copias de seguridad de buzón de correo de Microsoft 365 creadas por un agente local para Microsoft 365 es `[Mailbox ID]_mailbox_[Plan ID]A`.

El nombre predeterminado de las copias de seguridad de Microsoft Azure incluye el prefijo `[Mailbox ID]_`. Este prefijo no se puede eliminar.

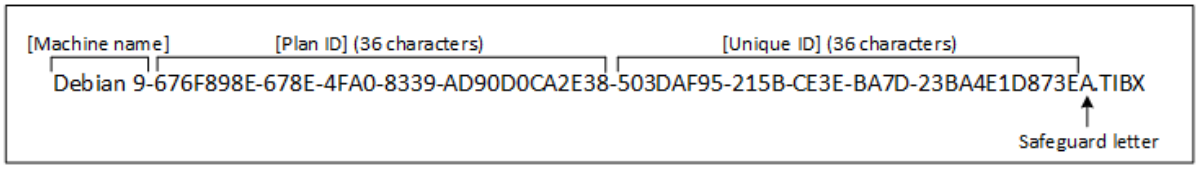
© Acronis International GmbH, 2003-2025

El nombre predeterminado para las copias de seguridad de la aplicación en la nube creadas por los agentes en la nube es `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

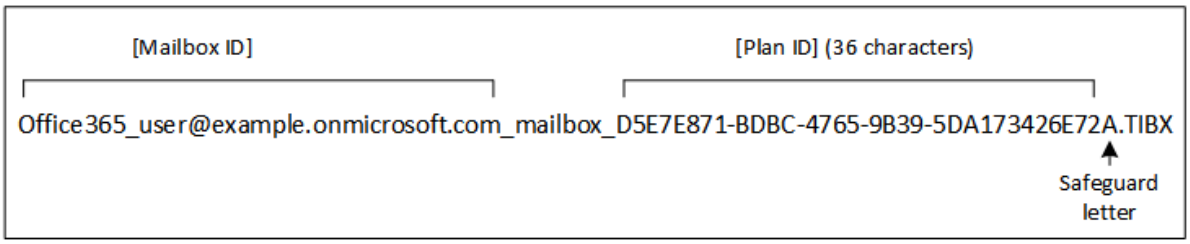
El nombre predeterminado consta de las siguientes variables:

- `[Machine Name]` Esta variable se sustituye por el nombre del equipo (el mismo nombre que aparece en la consola de Cyber Protect).
- `[Plan ID]`, `[Plan Id]` Estas variables se sustituyen por el identificador único del plan de protección. Este valor no cambia en caso de que se modifique el nombre del plan.
- `[Unique ID]` Esta variable se sustituye por el identificador único del equipo seleccionado. Este valor no se modifica si se cambia el nombre del equipo.
- `[Mailbox ID]` Esta variable se sustituye por el nombre principal del usuario (UPN) del buzón de correo.
- `[Resource Name]` Esta variable se sustituye por el nombre de origen de datos en la nube, como el nombre de usuario principal (UPN), la URL del sitio de SharePoint o el nombre de unidad compartida.
- `[Resource Type]` Esta variable se sustituye por el tipo de origen de datos en la nube, como `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` Esta variable se sustituye por el identificador único del origen de datos en la nube. Este valor no se modifica si se cambia el nombre del origen de datos de cloud.
- `"A"` es una letra de protección que se añade con el fin de impedir que el nombre acabe en un dígito.

El diagrama que aparece a continuación muestra el nombre del archivo de copia de seguridad predeterminado.



El diagrama que aparece a continuación muestra el nombre del archivo de copia de seguridad predeterminado para las copias de seguridad de buzón de correo de Microsoft 365 realizadas por un agente local.



Nombres sin variables

Si cambia el nombre del archivo de copia de seguridad a `MyBackup`, los archivos de copia de seguridad tendrán el aspecto que aparece a continuación. En ambos ejemplos se supone que hay

© Acronis International GmbH, 2003-2025

copias de seguridad incrementales diarias programadas a las 14:40, desde el 13 de septiembre de 2016.

Para el formato de la versión 12 con el esquema de copias de seguridad **Siempre incremental (un archivo)**:

```
MyBackup.tibx
```

Para el formato de la versión 12 con otros esquemas de copias de seguridad:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Uso de variables

Además de las variables que se usan de forma predeterminada, puede usar las siguientes variables:

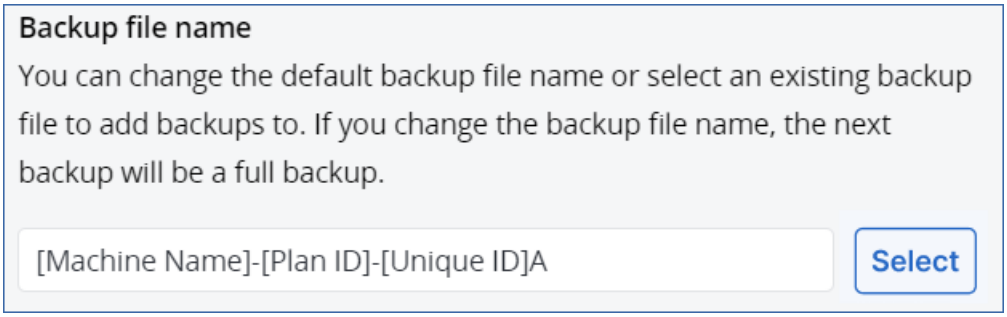
- La variable `[Plan name]`, que se sustituye por el nombre del plan de protección.
- La variable `[Virtualization Server Type]`, que se sustituye por "vmwesx" si Agent para VMware crea una copia de seguridad de los equipos virtuales o por "mshyperv" si Agente para Hyper-V crea una copia de seguridad de los equipos virtuales.

Si se seleccionan varios equipos o buzones de correo electrónico para la copia de seguridad, el nombre del archivo de copia de seguridad tiene que contener las variables `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]` o `[Resource Id]`.

Creación de copias de seguridad en un archivo de copias de seguridad existente

Puede configurar las copias de seguridad de una carga de trabajo para que se añadan a un archivo de copias de seguridad existente.

Esta opción podría ser útil, por ejemplo, cuando se aplica un plan de protección a un solo equipo, y tiene que eliminar este equipo de la consola de Cyber Protect, o bien desinstalar el agente junto con sus configuraciones. Después de añadir nuevamente el equipo o reinstalar el agente, puede forzar al plan de protección para que continúe haciendo copias de seguridad en el archivo original.



© Acronis International GmbH, 2003-2025

Para configurar las copias de seguridad de una carga de trabajo para que se añadan a un archivo de copia de seguridad existente

Cargas de trabajo que no son de nube a nube

1. En la pantalla **Todos los dispositivos**, haga clic en la carga de trabajo y luego en **Proteger**.
2. En la configuración del plan de protección, extienda el módulo **Copia de seguridad**.
3. Haga clic en **Opciones de copia de seguridad** y, a continuación, haga clic en **Modificar**.
4. En la pestaña **Nombre del archivo de la copia de seguridad**, haga clic en **Seleccionar**.
   El botón **Seleccionar** muestra las copias de seguridad de la ubicación seleccionada en la sección **Dónde guardar las copias de seguridad** del plan de protección.

   Nota
   El botón **Seleccionar** solo está disponible para aquellos planes de protección que se hayan creado para una única carga de trabajo y se hayan aplicado tan solo en esa.

5. Seleccione un archivo y luego haga clic en **Listo**.
6. Haga clic en **Listo** y luego haga clic en **Aplicar**.

Cargas de trabajo de la nube a la nube

1. En la pestaña **Gestión** > **Copias de seguridad de aplicaciones en la nube** , seleccione el plan.
2. Haga clic en **Editar** y luego en el ícono de engranaje junto al nombre del plan.
3. En la pestaña **Nombre de la copia de seguridad de archivos**, haga clic en **Seleccionar**.

   Nota
   El botón **Seleccionar** solo está disponible para los planes de copias de seguridad que se crean y aplican para una única carga de trabajo.

4. Seleccione un archivo de copia de seguridad y luego haga clic en **Listo**.
5. Haga clic en **Listo** y luego haga clic en **Guardar cambios**.

Formato de la copia de seguridad

La opción **Formato de la copia de seguridad** define el formato de las copias de seguridad creadas por el plan de protección. Esta opción está disponible únicamente para planes de protección que ya utilizan la versión 11 del formato de copias de seguridad. Si este es el caso, puede cambiar el formato de la copia de seguridad a la versión 12. Cuando cambie el formato de copia de seguridad a la versión 12, la opción deja de estar disponible.

- **Versión 11**
  El formato heredado que se conserva para permitir la compatibilidad con versiones anteriores.

© Acronis International GmbH, 2003-2025

Nota
No es posible realizar la copia de seguridad de Grupos de disponibilidad de bases de datos (DAG) con la versión 11 del formato de la copia de seguridad. La copia de seguridad de DAG solo es posible en el formato de la versión 12.

- **Versión 12**
  El formato de copia de seguridad que se introdujo en Acronis Backup 12 para realizar copias de seguridad y recuperaciones más rápido. Cada cadena de copias de seguridad (una copia de seguridad completa o diferencial y todas las copias de seguridad incrementales que dependen de ella) se guardan en un solo archivo TIBX.

Formato y archivos de copia de seguridad

En el caso de las ubicaciones de copia de seguridad que se puedan buscar con un administrador de archivos (como carpetas locales o de red), el formato de copia de seguridad determinará el número de archivos y su extensión. La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

	Siempre incremental (un archivo)	**Otros esquemas de copia de seguridad**
Formato de copia de seguridad **Versión 11**	Un archivo TIB y otro archivo de metadatos XML	Varios archivos TIB y un archivo de metadatos XML
Formato de copia de seguridad **Versión 12**	Un archivo TIBX por cadena de copia de seguridad (una copia de seguridad completa o diferencial y todas las copias de seguridad incrementales que dependan de ella). Si el tamaño de un archivo almacenado en una carpeta local o de red (SMB) sobrepasa los 200 GB, este se divide en archivos de 200 GB de manera predeterminada.	

Cambiar el formato de copia de seguridad a la versión 12 (TIBX)

Si cambia el formato de copia de seguridad de la versión 11 (formato TIB) a la 12 (formato TIBX):

- La siguiente copia de seguridad será completa.
- En el caso de las ubicaciones de copia de seguridad que se puedan buscar con un administrador de archivos (como carpetas locales o de red), se creará un nuevo archivo TIBX. El nuevo archivo llevará el nombre del archivo original con el sufijo **_v12A**.
- Solo se aplicarán reglas de retención y replicación a las copias de seguridad nuevas.
- Las copias de seguridad antiguas no se eliminarán y seguirán estando disponibles en la pestaña **Almacenamiento de la copia de seguridad**. Se pueden eliminar manualmente.
- Las copias de seguridad en el cloud antiguas no consumirán la cuota de **Almacenamiento en la nube**.
- Las copias de seguridad locales antiguas consumirán la cuota de **copia de seguridad local** hasta que las elimine manualmente.

© Acronis International GmbH, 2003-2025

Deduplicación en archivos comprimidos

El formato TIBX de las copias de seguridad de la versión 12 es compatible con la deduplicación en archivos comprimidos, que ofrece las siguientes ventajas:

- Tamaño de copia de seguridad reducido de forma importante, con deduplicación integrada a nivel de bloque para cualquier tipo de dato
- La gestión eficiente de enlaces fijos garantiza que no haya almacenamientos duplicados.
- Fragmentación basada en hashes

Nota
La deduplicación en archivos comprimidos está habilitada de forma predeterminada para todas las copias de seguridad en formato TIBX. No es necesario habilitarla en las opciones de copia de seguridad y no se puede deshabilitar.

La compatibilidad del formato de copia de seguridad en las diferentes versiones del producto

Para obtener información sobre la compatibilidad del formato de copia de seguridad, consulte este artículo de la base de conocimiento.

Validación de la copia de seguridad

La validación es una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad. Cuando esta opción está habilitada, cada copia de seguridad que crea el plan de protección se valida justo después de su creación a través del método de verificación de validaciones. Esta operación la realiza el agente de protección.

El valor predeterminado es el siguiente: **Deshabilitado**.

Si quiere obtener más información acerca de la validación por suma de comprobación, acceda a "Verificación de suma de comprobación" (p. 266).

Nota
En función de la configuración que elija su proveedor de servicios, es posible que la validación no esté disponible al realizar una copia de seguridad en el almacenamiento en la nube. La validación tampoco está disponible para las ubicaciones de copia de seguridad en nubes públicas.

Seguimiento de bloques modificados (CBT)

Esta opción es eficaz para las siguientes copias de seguridad:

- Copias de seguridad de disco de máquinas virtuales
- Copias de seguridad de disco de equipos físicos con Windows

© Acronis International GmbH, 2003-2025

- Copias de seguridad de bases de datos de Microsoft SQL Server
- Copias de seguridad de bases de datos de Microsoft Exchange Server

El valor predeterminado es el siguiente: **Habilitado**.

Esta opción determina si se usa el Seguimiento de bloques modificados (CBT) cuando se realiza una copia de seguridad incremental o diferencial.

La tecnología CBT acelera el proceso de copia de seguridad. Los cambios realizados en el disco o contenido de la base de datos se rastrean continuamente en el nivel del bloque. Cuando se inicia una copia de seguridad, los cambios se pueden guardar inmediatamente en esta.

Modo de copia de seguridad de clústeres

Nota
Esta función está disponible con el paquete Advanced Backup.

Estas opciones son eficaces para las copias de seguridad de nivel de la base de datos de Microsoft SQL Server y Microsoft Exchange Server.

Estas opciones son eficaces solo si se selecciona el propio clúster (Grupos de disponibilidad de Always On de Microsoft SQL Server [AAG] o el grupo de disponibilidad de base de datos de Microsoft Exchange Server [DAG]) para la copia de seguridad, en lugar de los nodos concretos o las bases de datos que tiene. Si selecciona elementos concretos del clúster, la copia de seguridad no será compatible con el clúster y solo se incluirán en la copia de seguridad las copias seleccionadas de los elementos.

Microsoft SQL Server

Esta opción determina el modo de copia de seguridad para los grupos de disponibilidad de Always On (AAG) de SQL Server. Para que se realice la operación, Agent for SQL debe estar instalado en todos los nodos de los AAG. Para obtener más información acerca de cómo realizar la copia de seguridad de los grupo de disponibilidad de Always On, consulte "Protección de los grupos de disponibilidad Always On (AAG)".

El valor predeterminado es el siguiente: **Si es posible, realice una réplica secundaria**.

Puede escoger una de las siguientes acciones:

- **Si es posible, realice una réplica secundaria**
  Si todas las réplicas secundarias están fuera de línea, se realizará una copia de seguridad de la principal. Realizar una copia de seguridad de la réplica principal podría ralentizar el funcionamiento de SQL Server, pero los datos se incluirán en la copia de seguridad con su estado más reciente.
- **Réplica secundaria**
  Si todas las réplicas secundarias están fuera de línea, no se podrá realizar la copia de seguridad. Realizar la copia de seguridad de las réplicas secundarias no afecta al rendimiento de SQL server

© Acronis International GmbH, 2003-2025

y le permite ampliar la ventana de copia de seguridad. No obstante, las réplicas pasivas podrían contener información que no está actualizada, ya que dichas réplicas frecuentemente se configuran para actualizarse asíncronamente (retrasado).

- **Réplica principal**

  Si la réplica principal está fuera de línea, no será posible realizar la copia de seguridad. Realizar una copia de seguridad de la réplica principal podría ralentizar el funcionamiento de SQL Server, pero los datos se incluirán en la copia de seguridad con su estado más reciente.

Independientemente del valor de esta opción, para garantizar la consistencia de la base de datos, el software omite las bases de datos que *no* tienen los estados **SINCRONIZADA** o **SINCRONIZANDO** cuando se inicia la copia de seguridad. Si se omiten todas las bases de datos, no se podrá realizar la copia de seguridad.

Microsoft Exchange Server

Esta opción determina el modo de copia de seguridad para los grupos de disponibilidad de base de datos de Exchange Server (DAG). Para que se realice la operación, Agente para Exchange debe estar instalado en todos los nodos del DAG. Para obtener más información acerca de cómo realizar la copia de seguridad de grupos de disponibilidad de base de datos, consulte "Protección de grupos de disponibilidad de base de datos (DAG)".

El valor predeterminado es el siguiente: **La copia pasiva si es posible.**

Puede escoger una de las siguientes acciones:

- **La copia pasiva si es posible.**

  Si todas las copias pasivas están fuera de línea, se realiza una copia de seguridad de la copia activa. Si realiza la copia de seguridad de la copia activa podría ralentizar el funcionamiento de Exchange Server, pero los datos se incluirían en la copia de seguridad en su estado más reciente.
- **Copia pasiva**

  Si todas las copias pasivas están fuera de línea, la copia de seguridad no se realizará correctamente. Realizar copias de seguridad de las copias pasivas no afecta el rendimiento de Exchange Server y le permite extender la ventana de copia de seguridad. Sin embargo, las copias pasivas pueden contener información que no este actualizada, porque dichas copias normalmente se configuran para actualizarse de forma asincrónica (retardada).
- **Copia activa**

  Si la copia activa está fuera de línea, la copia de seguridad no se realizará correctamente. Si realiza la copia de seguridad de la copia activa podría ralentizar el funcionamiento de Exchange Server, pero los datos se incluirían en la copia de seguridad en su estado más reciente.

Independientemente del valor de esta opción, para garantizar la consistencia de la base de datos, el software omite las bases de datos que *no* tienen los estados **BUENO** o **ACTIVO** cuando se inicia la copia de seguridad. Si se omiten todas las bases de datos, no se podrá realizar la copia de seguridad.

© Acronis International GmbH, 2003-2025

Tasa de compresión

Nota
Esta opción no está disponible para las copias de seguridad de la nube a la nube. La compresión de estas copias de seguridad está habilitada de forma predeterminada con un nivel fijo que corresponde al siguiente nivel **Normal**.

Esta opción define el tasa de compresión que se aplicará a los datos que se incluyen en la copia de seguridad. Los niveles disponibles son: **Ninguno**, **Normal**, **Alto**, **Máximo**.

El valor predeterminado es el siguiente: **Normal**.

Una tasa de compresión mayor implica que el proceso de copia de seguridad requiere más tiempo, pero que la copia de seguridad resultante ocupa menos espacio. Actualmente los niveles **Alto** y **Máximo** funcionan de forma similar.

El tasa de compresión de datos óptimo dependerá del tipo de datos que se incluyen en la copia de seguridad. Por ejemplo, ni siquiera la máxima compresión conseguirá reducir significativamente el tamaño de la copia de seguridad si esta contiene archivos esencialmente comprimidos, como .jpg, .pdf o .mp3. Sin embargo, los formatos como .doc o .xls se comprimirán correctamente.

Control de errores

Estas opciones le permiten que establezca como se manejarán los errores que puedan suceder durante la copia de seguridad.

Reintentar si se produce un error

El valor predeterminado es el siguiente: **Habilitado. Número de intentos: 30. Intervalo entre intentos: 30 segundos**.

Cuando se produce un error recuperable, Cyber Protect vuelve a intentar realizar la operación sin éxito. Puede establecer el número máximo de reintentos y el intervalo entre ellos. Si la operación no puede finalizar con éxito después del número máximo de reintentos, falla.

Para las copias de seguridad en una ubicación de red o en un almacenamiento en la nube (almacenamiento en Acronis Cloud o en un almacenamiento en la nube pública, como Amazon, Azure, Wasabi, compatible con S3 o Impossible Cloud), el manejo de errores depende del momento en que se produce el error.

Se ha producido un error al iniciar la copia de seguridad	Se ha producido un error durante una copia de seguridad en curso
El número de reintentos depende de la respuesta de la API de almacenamiento. Si la API devuelve una respuesta que se considera como reintentable (por ejemplo, el error "503 Servicio no disponible"),	El número de reintentos depende de la configuración de **Control de errores** que se configura en el plan de protección.

© Acronis International GmbH, 2003-2025

Se ha producido un error al iniciar la copia de seguridad	Se ha producido un error durante una copia de seguridad en curso
la operación podría tardar hasta dos horas en fallar. Normalmente, este escenario es más probable para un almacenamiento en la nube que para una ubicación de red.	Por ejemplo, 30 reintentos con un intervalo de 30 segundos entre cada uno.

Para las copias de seguridad en carpetas locales, la configuración **Control de errores** solo se aplica a los errores que ocurren durante una copia de seguridad en curso. Si ocurre un error al iniciar la copia de seguridad, la operación de copia de seguridad falla inmediatamente.

No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)

El valor predeterminado es el siguiente: **Habilitado**.

Cuando se habilite el modo silencioso, el programa manejará automáticamente las situaciones que requieran interacción del usuario (a excepción del manejo de sectores defectuosos que se definen con otra opción). Si una operación no puede continuar sin la acción del usuario, ésta fallará. Los detalles de la operación, incluyendo los errores, si los hubiera, pueden encontrarse en el registro de la operación.

Ignorar los sectores defectuosos

El valor predeterminado es el siguiente: **Deshabilitado**.

Cuando esta opción está deshabilitada, cada vez que el programa encuentre un sector defectuoso, se asignará a la actividad de copia de seguridad el estado **Interacción necesaria**. Para realizar una copia de seguridad de información válida en un disco que se está dañando rápidamente, habilite ignorar sectores defectuosos Se realizará una copia de seguridad del resto de los datos y podrá montar la copia de seguridad del disco resultante y extraer los archivos válidos a otro disco.

Nota
La opción de omitir sectores defectuosos no es compatible con Linux. Puede realizar copias de seguridad de sistemas Linux con sectores defectuosos en modo offline usando Bootable Media Builder en la versión in situ de Cyber Protect. Para usar Bootable Media Builder en la versión in situ necesita una licencia aparte. Póngase en contacto con el soporte técnico para obtener ayuda.

Reintentar si se produce un error durante la creación de instantáneas de VM

El valor predeterminado es el siguiente: **Habilitado. Número de intentos: 3. Intervalo entre intentos: 5 minutos.**

Cuando se produce un fallo al tomar una instantánea de un equipo virtual, el programa reintenta la operación fallida. Puede establecer el intervalo temporal y el número de intentos. Se detendrán los

© Acronis International GmbH, 2003-2025

intentos tan pronto como la operación se lleve a cabo correctamente O se realice el número de intentos especificados, lo que suceda primero.

Copias de seguridad incrementales/diferenciales rápidas

Esta opción es eficaz para las copias de seguridad incrementales y diferenciales a nivel de disco.

Esta opción no es efectiva (siempre está deshabilitada) para volúmenes formateados con los sistemas de archivos JFS, ReiserFS3, ReiserFS4, ReFS o XFS.

El valor predeterminado es el siguiente: **Habilitado**.

La copia de seguridad incremental o diferencial sólo captura los cambios en los datos. Para acelerar el proceso de copia de seguridad, el programa determina si un archivo ha cambiado por su tamaño y la fecha/hora en la que se guardó por última vez. Si deshabilita esta característica, el programa compara el contenido completo del archivo con el que esté almacenado en la copia de seguridad.

Filtros de archivo (inclusiones y exclusiones)

Puede utilizar filtros de archivo para incluir o excluir solo ciertos archivos y carpetas específicos en una copia de seguridad.

Los filtros de archivo están disponibles para las copias de seguridad de todo el equipo, de discos y de archivos, a menos que se indique lo contrario.

Los filtros de archivo no están disponibles con los sistemas de archivos XFS, JFS, exFAT ni ReiserFS4. Para obtener más información, consulte "Sistemas de archivos compatibles" (p. 525).

Los filtros de archivo no se aplican a discos dinámicos (volúmenes LVM o LDM) de máquinas virtuales con una copia de seguridad realizada, por ejemplo, por Agente para VMware, Agente para Hyper-V o Agente para Scale Computing en el modo sin agente.

Tipos de filtro de archivo

Los filtros de archivo son de los siguientes tipos:

- Filtros de inclusión (**Incluyen solo los archivos que cumplan los siguientes criterios**)
  Si especifica `C:\File.exe` en un filtro de inclusión, solo se incluirá este archivo en la copia de seguridad, aunque seleccione copia de seguridad de **Todo el equipo**. Para obtener más información, consulte "Ejemplos de filtros" (p. 609).

  Nota
  Este filtro no es compatible con las copias de seguridad de nivel de archivo de la **versión 11** que no se almacenan en el almacenamiento de la nube.

- Filtros de exclusión (**Excluyen los archivos que cumplan los siguientes criterios**)
  Si especifica `C:\File.exe` en el filtro de exclusión, este archivo se omitirá en el proceso de copia de seguridad, aunque seleccione copia de seguridad de **Todo el equipo**.

© Acronis International GmbH, 2003-2025

Valores de filtro de archivos

En un filtro de archivos, puede utilizar los siguientes valores:

- Nombre de la carpeta o archivo

  Especifique el nombre del archivo o carpeta, como por ejemplo `Document.txt`. Se seleccionarán todos los archivos y carpetas con ese nombre.
- Ruta completa a un archivo o carpeta

  Especifique la ruta completa hasta el archivo o carpeta, empezando por la letra de unidad de disco (al realizar copias de seguridad de datos en Windows) o del directorio raíz (al hacer copias de seguridad de datos en Linux o macOS). En Windows, Linux y macOS, puede utilizar barras diagonales (como en `C:/Temp/File.tmp`). En Windows, también puede usar las tradicionales barras inversas (como en `C:\Temp\File.tmp`).

  Importante

  Si el sistema operativo del equipo con copia de seguridad no se detecta durante una copia de seguridad a nivel de disco, los filtros de archivo con rutas completas no funcionarán. Para un filtro de exclusión, aparecerá una advertencia. Si hay un filtro de inclusión, la copia de seguridad fallará.

  Un ejemplo de ruta completa a un archivo es `C:\Temp\File.tmp`. Si el sistema operativo no se detecta correctamente, un filtro de ruta completa que incluya la letra de unidad o el directorio raíz, por ejemplo `C:\Temp\File.tmp` o `C:\Temp\*`, generará una advertencia o un error.

  Un filtro que no emplee la letra de unidad ni el directorio raíz (por ejemplo, `Temp\*` o `Temp\File.tmp`) o que empiece con un asterisco (por ejemplo, `*C:\`) no generará una advertencia o un error. Sin embargo, si el sistema operativo no se detecta correctamente, los filtros no funcionarán de todos modos.

Comodines

Tanto con los nombres de archivos o carpetas como con las rutas de archivos o carpetas, puede utilizar los siguientes caracteres comodín:

- Asterisco (*)

  El asterisco representa a cero o más caracteres.

  Por ejemplo, `Doc*.txt` coincide con los archivos `Doc.txt` y `Document.txt`.
- Asterisco doble (**)

  El asterisco doble representa a cero o más caracteres, incluido el carácter de la barra diagonal o inversa.

  Por ejemplo, `**/Docs/**.txt` coincide con todos los archivos .txt en todas las subcarpetas de todas las carpetas llamadas `Docs`.

  Solo puede utilizar el comodín del doble asterisco para copias de seguridad en el formato de la versión 12.
- Signo de interrogación (?)

© Acronis International GmbH, 2003-2025

El signo de interrogación representa solo un carácter.

Por ejemplo, `Doc?.txt` coincide con los archivos `Doc1.txt` y `Docs.txt`, pero no con los archivos `Doc.txt` o `Doc11.txt`.

Nota

Utilice el comodín de signo de interrogación si el nombre del archivo o de la carpeta incluye una coma o un punto y coma. La coma y el punto y coma se interpretan como delimitadores y dividirán el filtro en dos partes. Por ejemplo, si desea utilizar la carpeta `MyCompany,Inc` en un filtro, utilice `MyCompany?Inc` al especificar el valor del filtro. De lo contrario, creará dos filtros separados, como se muestra a continuación:

- `MyCompany`
- `Inc`

Configuración de filtros de archivo

Puede configurar los filtros de archivo en el plan de protección.

Pasos para configurar los filtros de archivo

1. En un plan de protección, expanda el módulo **Copia de seguridad**.
2. En **Opciones de copia de seguridad**, haga clic en **Modificar**.
3. Seleccione **Filtros de archivo (inclusiones y exclusiones)**.
4. Configure los filtros de archivo.

   Puede configurar un filtro (inclusión o exclusión) o ambos. El filtro de exclusión tiene prioridad sobre el filtro de inclusión. Por ejemplo, si especifica `C:\File.exe` en ambos filtros, `C:\File.exe` se omitirá durante una copia de seguridad.

   El uso de filtros no afecta la selección de archivos específicos en el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**). Para obtener más información, consulte "Ejemplos de filtros" (p. 609).

   Nota

   Si un nombre o una ruta incluyen una coma o un punto y coma, reemplácelos por el comodín de signo de interrogación (?). La coma y el punto y coma se interpretan como delimitadores y dividirán el filtro en dos partes. Para obtener más información, consulte " Comodines" (p. 608).
5. Haga clic en **Listo**.
6. Guarde el plan de protección.

Como resultado, los filtros de archivos se aplicarán al ámbito que se configura en la sección **Qué incorporar en la copia de seguridad** del plan de protección.

Ejemplos de filtros

Las tablas siguientes muestran ejemplos de configuraciones de filtro de archivos.

© Acronis International GmbH, 2003-2025

Filtro de inclusión			
Qué incorporar en la copia de seguridad	**Valor del filtro**	**El archivo de copia de seguridad contiene:**	**Descripción**
`C:\Folder1` (contiene `MyFile.txt` y otros archivos) `C:\Folder2` (contiene `MyDocument.txt` y otros archivos)	`MyFile.txt` `C:\Folder2\MyDocument.txt`	`C:\Folder1\MyFile.txt` `C:\Folder2\MyDocument.txt`	El filtro de inclusión coincide con el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**). Solo los archivos que se especifican en el filtro de inclusión están presentes en las carpetas de copia de seguridad. Puede configurar un filtro de archivos mediante nombres de archivos o carpetas o mediante rutas de archivos o carpetas.
`C:\Folder1` (contiene varios archivos)	`C:\Folder2\MyDocument.txt`	`C:\Folder1` (como una carpeta vacía)	El filtro de inclusión no coincide con el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**).

© Acronis International GmbH, 2003-2025

Filtro de inclusión			
Qué incorporar en la copia de seguridad	**Valor del filtro**	**El archivo de copia de seguridad contiene:**	**Descripción**
			`Folder1` se ha incluido en la copia de seguridad, pero está vacía porque no contiene el archivo del filtro de inclusión. El archivo del filtro de inclusión no se ha incluido en la copia de seguridad porque no forma parte del ámbito de la copia de seguridad.
`C:\Folder1` (contiene `MyFile.txt` y otros archivos) `C:\Folder2` (contiene `MyDocument.txt` y otros archivos)	`MyFile.txt`	`C:\Folder1\MyFile.txt` `C:\Folder2` (como una carpeta vacía)	El filtro de inclusión coincide parcialmente con el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**). `Folder1` se ha incluido en la copia de seguridad, pero solo contiene el archivo que se especifica en el filtro de

© Acronis International GmbH, 2003-2025

Filtro de inclusión			
Qué incorporar en la copia de seguridad	**Valor del filtro**	**El archivo de copia de seguridad contiene:**	**Descripción**
			inclusión. `Folder2` se ha incluido en la copia de seguridad, pero está vacía porque no contiene el archivo del filtro de inclusión.
`C:\Folder1` (contiene `MyFile.txt` y otros archivos) `C:\Folder2\MyDocument.txt`	`MyFile.txt`	`C:\Folder1\MyFile.txt` `C:\Folder2\MyDocument.txt`	`Folder1` se ha incluido en la copia de seguridad, pero solo contiene el archivo que se especifica en el filtro de inclusión. También se ha realizado una copia de seguridad del segundo archivo seleccionado. El uso de filtros no afecta la selección de archivos específicos en el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**).

© Acronis International GmbH, 2003-2025

Filtro de exclusión			
Qué incorporar en la copia de seguridad	**Valor del filtro**	**El archivo de copia de seguridad contiene:**	**Descripción**

`C:\Folder1` (contiene `MyFile.txt` y otros archivos)
 	
`C:\Folder2` (contiene `MyDocument.txt` y otros archivos)
	`MyFile.txt`
	
	`C:\Folder2\MyDocument.txt`
		`C:\Folder1`: todos los archivos excepto `MyFile.txt`
		
		`C:\Folder2`: todos los archivos excepto `MyDocument.txt`
			El filtro de exclusión coincide con el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**).
			
			Faltan los archivos que se especifican en el filtro de exclusión en las carpetas de las que se realizó la copia de seguridad.
			
			Puede configurar un filtro de archivos mediante nombres de archivos o carpetas o mediante rutas de archivos o carpetas.

`C:\Folder1` (contiene varios archivos)	`C:\Folder2\MyDocument.txt`	`C:\Folder1`: todos los archivos	El filtro de exclusión no coincide con el ámbito de la copia de seguridad (**Qué**

© Acronis International GmbH, 2003-2025

Filtro de exclusión			
Qué incorporar en la copia de seguridad	**Valor del filtro**	**El archivo de copia de seguridad contiene:**	**Descripción**
			incorporar en la copia de seguridad). Se ha realizado una copia de seguridad de todo el contenido de `Folder1`.
`C:\Folder1` (contiene `MyFile.txt` y otros archivos) `C:\Folder2` (contiene `MyDocument.txt` y otros archivos)	`MyFile.txt`	`C:\Folder1`: todos los archivos excepto `MyFile.txt` `C:\Folder2`: todos los archivos	El filtro de inclusión coincide parcialmente con el ámbito de la copia de seguridad (**Qué incorporar en la copia de seguridad**). `Folder1` se ha incluido en la copia de seguridad, pero falta el archivo que se especifica en el filtro de exclusión. Se ha realizado una copia de seguridad de todo el contenido de `Folder2`.
`C:\Folder1` (contiene `MyFile.txt` y otros archivos)	`MyFile.txt`	`C:\Folder1`: todos los archivos excepto `MyFile.txt`	`Folder1` se ha incluido en la copia de

© Acronis International GmbH, 2003-2025

Filtro de exclusión			
Qué incorporar en la copia de seguridad	**Valor del filtro**	**El archivo de copia de seguridad contiene:**	**Descripción**
`C:\Folder2\MyDocument.txt`		`C:\Folder2\MyDocument.txt`	seguridad, pero falta el archivo que se especifica en el filtro de exclusión. Se realiza una copia de seguridad del segundo archivo seleccionado porque no coincide con el filtro de exclusión.

Instantánea de la copia de seguridad a nivel de archivo

Esta opción solo sirve para la copia de seguridad a nivel de archivo.

Esta opción define si se hace una copia de seguridad archivo por archivo o si se toma una instantánea de los datos.

Nota
A los archivos que no estén almacenados en redes compartidas se le realizará la copia de seguridad uno a uno.

El valor predeterminado es el siguiente:

- Si se han seleccionado únicamente equipos que se ejecutan en Linux para realizar la copia de seguridad: **No se crea una instantánea.**
- De lo contrario: **Se crea una instantánea si es posible.**

Puede seleccionar una de las siguientes opciones:

- **Crear una instantánea si es posible**
  Realizar la copia de seguridad directamente si no es posible tomar una instantánea.
- **Siempre crear una instantánea**
  La instantánea permite la copia de seguridad de todos los archivos, inclusive los archivos abiertos para accesos exclusivos. Los archivos se incluirán en la copia de seguridad al mismo momento determinado. Seleccione esta configuración sólo si los factores son críticos, es decir: la copia de

© Acronis International GmbH, 2003-2025

seguridad sin tomar una instantánea no tiene sentido. Si no se puede tomar una instantánea, la copia de seguridad fallará.

- **No crear una instantánea**

  Siempre realizar la copia de seguridad directamente. El intento de copia de seguridad de archivos que están abiertos para acceso exclusivo generará un error de lectura. Los archivos en la copia de seguridad puede que no sean consistentes en el tiempo.

Datos forenses

Los virus, el malware y el ransomware pueden llevar a cabo actividades maliciosas como robar o cambiar datos. Es posible que haya que investigar estas actividades, pero esto se puede hacer únicamente si hay pruebas digitales. Sin embargo, las pruebas digitales, al igual que el rastro de archivos o actividad, pueden borrarse o el equipo en el que se ha completado la actividad maliciosa puede dejar de estar disponible.

Las copias de seguridad con datos forenses permiten a los investigadores analizar áreas del disco que no suelen incluirse en una copia de seguridad normal del disco. Al habilitar la opción de copia de seguridad **Datos forenses**, puede recopilar las siguientes pruebas digitales que pueden utilizarse en investigaciones forenses:

- Instantáneas del espacio en disco no utilizado
- Volcados de memoria
- Instantáneas de los procesos en ejecución

Las copias de seguridad con datos forenses se certifican automáticamente.

La opción copia de seguridad de **Datos forenses** está disponible para copias de seguridad de **Todo el equipo** de recursos informáticos de Windows que ejecutan los siguientes sistemas operativos:

- Windows 8.1 y posterior
- Windows Server 2012 R2 y posterior

Las copias de seguridad con datos forenses no se encuentran disponibles para los siguientes recursos informáticos:

- Recursos informáticos conectados a la red mediante una VPN y sin acceso directo a Internet.
- Recursos informáticos con discos cifrados por BitLocker.

Las copias de seguridad con datos forenses son compatibles con las siguientes ubicaciones de copia de seguridad:

- Almacenamiento en la nube
- Carpeta de red
- Carpeta local

© Acronis International GmbH, 2003-2025

Nota
La carpeta local solo es compatible con las unidades externas que están conectadas al recurso informático respaldado a través de USB.
Los discos dinámicos locales no se admiten como ubicaciones para copias de seguridad de datos forenses.

Proceso de copia de seguridad forense

Durante una copia de seguridad forense, se realizan las siguientes operaciones:

1. Se captura un volcado de memoria en bruto y una lista de procesos en ejecución.
2. El recurso informático respaldado se reinicia y se abre la interfaz del dispositivo de arranque.
3. Se crea una copia de seguridad que incluye tanto el espacio utilizado como el espacio sin asignar.
4. Los discos de los que se ha realizado una copia de seguridad están certificados.
5. El sistema operativo del recurso informático se reinicia y se ejecutan otras operaciones configuradas. Por ejemplo, replicación, retención, validación.

Configuración de la recopilación de datos forenses

Puede configurar la recopilación de datos forenses mediante las opciones de copia de seguridad en un plan de protección.

Pasos para configurar la recopilación de datos forenses

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un recurso informático y haga clic en **Proteger**.
3. Haga clic en **Agregar plan** y, a continuación, haga clic en **Crear plan** > **Plan de protección**.
4. En el plan de protección, asegúrese de que el módulo **Copia de seguridad** esté habilitado y expandido.
5. En **Qué incorporar en la copia de seguridad**, seleccione **Todo el equipo**.
6. Para configurar la recopilación de datos forenses, en **Opciones de copia de seguridad**, haga clic en **Modificar**.
   a. Haga clic en **Datos forenses**.
   b. Active el interruptor **Recopilar datos forenses**.
   c. Haga clic en **Listo**.

Nota
No puede cambiar la configuración de los datos forenses después de aplicar el plan de protección. Para usar diferentes configuraciones de datos forenses, cree y aplique un nuevo un plan de protección.

© Acronis International GmbH, 2003-2025

7. En **Dónde guardar las copias de seguridad**, especifique una ubicación de copia de seguridad.
8. En **Planificación**, configure la planificación del plan.
9. Para configurar la contraseña de cifrado, en **Cifrado**, haga clic en **Especifique una contraseña**.
   a. Escriba y confirme la contraseña.
   b. Haga clic en **Aceptar**.
10. Haga clic en **Crear**.

Como resultado, se crea y aplica un plan de protección. Durante la copia de seguridad, se captura un volcado de memoria y una instantánea de los procesos en ejecución. Después de que se complete la copia de seguridad, puede recuperar los datos forenses y analizarlos.

Importante
El volcado de memoria puede incluir datos confidenciales, como contraseñas.

Recuperación de datos forenses

Puede recuperar datos forenses de una copia de seguridad descargando o recuperando esos datos.

Pasos para recuperar datos forenses

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione una ubicación de copia de seguridad que sea compatible con los archivos de copia de seguridad con datos forenses.
3. Seleccione un archivo de copia de seguridad que contenga datos forenses y, a continuación, haga clic en **Mostrar copias de seguridad**.
4. Seleccione una copia de seguridad (punto de recuperación) que contenga datos forenses y, a continuación, haga clic en **Recuperar**.
5. [Para descargar o recuperar solo archivos de datos forenses] Haga clic en **Datos forenses**.
   Se muestran los archivos que contienen datos forenses.
   a. [Para descargar archivos] Seleccione uno o más archivos y, a continuación, haga clic en **Descargar**.
   b. [Para recuperar archivos] Seleccione uno o más archivos y, a continuación, haga clic en **Recuperar**.

   Nota
   En la consola de Cyber Protect, no puede descargar archivos de más de 100 MB. Normalmente, el archivo de volcado de memoria (`raw.dmp`) es más grande. Puede recuperar este archivo y luego copiarlo.
   Puede usar el volcado de memoria con software forense de terceros. Por ejemplo, puede usar Volatility Framework (https://www.volatilityfoundation.org/) para obtener un mayor análisis de la memoria.

6. [Para recuperar la copia de seguridad completa] Haga clic en **Todo el equipo**.

© Acronis International GmbH, 2003-2025

a. Configure las opciones de recuperación.

b. Haga clic en **Iniciar recuperación**.

c. Para confirmar que desea sobrescribir los discos del equipo de destino, haga clic en **Iniciar recuperación**.

Importante
Para garantizar que no se realicen cambios en el disco durante el proceso de arranque, el equipo recuperado no tiene capacidad de arranque.

Visualización de archivos de copia de seguridad que contienen datos forenses

Puede comprobar qué archivos de copia de seguridad contienen datos forenses en la consola de Cyber Protect.

Pasos para ver los archivos de copia de seguridad que contienen datos forenses en contenedores

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad**.
2. Seleccione una ubicación de copia de seguridad que sea compatible con los archivos de copia de seguridad con datos forenses.
3. Haga clic en el icono de engranaje en la esquina superior derecha de la tabla y, a continuación, seleccione **Datos forenses**.
   Aparece la columna **Datos forenses**.
4. Haga clic en el nombre de la columna para ordenar los archivos de copia de seguridad según la presencia de datos forenses.

Certificación de copias de seguridad con datos forenses

Para asegurarse de que una copia de seguridad con datos forenses es exactamente igual que el contenido que se incluyó y que no se ha alterado nada, el módulo de copia de seguridad ofrece la certificación de las copias de seguridad con datos forenses.

Cómo funciona

La certificación permite demostrar que un disco con datos forenses es auténtico y que no ha cambiado desde su copia de seguridad.

Durante una copia de seguridad, el agente calcula los códigos de cifrado de los discos de los que se ha realizado la copia de seguridad, crea un árbol de cifrado, guarda el árbol en la copia de seguridad y envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización guarda la raíz del árbol de cifrado en la base de datos de cadenas de bloques de Ethereum para garantizar que este valor no cambie.

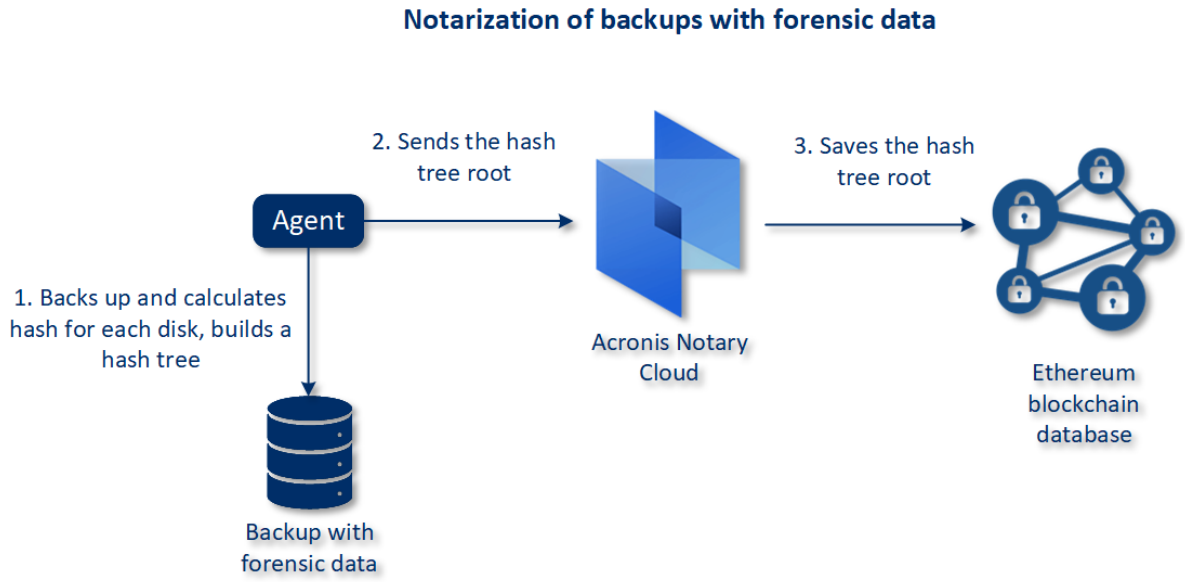
Al verificar la autenticidad del disco con datos forenses, el agente calcula su cifrado y lo compara con el almacenado en el árbol de cifrado de la copia de seguridad. Si los hashes no coinciden, se

© Acronis International GmbH, 2003-2025

considerará que el disco no es auténtico. De lo contrario, la autenticidad del disco queda garantizada por el árbol de cifrado.

Para verificar que el propio árbol de cifrado no se haya visto alterado, el agente envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización lo compara con el almacenado en la base de datos de cadenas de bloques. Si los hashes coinciden, se garantiza que el disco seleccionado es auténtico. De lo contrario, el software muestra un mensaje para indicar que el disco no es auténtico.

En el esquema que aparece a continuación se muestra brevemente el proceso de certificación de copias de seguridad con datos forenses.



Para comprobar manualmente la copia de seguridad del disco certificada, puede obtener su certificado y seguir el proceso de verificación que viene con él mediante la herramienta tibxread.

Obtener el certificado de copias de seguridad con datos forenses

Para obtener el certificado de una copia de seguridad con datos forenses de la consola, lleve a cabo los siguientes pasos:

1. Vaya a **Almacenamiento de la copia de seguridad** y seleccione la copia de seguridad con datos forenses.
2. Recupere todo el equipo.
3. El sistema abre la vista **Asignación de discos**.
4. Haga clic en el icono **Obtener certificado** del disco.
5. El sistema generará el certificado y este aparecerá en la nueva ventana de navegador que se abrirá. Debajo de certificado, verá las instrucciones necesarias para comprobar manualmente una copia de seguridad del disco certificada.

© Acronis International GmbH, 2003-2025

Herramienta "tibxread" para obtener datos incluidos en una copia de seguridad

Cyber Protection ofrece la herramienta llamada `tibxread`, que sirve para comprobar manualmente la integridad de los datos incluidos en una copia de seguridad. Con esta herramienta, puede obtener los datos de una copia de seguridad y calcular el hash del disco especificado. Además, se instala automáticamente con los siguientes componentes: Agente para Windows, Agente para Linux y Agente para Mac.

La ruta de instalación es la misma carpeta que tiene el agente (por ejemplo, `C:\Program Files\BackupClient\BackupAndRecovery`).

Las ubicaciones admitidas son las siguientes:

- El disco local.
- La carpeta de red (CIFS/SMB) a la que se puede acceder sin credenciales.
  En el caso de que la carpeta de red esté protegida por una contraseña, puede montar la carpeta de red en la carpeta local mediante las herramientas del sistema operativo, y luego la carpeta local como fuente para esta herramienta.
- El almacenamiento en la cloud
  Debe proporcionar la URL, el puerto y el certificado. La URL y el puerto se pueden obtener de la clave del registro de Windows, o de los archivos de configuración en equipos Linux o Mac.
  Para Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Para Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Para macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  El certificado se puede encontrar en las siguientes ubicaciones:
  Para Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Para Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```


© Acronis International GmbH, 2003-2025

Para macOS:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

La herramienta cuenta con los siguientes comandos:

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

Enumera los puntos de recuperación de una copia de seguridad.

RESUMEN:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

Plantilla de salida:

```
GUID Date Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid>: GUID de copia de seguridad.

<date>: fecha de creación de la copia de seguridad. El formato es "DD.MM.AAAA HH24:MM:SS". En la zona horaria local predeterminada (se puede cambiar mediante la opción --utc).

Ejemplo de salida:

```
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

Enumera el contenido de un punto de recuperación.

© Acronis International GmbH, 2003-2025

RESUMEN:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Plantilla de salida:

```
Disk Size Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number>: identificador del disco.

<size>: tamaño en bytes.

<notarization_status>: se pueden dar los siguientes estados: Sin certificación, Certificada y Siguiente copia de seguridad.

Ejemplo de salida:

```
Disk Size Notary status
-------- ------ --------------
1 123123465798 Notarized
2 123123465798 Notarized
```

get content

Escribe contenido del disco especificado del punto de recuperación en la salida estándar.

RESUMEN:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
```


© Acronis International GmbH, 2003-2025

```
--log=PATH
--progress
```

calculate hash

Calcula el hash del disco especificado en el punto de recuperación usando el algoritmo SHA-2 (256 bits) y lo escribe en la salida estándar.

RESUMEN:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Descripción de la opción

Opción	Descripción
--arc=BACKUP_NAME	Nombre del archivo de la copia de seguridad que puede obtener de las propiedades de la copia de seguridad en la consola de Cyber Protect. El archivo de la copia de seguridad se debe especificar con la extensión .tibx.
--backup=RECOVERY_POINT_ID	Identificador del punto de recuperación
--disk=DISK_NUMBER	Número del disco (el mismo que se escribió en la salida del comando "get content")

--loc=URI	URI de la ubicación de una copia de seguridad. Los posibles formatos de la opción "--loc" son:
	• Nombre de la ruta local (Windows)
	`c:/upload/backups`
	• Nombre de la ruta local (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Almacenamiento en la nube

© Acronis International GmbH, 2003-2025

	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]` `<IP_address>`: puede encontrarla en la clave de registro en Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri `<path_to_certificate>`: ruta al archivo del certificado para acceder a Cyber Protect Cloud. Por ejemplo, en Windows este certificado se encuentra en `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt` donde <username> es su nombre de cuenta para acceder a Cyber Protect Cloud.
--log=PATH	Habilita que se pueda escribir en los registros mediante la RUTA especificada (únicamente la ruta local, el formato es el mismo que para el parámetro `--loc=URI`). El nivel de registro es DEPURACIÓN.
--password=PASSWORD	Contraseña de cifrado para su copia de seguridad. Si la copia de seguridad no está cifrada, deje este valor vacío.

--raw	Oculta los encabezados (2 primeras filas) de la salida del comando. Se usa cuando se debe transmitir la salida del comando.
	Ejemplo de salida sin "`--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`
	Salida con "`--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	Muestra fechas en UTC.

--progress	Muestra el progreso de la operación.
	Por ejemplo:
	`1 %`
	`2 %`
	`3 %`
	`4 %`
	`...`
	`100 %`

Truncamiento de registros

Esta opción funciona para las copias de seguridad de bases de datos de Microsoft SQL Server y para las copias de seguridad a nivel de disco con la copia de seguridad de aplicaciones de Microsoft SQL Server habilitada.

© Acronis International GmbH, 2003-2025

La opción define si los registros de transacciones de SQL Server se truncan antes de tomar una instantánea al comienzo de la operación de copia de seguridad.

El valor predeterminado es el siguiente: **Habilitado**.

Cuando está opción está habilitada, una base de datos solo se puede recuperar a un momento específico de una copia de seguridad que haya creado Cyber Protection.

Nota
Deshabilite esta opción si realiza copias de seguridad de los registros de transacción usando el motor nativo de copia de seguridad de Microsoft SQL Server.

Toma de instantáneas de LVM

Esta opción solo sirve para los equipos físicos.

Esta opción solo sirve para la copia de seguridad a nivel de disco de los volúmenes gestionados por Logical Volume Manager (LVM) de Linux. Dichos volúmenes también se llaman volúmenes lógicos.

Esta opción define cómo se toma una instantánea de un volumen lógico. El software de copia de seguridad puede hacerlo por sí mismo o recurrir a Logical Volume Manager (LVM) de Linux.

El valor predeterminado es el siguiente: **Con el software de copia de seguridad**.

- **Con el software de copia de seguridad**. Los datos de la instantánea se guardan, principalmente, en RAM. La copia de seguridad es más rápida y no se necesita espacio sin asignar en el grupo del volumen. Por lo tanto, le recomendamos cambiar el valor predeterminado solo si experimenta problemas al crear copias de seguridad de volúmenes lógicos.
- **Con LVM**. La instantánea se almacena en espacio no asignado del grupo del volumen. Si falta espacio no asignado, la instantánea la realizará el software de copia de seguridad.

La instantánea se utiliza solo durante la operación de copia de seguridad y se elimina automáticamente cuando se completa dicha operación. No se conservan archivos temporales.

Puntos de montaje

Esta opción solo se aplica en Windows a la copia de seguridad a nivel de archivos de un origen de datos que incluye volúmenes montados o volúmenes compartidos del clúster.

Nota
Para Linux y macOS, se ignorará la opción **Puntos de montaje de la copia de seguridad** y el comportamiento será el siguiente:

- Los datos en los puntos de montaje "locales", como los discos locales, las unidades USB, etc., siempre se incluirán en la copia de seguridad.
- Los datos en los puntos de montaje "remotos", como las acciones CIFS/NFS, etc., nunca se incluirán en la copia de seguridad.

© Acronis International GmbH, 2003-2025

Esta opción es eficaz solo cuando selecciona realizar una copia de seguridad a una carpeta que se encuentra en un nivel superior en la jerarquía que el punto de montaje. (Un punto de montaje es una carpeta que posee un volumen adicional que está conectado lógicamente.)

- Si dicha carpeta (o carpeta principal) se selecciona para la copia de seguridad y la opción **Puntos de montaje** está seleccionada, todos los archivos en el volumen montado se incluirán en la copia de seguridad. Si la opción **Puntos de montaje** está deshabilitada, el punto de montaje en la copia de seguridad estará vacío.

  Durante la recuperación de una carpeta principal, el contenido del punto de montaje se recuperará o no según si la opción para la recuperación de **Puntos de montaje** está habilitada o deshabilitada.
- Si selecciona un punto de montaje directamente o selecciona cualquier carpeta dentro del volumen montado, las carpetas seleccionadas se considerarán como carpetas normales. Se incluirán en la copia de seguridad sin importar el estado de la opción **Puntos de montaje** y se recuperarán sin importar el estado de la opción para la recuperación de **Puntos de montaje**.

El valor predeterminado es el siguiente: **Deshabilitado**.

Nota
Puede realizar copias de seguridad de equipos virtuales de Hyper-V en un volumen compartido del clúster al realizar la copia de seguridad de los archivos necesarios o de todo el volumen con la copia de seguridad a nivel de archivo. Solo apague los equipos virtuales para asegurarse que se incluyen en la copia de seguridad en el estado consistente.

Ejemplo

Supongamos que la carpeta **C:\Datos1** es un punto de montaje para el volumen montado. El volumen contiene las carpetas **Carpeta1** y **Carpeta2**. Puede crear un plan de protección para realizar la copia de seguridad a nivel de archivos de sus datos.

Si selecciona la casilla de verificación para el volumen C y habilita la opción **Puntos de montaje**, la carpeta **C:\Datos1** en su copia de seguridad contendrá la **Carpeta1** y **Carpeta2**. Al recuperar los datos incluidos en la copia de seguridad, tenga en cuenta de utilizar adecuadamente la opción para la recuperación de **Puntos de montaje**.

Si selecciona la casilla de verificación para el volumen C y deshabilita la opción **Puntos de montaje**, la carpeta **C:\Datos1** en su copia de seguridad estará vacía.

Si selecciona la casilla de verificación para la carpeta **Datos1**, **Carpeta1** o **Carpeta2**, las carpetas marcadas se incluirán en la copia de seguridad como carpetas normales, sin importar el estado de la opción de los **Puntos de montaje**.

Instantánea multivolumen

Esta opción sirve para las copias de seguridad de equipos físicos que ejecutan Windows o Linux.

Esta opción se aplica a la copia de seguridad de nivel del disco. Esta opción también se aplica a la copia de seguridad a nivel de archivo cuando se realiza una copia de seguridad a nivel de archivo al

© Acronis International GmbH, 2003-2025

tomar una instantánea. (La opción "Instantánea de la copia de seguridad a nivel de archivo" determina si se tomará una instantánea durante la copia de seguridad a nivel de archivo).

Esta opción determina si se tomarán las instantáneas de varios volúmenes al mismo tiempo o una a una.

El valor predeterminado es el siguiente:

- Si se selecciona al menos un equipo que ejecute Windows para la copia de seguridad: **Habilitado**.
- De lo contrario: **Deshabilitado**.

Cuando esta opción está habilitada, se crean simultáneamente instantáneas de todos los volúmenes de los que se hace la copia de seguridad. Utilice esta opción para crear una copia de seguridad consistente en el tiempo de datos que abarcan varios volúmenes, por ejemplo, para una base de datos de Oracle.

Cuando esta opción está deshabilitada, las instantáneas de los volúmenes se toman una después de la otra. Como resultado, si los datos abarcan varios volúmenes, puede que la copia de seguridad obtenida no sea consistente.

Recuperación con un clic

Nota
Esta función está disponible con el paquete Advanced Backup.

Con la recuperación con un clic, puede recuperar automáticamente una copia de seguridad del disco de su equipo Windows o Linux. La copia de seguridad puede ser de todo el equipo o de discos o volúmenes específicos del equipo. Se admiten equipos con arranque seguro y cifrado BitLocker.

Recuperación con un clic admite las siguientes operaciones:

- Recuperación automática desde la copia de seguridad más reciente
- Recuperación de una copia de seguridad específica (también conocida como punto de recuperación) dentro del archivo de copia de seguridad

Recuperación con un clic admite los siguientes tipos de almacenamiento de copias de seguridad:

- Secure Zone
- Carpeta de red
- Almacenamiento en la nube

© Acronis International GmbH, 2003-2025

Importante
Suspenda el cifrado por BitLocker hasta el próximo reinicio de su equipo cuando realice cualquiera de las siguientes operaciones:

- Crear, modificar o eliminar Secure Zone.
- Habilitar o deshabilitar Startup Recovery Manager.
- [Solo si Startup Recovery Manager no estaba ya habilitado] Ejecutar la primera copia de seguridad después de habilitar la recuperación con un clic en el plan de protección. Esta operación habilita Startup Recovery Manager automáticamente.
- Actualizar Startup Recovery Manager, por ejemplo, actualizando la protección.

Si el cifrado por BitLocker no se suspendió durante estas operaciones, deberá especificar su PIN de BitLocker después de reiniciar el equipo.

Habilitación de la recuperación con un clic

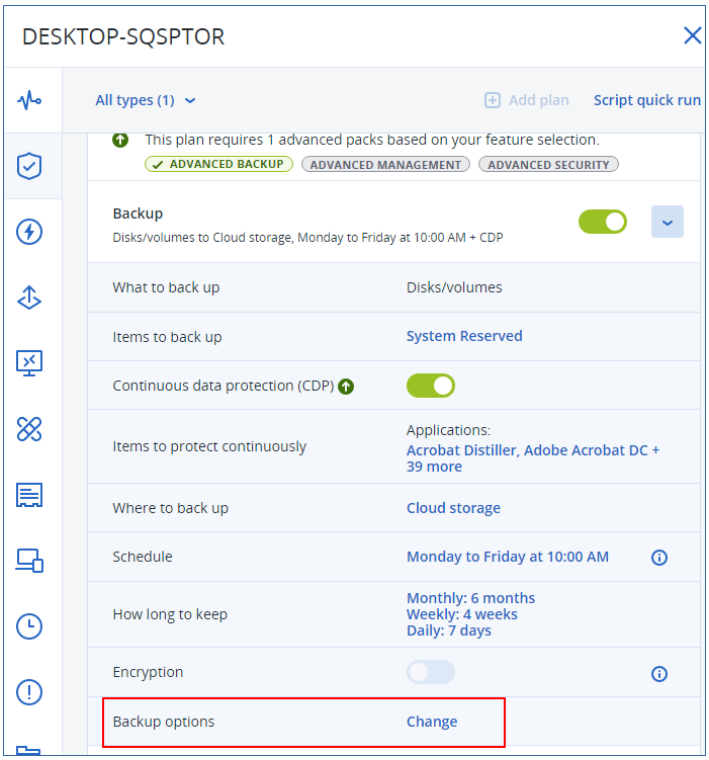
La recuperación con un clic es una opción de copia de seguridad en el plan de protección. Para obtener más información sobre cómo crear un plan, consulte "Creación de un plan de protección" (p. 250).

Nota
Habilitar la recuperación con un clic también habilita Startup Recovery Manager en el equipo de destino. Si Startup Recovery Manager no se puede habilitar, la operación de copia de seguridad que crea copias de seguridad con recuperación con un clic no funcionará. Para obtener más información sobre Startup Recovery Manager, consulte "Startup Recovery Manager" (p. 1007).

Para habilitar la recuperación con un clic

1. En el plan de protección, expanda el módulo **Copia de seguridad**.
2. En **Qué incorporar en la copia de seguridad**, seleccione **Todo el equipo** o **Disco/volúmenes**.
3. [Si ha seleccionado **Disco/volúmenes**]. En **Elementos que se incluirán en la copia de seguridad**, especifique el disco o los volúmenes que desea incluir en la copia de seguridad.
4. En **Opciones de copia de seguridad**, haga clic en **Modificar** y, a continuación, seleccione **Recuperación con un clic**.

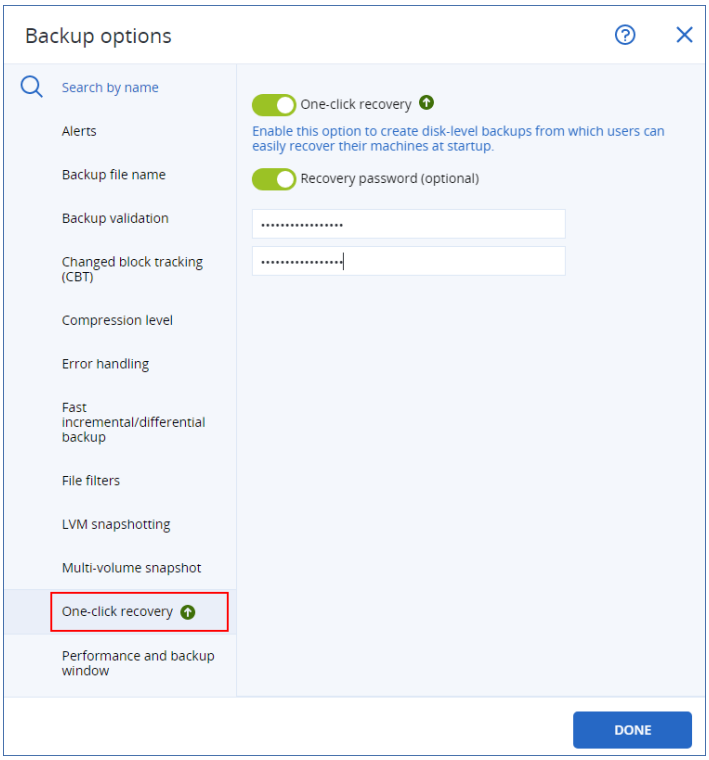
© Acronis International GmbH, 2003-2025



5. Habilite el conmutador **Recuperación con un clic**.
6. [Opcional] Habilite el conmutador **Contraseña de recuperación** y especifique una contraseña.

Importante
Le recomendamos encarecidamente que especifique una contraseña de recuperación. Asegúrese de que el usuario que realiza la recuperación con un clic en el equipo de destino conozca la contraseña.

© Acronis International GmbH, 2003-2025



7. Haga clic en **Listo**.
8. Configure los otros elementos del plan de protección según sus necesidades y guarde el plan.

Como resultado, después de que el plan de protección se ejecute y cree una copia de seguridad, la recuperación con un clic se vuelve accesible para los usuarios del equipo protegido.

Deshabilitación de la Recuperación con un clic

Puede deshabilitar la Recuperación con un clic para una carga de trabajo específica de las siguientes maneras:

- Deshabilite la opción **Recuperación con un clic** en el plan de protección que se aplica a la carga de trabajo.
- Revoque el plan de protección en el que la opción de **Recuperación con un clic** está habilitada.
- Elimine el plan de protección en el que la opción de **Recuperación con un clic** está habilitada.

Recuperar un equipo con Recuperación con un clic

Requisitos previos

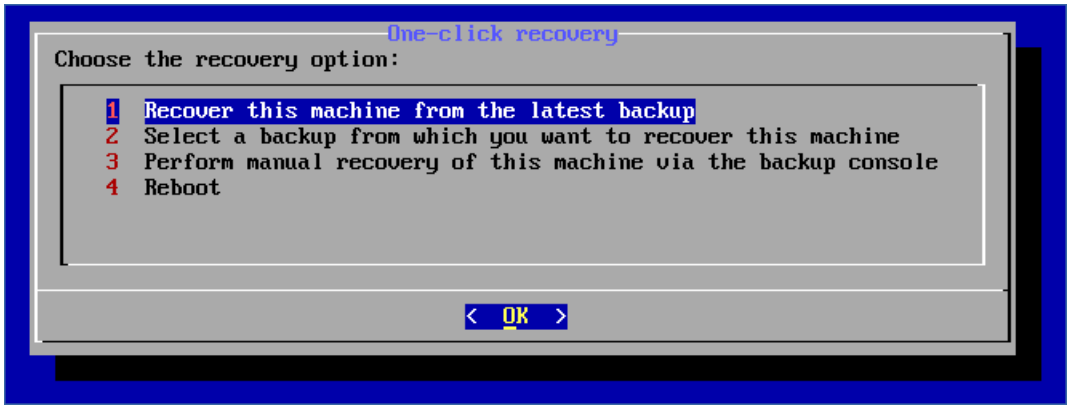
- Se aplica al equipo un plan de protección con la opción de copia de seguridad **Recuperación con un clic** habilitada.
- Existe al menos una copia de seguridad del disco del equipo.

Para recuperar un equipo

© Acronis International GmbH, 2003-2025

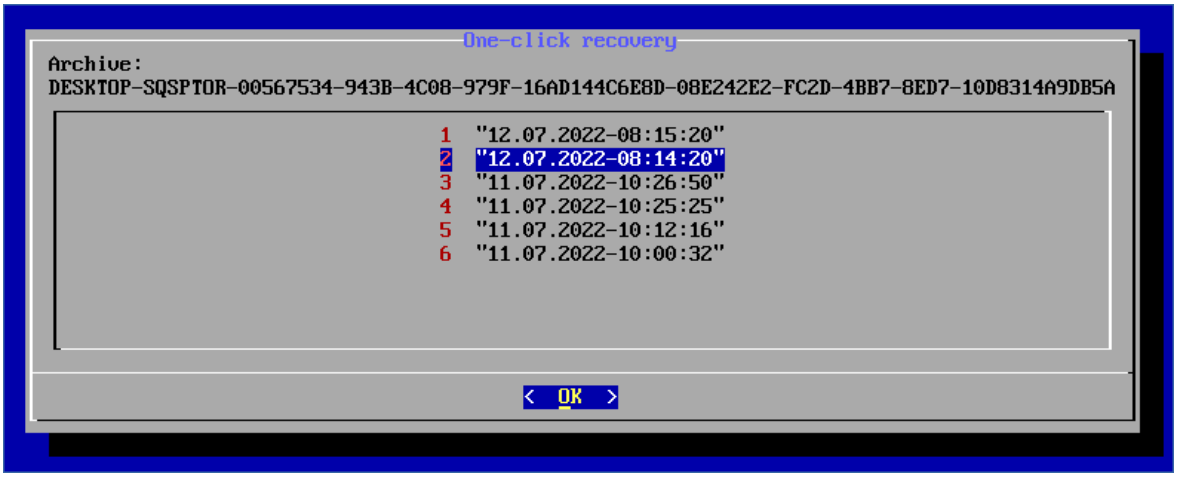
1. Reinicie el equipo que desea recuperar.
2. Durante el reinicio, pulse F11 para entrar en Startup Recovery Manager.

   Se abre la ventana del dispositivo de rescate.
3. Seleccione **Acronis Cyber Protect**.
4. [Si se ha especificado una contraseña de recuperación en el plan de protección] Introduzca la contraseña de recuperación y, a continuación, haga clic en **Aceptar**.
5. Seleccione la opción de Recuperación con un clic.
   - Para recuperar automáticamente la copia de seguridad más reciente, seleccione la primera opción y, seguidamente, haga clic en **Aceptar**.
   - Para recuperar otra copia de seguridad dentro del archivo de copia de seguridad, seleccione la segunda opción y haga clic en **Aceptar**.



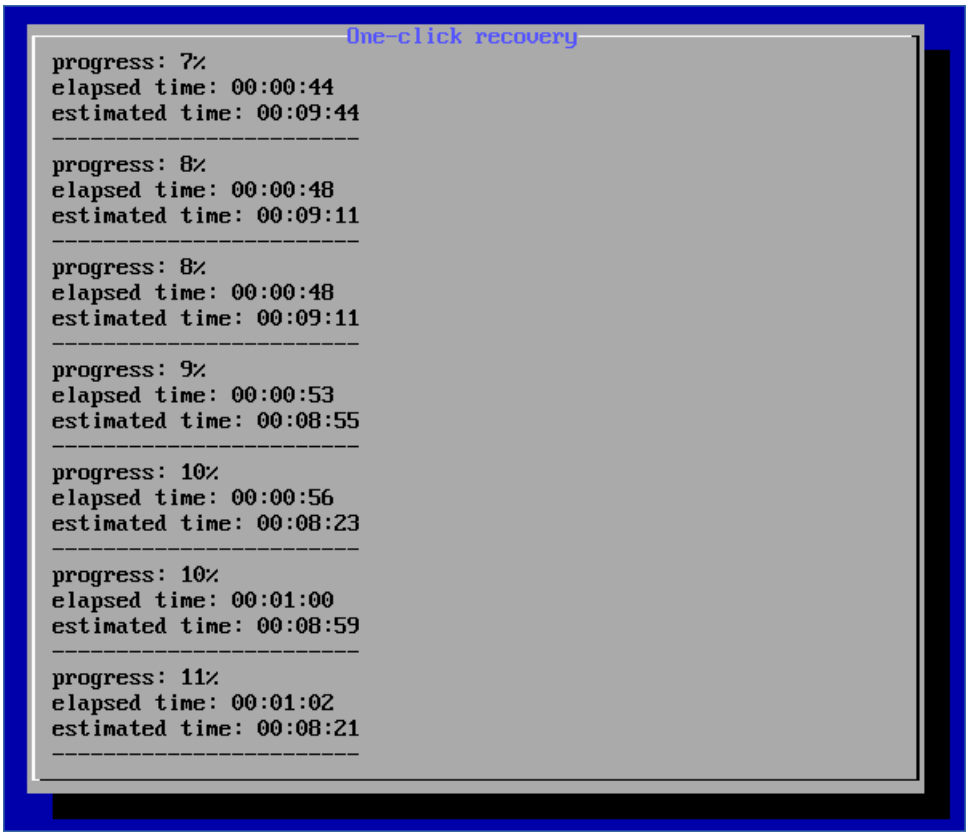
6. Haga clic en **Sí** para confirmar su elección.

   Se abre la ventana del dispositivo de rescate y luego desaparece. El procedimiento de recuperación continúa sin ella.
7. [Si decide recuperar una copia de seguridad específica] Seleccione la copia de seguridad que desea recuperar y, a continuación, haga clic en **Aceptar**.



Pasado un tiempo, se inicia la recuperación y se muestra el progreso. Una vez que la recuperación se completa, el equipo se reinicia.

© Acronis International GmbH, 2003-2025



Ventana de copia de seguridad y rendimiento

Esta opción le sirve para establecer uno de los tres niveles de rendimiento de copia de seguridad (alto, bajo o sin permiso) para cada hora durante una semana. De esta forma, puede definir un intervalo de tiempo en el que las copias de seguridad se puedan iniciar y ejecutar. El nivel de rendimiento alto y el bajo se pueden configurar en lo que respecta a la velocidad de salida y prioridad del proceso.

Esta opción no está disponible para copias de seguridad que ejecutan agentes en la nube, como copias de seguridad de sitios web o de servidores alojados en el sitio web de recuperación en la nube.

Esta opción es válida únicamente para los procesos de copia de seguridad y réplicas de copias de seguridad. Los comandos posteriores a la copia de seguridad y otras operaciones incluidas en un plan de protección (por ejemplo, validación) se ejecutarán independientemente de si esta opción está habilitada.

El valor predeterminado es el siguiente: **Deshabilitado**.

Cuando esta opción está deshabilitada, las copias de seguridad se pueden ejecutar en cualquier momento con los siguientes parámetros (no importa si los parámetros se cambiaron sin respetar el valor predeterminado):

- Prioridad de CPU: **Baja** (en Windows, corresponde a **Por debajo de lo normal**)
- Velocidad de salida: **Ilimitada**

© Acronis International GmbH, 2003-2025

Cuando esta opción está habilitada, las copias de seguridad programadas se permiten o bloquean de acuerdo con los parámetros de realización especificados para la hora actual. Al comienzo de una hora en que las copias de seguridad están bloqueadas, los procesos de copia de seguridad se detienen automáticamente y se genera una alerta. Incluso si se bloquean las copias de seguridad programadas, se puede iniciar una copia de seguridad de forma manual. Se utilizarán los parámetros de rendimiento de la hora más reciente en que se permitieron las copias de seguridad.

Nota
Puede configurar la realización y el período de copia de seguridad para cada ubicación de replicación de manera individual. Para acceder a la configuración de la ubicación de replicación, en el plan de protección, haga clic en el ícono de engranaje junto al nombre de la ubicación, y luego haga clic en **Ventana de copia de seguridad y rendimiento**.

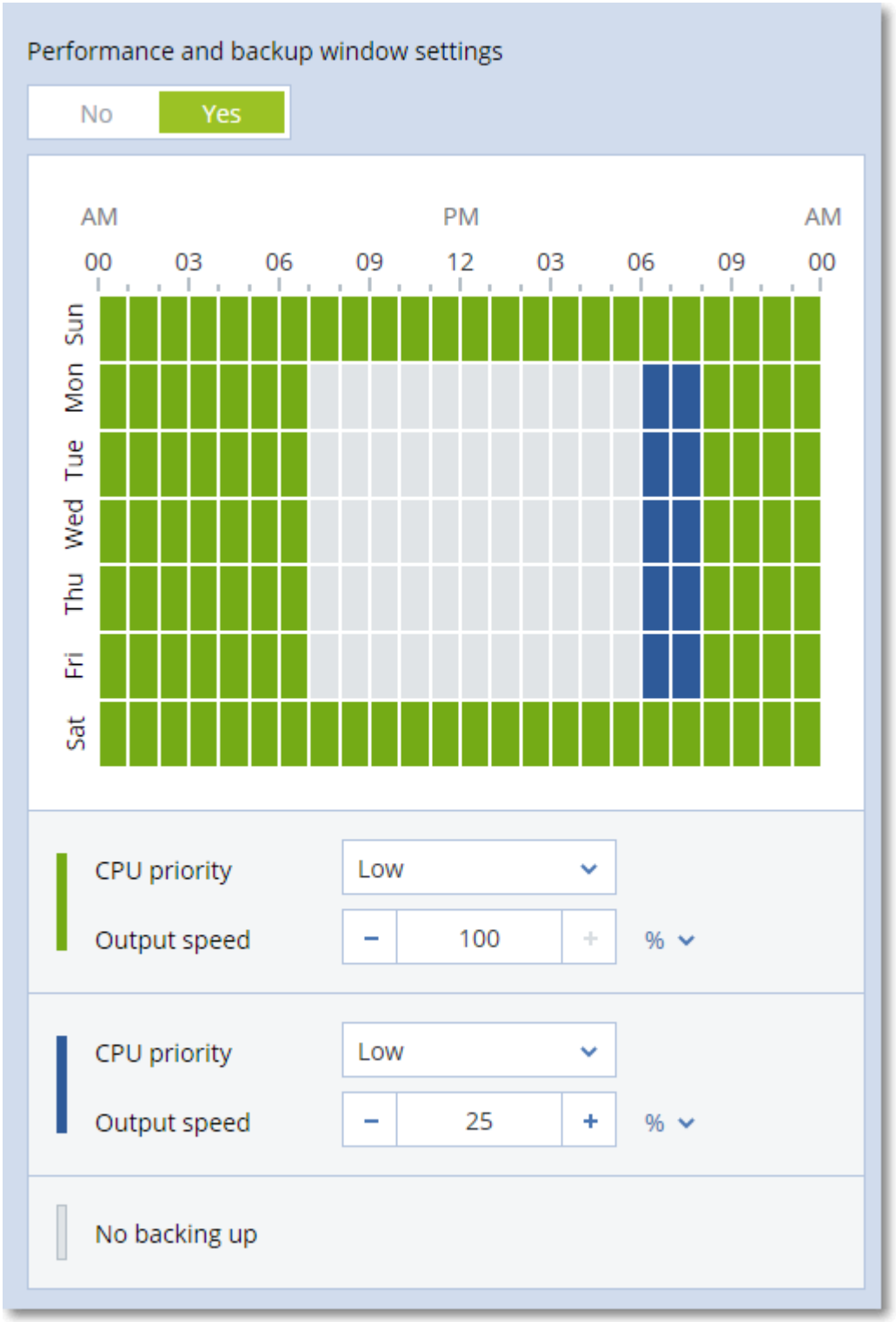
Ventana de copias de seguridad

Cada rectángulo representa una hora de un día de la semana. Haga clic en un rectángulo para desplazarse por los siguientes estados:

- **Verde:** se permite la realización de copias de seguridad con los parámetros especificados en la sección verde que aparece a continuación.
- **Azul:** se permite la realización de copias de seguridad con los parámetros especificados en la sección azul que aparece a continuación.
  Este estado no está disponible si el formato de copia de seguridad está establecido en la **Versión 11**.
- **Gris:** la realización de copias de seguridad está bloqueada.

Puede hacer clic y arrastrar para cambiar el estado de varios rectángulos de forma simultánea.

© Acronis International GmbH, 2003-2025



Prioridad de la CPU

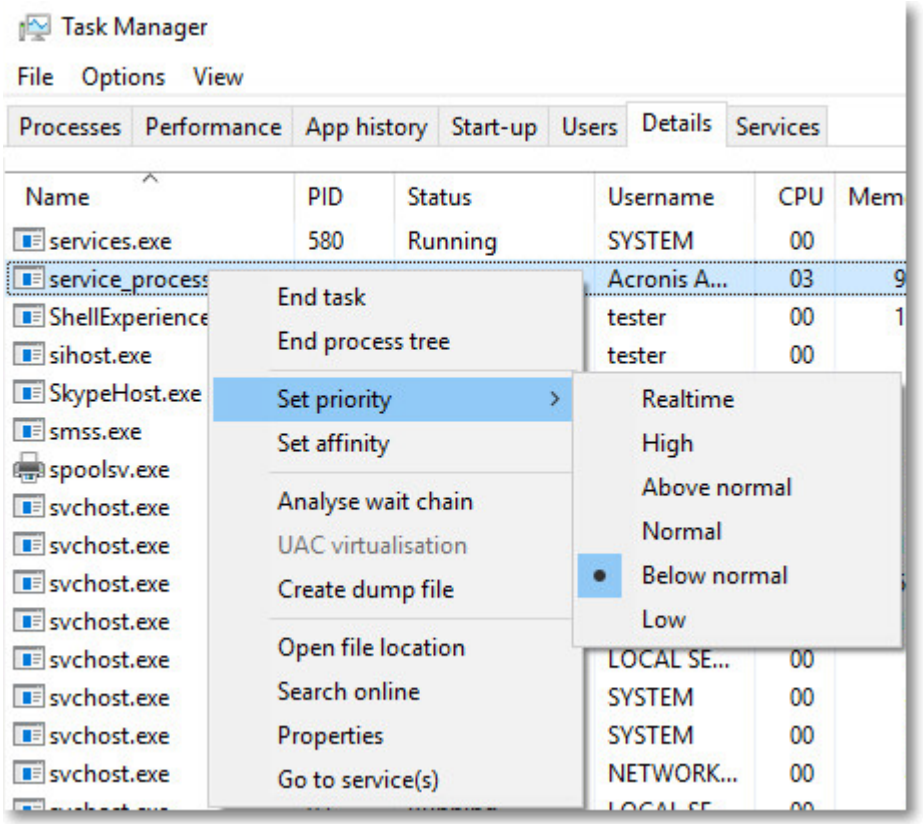
Este parámetro define la prioridad del proceso de copia de seguridad en el sistema operativo.

Los ajustes disponibles son: **Baja**, **Normal**, **Alta**.

© Acronis International GmbH, 2003-2025

La prioridad de un proceso que se ejecute en un sistema determina la cantidad de uso de la CPU y los recursos del sistema que se asignan a dicho proceso. La disminución de la prioridad de la copia de seguridad liberará más recursos para otras aplicaciones. El aumento de la prioridad podría acelerar el proceso de copia de seguridad al solicitar que el sistema operativo asigne más recursos, como CPU, a la aplicación de copia de seguridad. Sin embargo, el efecto resultante dependerá del uso total de CPU y otros factores, como la velocidad de salida o entrada del disco, o el tráfico en la red.

Esta opción define la prioridad de un proceso de copia de seguridad (**service_process.exe)** en Windows y la perfección de este proceso (**service_process)** en Linux y en macOS.



La siguiente tabla resume la asignación de esta configuración en Windows, Linux y macOS.

Prioridad de Cyber Protection	Prioridad de Windows	Perfección de de Linux y macOS
Bajo	Por debajo de lo normal	10
Normal	Normal	0
Alto	Alto	-10

© Acronis International GmbH, 2003-2025

Velocidad de salida durante la copia de seguridad

Este parámetro permite limitar la velocidad de escritura en el disco duro (al hacer copias de seguridad en una carpeta local) o la velocidad de transferencia de los datos de la copia de seguridad a través de la red (al hacer copias de seguridad en un recurso compartido de red o en el almacenamiento en cloud).

Cuando esta opción está habilitada, puede especificar la velocidad de salida máxima permitida:

- Como porcentaje de la velocidad de escritura estimada del disco rígido de destino (al hacer copias de seguridad en una carpeta local) o la velocidad máxima estimada de la conexión de red (al hacer copias de seguridad en un recurso compartido de red o en el almacenamiento en cloud).

  Esta configuración solo funciona si el agente se ejecuta en Windows.
- En KB/segundo (para todos los destinos).

Envío de datos físicos

Esta opción está disponible si el destino de la copia de seguridad o de replicación es el almacenamiento en la nube y el formato de la copia de seguridad está establecido en la **Versión 12**.

Esta opción se aplica a las copias de seguridad de discos y archivos creadas por el agente para Windows, Linux, Mac, VMware, Hyper-V y Virtuozzo.

Utilice esta opción para enviar la primera copia de seguridad completa creada por un plan de protección en el almacenamiento en la nube en una unidad de disco rígido mediante el servicio de envío de datos físicos. Las copias de seguridad incrementales posteriores se transfieren a través de la red.

En las copias de seguridad locales replicadas en la nube, se mantienen las copias de seguridad incrementales y se guardan de manera local hasta que se carga la copia de seguridad inicial al almacenamiento de la nube. Entonces, se replican todos los cambios incrementales a la nube y la replicación sigue por planificación de copia de seguridad.

El valor predeterminado es el siguiente: **Deshabilitado**.

Acerca del servicio de envío de datos físicos

La interfaz web del servicio de envío de datos físicos solo está disponible para los administradores.

Para obtener instrucciones detalladas acerca del uso del servicio de envío de datos físicos y la herramienta de creación de pedidos, consulte la Guía del administrador para el envío de datos físicos. Para acceder a este documento en la interfaz web del servicio de envío de datos físicos, haga clic en el icono de signo de interrogación.

© Acronis International GmbH, 2003-2025

Información general acerca del proceso de envío de datos físicos

1. [Pasos para enviar copias de seguridad con almacenamiento en la nube como ubicación de la copia de seguridad principal]
   a. Cree un nuevo plan de protección con copia de seguridad en la nube.
   b. En la fila **Opciones de copia de seguridad**, haga clic en **Modificar**.
   c. En la lista de opciones disponibles, haga clic en **Envío de datos físicos**.

   Puede realizar la copia de seguridad directamente en una unidad extraíble, o bien realizarla en una carpeta local o de red y, a continuación, copiarla o moverla a la unidad.
2. [Pasos para enviar copias de seguridad locales replicadas en la nube]

   Nota
   Esta opción es compatible con el agente de protección a partir de la versión C21.06 o posterior.

   a. Cree un nuevo plan de protección con copia de seguridad en un almacenamiento local o en red.
   b. Haga clic en **Añadir ubicación** y seleccione **Almacenamiento en la nube**.
   c. En la fila de la ubicación **Almacenamiento en la nube**, haga clic en el icono de engranaje y seleccione **Envío de datos físicos**.
3. En **Usar envío de datos físicos**, haga clic en **Sí** y en **Listo**.
   La opción Cifrado se habilita automáticamente en el plan de protección porque todas las copias de seguridad que se envían deben estar cifradas.
4. En la fila **Cifrado**, haga clic en **Especifique una contraseña** e indique una contraseña para el cifrado.
5. En la fila **Envío de datos físicos**, seleccione la unidad extraíble en la que se guardará la copia de seguridad inicial.
6. Haga clic en **Crear** para guardar el plan de protección.
7. Tras completar la primera copia de seguridad, use la interfaz web del servicio de envío de datos físicos para descargar la herramienta de creación de pedidos y cree uno.
   Para acceder a la interfaz web, inicie sesión en el portal de gestión, haga clic en **Información general** > **Uso** y, a continuación, en **Gestionar servicio**, que encontrará en **Envío de datos físicos**.

   Importante
   Tras finalizar la primera copia de seguridad completa, las copias de seguridad posteriores deben realizarse en el mismo plan de protección. Cualquier otro plan de protección, incluso uno con los mismos parámetros y para el mismo equipo, requerirá otro ciclo de envío de datos físicos.
8. Empaquete las unidades y envíelas al centro de datos.

© Acronis International GmbH, 2003-2025

Importante
Asegúrese de seguir las instrucciones de empaquetado que se proporcionan en la Guía del administrador para el envío de datos físicos.

9. La interfaz web del servicio de envío de datos físicos permite realizar el seguimiento del estado del pedido. Tenga en cuenta que las copias de seguridad posteriores generarán un error hasta que la primera copia de seguridad se cargue en el almacenamiento en la cloud.

Comandos previos/posteriores

Esta opción le permite definir los comandos a ejecutar automáticamente antes y después del proceso de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post.

Comando de precopia de seguridad	Copia de seguridad	Comando de Post-copia de seguridad

Ejemplos de como se pueden usar los comandos pre/post:

- Eliminación de archivos temporales antes de comenzar la copia de seguridad.
- Configuración de un producto antivirus de terceros antes de comenzar la copia de seguridad.
- Copia selectiva de copias de seguridad en otra ubicación. Esta opción puede ser útil porque la replicación configurada en un plan de protección copia *todas* las copias de seguridad a ubicaciones posteriores.

El agente realiza la replicación *después* de ejecutar el comando posterior a la copia de seguridad.

El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pausa”).

Comando de precopia de seguridad

Para especificar un comando o archivo de proceso por lotes para que se ejecute antes de que comience la copia de seguridad

1. Habilite el conmutador **Ejecutar un comando antes de la copia de seguridad**.
2. En el campo **Comando o ruta de archivo de proceso por lotes en el equipo con un agente**, escriba un comando o busque un archivo de proceso por lotes.
   No se admite el uso de comandos que requieran la participación del usuario (por ejemplo, `pause`).
   Si utiliza PowerShell, pase el comando como argumento a `powershell.exe`.
   Por ejemplo, utilice:

   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```

   en lugar de:

© Acronis International GmbH, 2003-2025

```
New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
```

3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos para el comando, si es necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Listo**.

Casilla de verificación	**Selección**			
Hacer que la copia de seguridad falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la copia de seguridad hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Realizar la copia de seguridad solo después de que se ejecute el comando correctamente. Hacer que la copia de seguridad falle si falla la ejecución del comando.	Realizar la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de la ejecución	N/D	Realizar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

* Un comando se considerará fallido si su código de salida no es igual a cero.

© Acronis International GmbH, 2003-2025

Nota

Si un script falla debido a un conflicto relacionado con la versión de la biblioteca requerida en Linux, excluya las variables del entorno `LD_LIBRARY_PATH` y `LD_PRELOAD` añadiendo estas líneas a su script:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Comando de Post-copia de seguridad

Para especificar un comando o archivo de proceso por lotes que se ejecute después de completar la copia de seguridad

1. Habilite el conmutador **Ejecutar un comando tras la copia de seguridad**.
2. En el campo **Comando o ruta de archivo de proceso por lotes en el equipo con un agente**, escriba un comando o busque un archivo de proceso por lotes.

   No se admite el uso de comandos que requieran la participación del usuario (por ejemplo, `pause`).

   Si utiliza PowerShell, pase el comando como argumento a `powershell.exe`.

   Por ejemplo, utilice:

   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```

   en lugar de:

   ```
   New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
   ```
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos para el comando, si es necesario.
5. Si es crítico que la ejecución del comando sea satisfactoria, marque la casilla de verificación **No realizar la copia de seguridad si no se ejecuta el comando**.

   Un comando se considera fallido si su código de salida no es igual a cero. Si la ejecución del comando falla, el estado de la copia de seguridad se establece en **Error**.

   Si la casilla de verificación **No realizar la copia de seguridad si no se ejecuta el comando** no está marcada, el resultado de la ejecución del comando no afecta al estado de la copia de seguridad.

   Puede comprobar el resultado de la ejecución del comando en la pestaña **Actividades**.
6. Haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Comandos previos o posteriores a la captura de datos

La opción le permite definir los comandos que se ejecutarán automáticamente antes y después de la captura de datos (es decir, tomar la instantánea de los datos). La captura de datos se realiza al comienzo del procedimiento de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post de la captura de datos.

	<---------- **Copia de seguridad** ---------->				
Comando de precopia de seguridad	Comandos antes de la captura de datos	Captura de datos	Comandos Post de la captura de datos	Escribir datos en el archivo de copia de seguridad	Comando de Post-copia de seguridad

Interacción con otras opciones de copia de seguridad

La ejecución de comandos antes y después de la captura de datos puede modificarse mediante otras opciones de copia de seguridad.

Si la opción **Instantánea multivolumen** está habilitada, los comandos anteriores y posteriores a la captura de datos se ejecutarán solo una vez, porque las instantáneas de todos los volúmenes se crean de forma simultánea. Si la opción **Instantánea multivolumen** está deshabilitada, los comandos anteriores y posteriores a la captura de datos se ejecutarán para cada volumen del que se crea una copia de seguridad, porque las instantáneas se crean de forma secuencial, un volumen después de otro.

Si la opción **Servicio de instantáneas de volumen (VSS)** está habilitada, los comandos anteriores y posteriores a la captura de datos y las acciones de Microsoft VSS se ejecutarán tal y como se indica a continuación:

Comandos anteriores a la captura de datos > Suspensión de VSS > Captura de datos > Reanudación de VSS > Comandos posteriores a la captura de datos

El uso de comandos previos y posteriores a la captura de datos permite suspender y reanudar una base de datos o una aplicación que no sean compatibles con VSS. Como la captura de datos tarda unos segundos, el tiempo de inactividad de la base de datos o la aplicación será mínimo.

Comandos antes de la captura de datos

Para especificar un comando o archivo por lotes para que se ejecute antes de la captura de datos

1. Habilite el conmutador **Ejecutar un comando antes de la captura de datos**.
2. En el campo **Comando o ruta de archivo de proceso por lotes en el equipo con un agente**, escriba un comando o busque un archivo de proceso por lotes.

© Acronis International GmbH, 2003-2025

No se admite el uso de comandos que requieran la participación del usuario (por ejemplo, `pause`).

Si utiliza PowerShell, pase el comando como argumento a `powershell.exe`.

Por ejemplo, utilice:

```
powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
```

en lugar de:

```
New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
```

3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos para el comando, si es necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Listo**.

Casilla de verificación	**Selección**			
Hacer que la copia de seguridad falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la captura de datos hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Realizar la captura de datos solo después de que se ejecute el comando correctamente. Hacer que la copia de seguridad falle si falla la ejecución del comando.	Realizar la captura de datos después de que se ejecute el comando a pesar del éxito o fallo de la ejecución	N/D	Realizar la captura de datos al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

* Un comando se considerará fallido si su código de salida no es igual a cero.

© Acronis International GmbH, 2003-2025

Nota
Si un script falla debido a un conflicto relacionado con la versión de la biblioteca requerida en Linux, excluya las variables del entorno `LD_LIBRARY_PATH` y `LD_PRELOAD` añadiendo estas líneas a su script:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Comandos Post de la captura de datos

Para especificar un comando o archivo de proceso por lotes para que se ejecute después de la captura de datos

1. Habilite el conmutador **Ejecutar un comando tras la captura de datos**.
2. En el campo **Comando o ruta de archivo de proceso por lotes en el equipo con un agente**, escriba un comando o busque un archivo de proceso por lotes.
   No se admite el uso de comandos que requieran la participación del usuario (por ejemplo, `pause`).
   Si utiliza PowerShell, pase el comando como argumento a `powershell.exe`.
   Por ejemplo, utilice:
   ```
   powershell.exe -C "New-Item -Force -ItemType file -Path 'C:\temp\file.txt'"
   ```
   en lugar de:
   ```
   New-Item -Force -ItemType file -Path 'C:\temp\file.txt'
   ```
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos para el comando, si es necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Listo**.

Casilla de verificación	Selección			
Hacer que la copia de seguridad falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la	Seleccionado	Seleccionado	Borrado	Borrado

© Acronis International GmbH, 2003-2025

copia de seguridad hasta que finalice la ejecución de comandos				
Resultado				
	Valor predeterminado Continúe la copia de seguridad solo después de que se ejecute el comando correctamente.	Continúe la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de su ejecución.	N/D	Continuar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

* Un comando se considerará fallido si su código de salida no es igual a cero.

Planificación

Esta opción define si las copias de seguridad empiezan exactamente según lo planificado o con demora, así como el número de máquinas virtuales de los que se hace copia de seguridad simultáneamente.

Para obtener más información sobre cómo configurar la planificación de las copias de seguridad, consulte "Ejecutar una copia de seguridad en una planificación" (p. 559).

El valor predeterminado es el siguiente: **Distribuya las horas de inicio de la copia de seguridad en un período de tiempo**. **Retraso máximo**: **30 minutos**.

Puede seleccionar una de las siguientes opciones:

- **Iniciar todas las copias de seguridad según lo planificado**.
  Las copias de seguridad de los equipos físicos empezarán exactamente según la planificación. Las copias de seguridad de los equipos virtuales se harán una a una.
- **Distribuir las horas de inicio en una ventana de tiempo**
  Las copias de seguridad de los equipos físicos empezarán con demora respecto a la hora planificada. El valor de demora de cada equipo se selecciona de forma aleatoria y oscila entre cero y el valor máximo que especifique. Puede resultarle útil para evitar una carga excesiva de la red al realizar copias de seguridad de varios equipos simultáneamente en una misma ubicación de red. El valor de demora de cada equipo se determina cuando se aplica el plan de protección en el equipo y permanece igual hasta que se edita el plan de protección y se modifica el valor máximo de demora.
  Las copias de seguridad de los equipos virtuales se harán una a una.
- **Limitar el número de copias de seguridad ejecutadas a la vez a**

© Acronis International GmbH, 2003-2025

Utilice esta opción para gestionar la copia de seguridad paralela de las máquinas virtuales de las que se hace una copia de seguridad a nivel del hipervisor (copia de seguridad sin agente).

Los planes de protección en los que está seleccionada esta opción se pueden ejecutar con otros planes de protección que el agente esté operando simultáneamente. Cuando seleccione esta opción, debe especificar el número de copias de seguridad paralelas por plan. El número total de equipos de los que se hace una copia de seguridad simultáneamente por todos los planes se limita a 10 por agente. Para saber cómo cambiar el límite predeterminado, consulte "Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo" (p. 980).

Los planes de protección en los que no está seleccionada esta opción ejecutan operaciones de copia de seguridad de forma secuencial en una máquina virtual tras otra.

Copia de seguridad sector por sector

La opción es eficaz solo para la copia de seguridad a nivel del disco.

Esta opción define si se crea una copia exacta de un disco o volumen en un nivel físico.

El valor predeterminado es el siguiente: **Deshabilitado**.

Si esta opción está habilitada, se hará copia de seguridad de todos los sectores del disco o volumen, incluido el espacio no asignado y los sectores que no tengan datos. La copia de seguridad resultante tendrá el mismo tamaño que el disco objeto de la copia de seguridad (si la opción "Nivel de compresión" se establece en **Ninguno**). El software cambia automáticamente al modo sector por sector al hacer copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles.

Nota
Será imposible realizar una recuperación de datos de aplicaciones desde las copias de seguridad creadas en el modo sector por sector.

División

Al crear un plan de protección, puede seleccionar el método de división de copias de seguridad grandes en archivos más pequeños.

Nota
No se puede dividir en planes de protección que usen el almacenamiento en la nube como ubicación principal o secundaria de la copia de seguridad.

De forma predeterminada es:

- Si la ubicación de la copia de seguridad es una carpeta local o de red (SMB) y la copia de seguridad tiene el formato TIBX (a.k.a. Versión 12): **Tamaño fijo: 200 GB**

© Acronis International GmbH, 2003-2025

Esta configuración permite que el software de copia de seguridad funcione con grandes volúmenes de datos en sistemas de archivos NTFS sin los efectos negativos causados por la fragmentación de archivos.

- De lo contrario: **Automático**

Están disponibles las siguientes configuraciones:

- **Automático**
  La copia de seguridad se dividirá si supera el tamaño de archivo máximo que admite el sistema de archivos.
- **Tamaño fijo**
  Introduzca el tamaño de archivo deseado o selecciónelo en el menú desplegable y guarde el plan.

Nota
Cambiar la opción de división en un plan de copias de seguridad no afecta a los archivos comprimidos ya creados.

Manejo de fallos de la tarea

Esta opción determina el comportamiento del programa cuando falle la ejecución planificada de un plan de protección o su equipo se reinicie mientras se está ejecutando una copia de seguridad. Esta opción no se aplica si se inicia un plan de protección manualmente.

Si esta opción está habilitada, el programa intentará ejecutar de nuevo el plan de protección. Puede especificar el número de intentos y el intervalo de tiempo entre los intentos. El programa dejará de intentar tan pronto como un intento finalice correctamente o se haya realizado el número de intentos especificados, lo que suceda primero.

Si esta opción está habilitada y su equipo se reinicia mientras se está ejecutando una copia de seguridad, la operación de copia de seguridad no fallará. Unos minutos después del reinicio, la operación de copia de seguridad continuará de forma automática y completará el archivo de copia de seguridad con los datos que faltan. En este caso de uso, la opción **Intervalo entre intentos** no es importante.

El valor predeterminado es el siguiente: **Habilitado**.

Nota
Esta opción no es eficaz para las copias de seguridad forenses.

Condiciones de inicio de la tarea

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción determina el comportamiento del programa si hay una tarea que esté a punto de iniciarse (cuando llegue el momento programado o cuando ocurra el evento especificado en el programa), pero no se cumple con la condición (o cualquiera de las condiciones). Para obtener más información acerca de las condiciones, consulte "Condiciones de inicio" (p. 566).

© Acronis International GmbH, 2003-2025

El valor predeterminado es el siguiente: **Esperar hasta que se cumplan las condiciones de la planificación**.

Esperar hasta que se cumplan las condiciones de la planificación

Con esta configuración, el Programador comienza a supervisar las condiciones e inicia la tarea cuando se cumplen las condiciones. Si no se cumplen las condiciones, la tarea no comenzará nunca.

Para manejar la situación cuando no se cumplen con las condiciones por mucho tiempo y el retraso de la tarea se vuelve peligroso, puede definir el intervalo en el cual la tarea se ejecutará independientemente de la condición. Seleccione la casilla de verificación **Ejecutar la tarea de todos modos después** y especifique el intervalo de tiempo. La tarea comenzará tan pronto como se cumpla con las condiciones o pase el período máximo de tiempo, lo que suceda primero.

Omitir la ejecución de tarea

El retraso de una tarea puede ser inadmisible, por ejemplo, cuando necesite ejecutar una tarea estrictamente a la hora especificada. Entonces parece sensato omitir la tarea en vez de esperar a que se cumplan las condiciones, en especial si las tareas son frecuentes.

Servicio de instantáneas de volumen (VSS)

Esta opción solo se aplica a los sistemas operativos de Windows.

Define si se puede realizar una copia de seguridad correctamente si fallan uno o más escritores del servicio de instantáneas de volumen (VSS) y qué proveedor debe notificar a las aplicaciones compatibles con VSS que se iniciará la copia de seguridad.

Al utilizar el servicio de instantáneas de volumen, se garantiza el estado coherente de todos los datos que usan las aplicaciones, en particular la finalización de todas las transacciones de bases de datos en el momento en que el software de copia de seguridad realiza la instantánea de los datos. En cambio, la consistencia de los datos garantiza que la aplicación se recuperará en el estado correcto y será operativa inmediatamente después de la recuperación.

La instantánea se utiliza solo durante la operación de copia de seguridad y se elimina automáticamente cuando se completa dicha operación. No se conservan archivos temporales.

También puede usar los comandos previos o posteriores a la captura de datos para garantizar que se haga una copia de seguridad de los datos con un estado coherente. Por ejemplo, especifique los comandos previos a la captura de datos que suspenderán la base de datos y vacíe la memoria caché para garantizar que se completen todos las transacciones, y, a continuación, especifique los comandos posteriores a la captura de datos que reanudarán las operaciones de base de datos después de tomar la instantánea.

© Acronis International GmbH, 2003-2025

Nota
No se crearán copias de seguridad de las carpetas ni de los archivos especificados en la clave de registro **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**. En concreto, no se crean copias de seguridad de los archivos de datos fuera de línea de Outlook (.ost), porque se especifican en el valor **OutlookOST** de esta clave.

Ignorar escritores de VSS fallidos

Puede seleccionar una de las siguientes opciones:

- **Ignorar escritores de VSS fallidos**
  Con esta opción, puede realizar copias de seguridad correctamente incluso en el caso de que fallen uno o más escritores de VSS.

  Importante
  Las copias de seguridad con información de aplicaciones siempre fallarán si falla el escritor de esa aplicación específica. Por ejemplo, si realizas una copia de seguridad con información de aplicaciones de los datos de SQL Server y falla **SqlServerWriter**, también fallará la operación de copia de seguridad.

  Cuando se habilita esta opción, se intentará hacer una instantánea de VSS hasta tres veces consecutivas.
  En el primer intento, se requieren todos los escritores de VSS. Si falla, se repetirá el proceso. Si falla el segundo intento, se excluirán los escritores de VSS fallidos del ámbito de la operación de copia de seguridad y se hará un tercer intento. Si se consigue al tercer intento, se completará la copia de seguridad con un aviso sobre los escritores de VSS fallidos. Si falla, no se podrá realizar la copia de seguridad.
- **Se requiere el procesamiento correcto de todos los escritores de VSS**
  Si falla alguno de los escritores de VSS, también lo hará la operación de copia de seguridad.

Seleccionar el proveedor de instantáneas

Puede seleccionar una de las siguientes opciones:

- **Seleccione automáticamente el proveedor de instantáneas**
  Seleccione automáticamente entre el proveedor de instantáneas de hardware, un proveedor de instantáneas de software o el Microsoft Software Shadow Copy Provider.

  Nota
  Le recomendamos que utilice la selección automática de un proveedor de instantáneas siempre que sea posible.
- **Usar Microsoft Software Shadow Copy Provider**

© Acronis International GmbH, 2003-2025

Le recomendamos que fuerce el uso de Microsoft Software Shadow Copy Provider si tiene otros proveedores de VSS de terceros que no desea utilizar y cuando la carga de trabajo protegida no contenga volúmenes compartidos de clúster.

Advertencia.
Fuerce el uso de Microsoft Software Shadow Copy Provider solo si necesita usarlo explícitamente, ya que puede hacer que no se completen las copias de seguridad en entornos con volúmenes compartidos de clúster y otros volúmenes no compatibles con Microsoft Software Shadow Copy Provider.

Permitir copia de seguridad completa de VSS

Al habilitar esta opción, se truncarán los registros de Microsoft Exchange Server y de las demás aplicaciones compatibles con VSS (excepto Microsoft SQL Server) después de cada copia de seguridad completa, incremental o diferencial que se realice correctamente a nivel de disco.

El valor predeterminado es el siguiente: **Deshabilitado**.

Mantenga esta opción deshabilitada en los siguientes casos:

- Si utiliza Agente para Exchange o un software de terceros para realizar una copia de seguridad de los datos de Exchange Server. Esto se debe a que el truncamiento de registros interferirá con las copias de seguridad consecutivas de los registros de las transacciones.
- Si utiliza un software de terceros para realizar una copia de seguridad de los datos de SQL Server. El motivo es que el software de terceros tomará la copia de seguridad a nivel de discos resultante para su "propia" copia de seguridad completa. Como consecuencia, no se podrá realizar la siguiente copia de seguridad diferencial de los datos de SQL Server. No se podrán realizar copias de seguridad hasta que el software de terceros cree la siguiente copia de seguridad completa "propia".
- Si en el equipo se están ejecutando otras aplicaciones que reconocen la característica VSS y debe mantener sus registros por cualquier motivo.

Importante
Al habilitar esta opción, no se truncan los registros de Microsoft SQL Server. Para truncar el registro de SQL Server después de una copia de seguridad, habilite la opción de copia de seguridad Truncamiento de registros.

Servicio de instantáneas de volumen (VSS) para equipos virtuales

Esta opción controla la creación de instantáneas en modo de inactividad para máquinas virtuales protegidas.

El valor predeterminado es el siguiente: **Habilitado**.

Cuando esta opción está habilita, se completan las transacciones de todas las aplicaciones compatibles con VSS que se ejecutan en la máquina virtual antes de tomar una instantánea en modo inactivo.

© Acronis International GmbH, 2003-2025

Si no se puede tomar una instantánea en modo de inactividad por algún motivo, el resultado de la operación de copia de seguridad depende de la configuración de la aplicación de copia de seguridad de la siguiente manera.

- Si la copia de seguridad de la aplicación está configurada como **Habilitada** y no se puede tomar una instantánea en modo de inactividad después del número de reintentos especificados en la opción Manejo de errores, la copia de seguridad falla.
- Si la copia de seguridad de la aplicación está configurada en **Deshabilitada** y no se puede tomar una instantánea en modo de inactividad después del número de reintentos especificados en la opción Manejo de errores, se crea una copia de seguridad coherente con el bloqueo.

  Para que la copia de seguridad falle en lugar de crear una copia de seguridad coherente, seleccione la casilla de verificación **Hacer que la copia de seguridad falle si no es posible tomar una instantánea en modo de inactividad**.

Cuando esta opción está deshabilitada, se toma una instantánea en modo activo. Se realizará una copia de seguridad de la máquina virtual en un estado coherente con un bloqueo.

La siguiente tabla resume los ajustes disponibles y sus resultados.

Configuración	La instantánea en modo inactivo se ha tomado correctamente		No se ha tomado la instantánea en modo inactivo	
	Copia de seguridad de la aplicación habilitada	**Copia de seguridad de la aplicación deshabilitada**	**Copia de seguridad de la aplicación habilitada**	**Copia de seguridad de la aplicación deshabilitada**
Servicio de instantáneas de volumen (VSS) para máquinas virtuales habilitado **Error en la copia de seguridad si no es posible tomar una instantánea en modo de inactividad** no seleccionado	Se toma la instantánea en modo inactivo. Se crea una copia de seguridad coherente con la aplicación.	Se toma la instantánea en modo inactivo. Se crea una copia de seguridad coherente con la aplicación.	Error al realizar la copia de seguridad.	Se toma una instantánea en modo activo. Se crea una copia de seguridad coherente con un bloqueo.
Servicio de instantáneas de volumen (VSS) para máquinas virtuales habilitado **Error en la copia de seguridad si no es posible tomar**	Se toma la instantánea en modo inactivo. Se crea una copia de seguridad coherente con la aplicación.	Se toma la instantánea en modo inactivo. Se crea una copia de seguridad coherente con la aplicación.	Error al realizar la copia de seguridad.	Error al realizar la copia de seguridad.

© Acronis International GmbH, 2003-2025

Configuración	La instantánea en modo inactivo se ha tomado correctamente		No se ha tomado la instantánea en modo inactivo	
	Copia de seguridad de la aplicación habilitada	**Copia de seguridad de la aplicación deshabilitada**	**Copia de seguridad de la aplicación habilitada**	**Copia de seguridad de la aplicación deshabilitada**
una instantánea en modo de inactividad seleccionado				
Servicio de instantáneas de volumen (VSS) para máquinas virtuales deshabilitado	Se toma una instantánea en modo activo. Se crea una copia de seguridad coherente con un bloqueo.	Se toma una instantánea en modo activo. Se crea una copia de seguridad coherente con un bloqueo.	Se toma una instantánea en modo activo. Se crea una copia de seguridad coherente con un bloqueo.	Se toma una instantánea en modo activo. Se crea una copia de seguridad coherente con un bloqueo.

Al habilitar la opción **Servicio de instantáneas de volumen (VSS) para equipos virtuales** también se activan los comandos de antes y después de la instantánea que podría tener en la copia de seguridad de la máquina virtual. Para obtener más información sobre estos scripts, consulte "Ejecución de comandos anteriores y posteriores a la instantánea automáticamente" (p. 968).

Para realizar una instantánea inactiva, el software de copia de seguridad aplica VSS dentro de una máquina virtual mediante las herramientas de VMware, Hyper-V Integration Services, las herramientas externas de Virtuozzo, las herramientas externas de Red Hat Virtualization o las herramientas externas de QEMU, respectivamente.

Nota

Para máquinas virtuales de Red Hat Virtualization (oVirt), le recomendamos que instale herramientas externas de QEMU en lugar de herramientas externas de Red Hat Virtualization. Algunas versiones de las herramientas externas de Red Hat Virtualization no son compatibles con las instantáneas coherentes con la aplicación.

Esta opción no afecta a los equipos virtuales de Scale Computing HC3. En estas máquinas, la inactividad depende de si las herramientas de Scale están instaladas en la máquina virtual o no.

Copia de seguridad semanal

Esta opción determina las copias de seguridad que se consideran "semanales" en las reglas de retención y los esquemas de copias de seguridad. Una copia de seguridad "semanal" es la primera copia de seguridad creada una vez comenzada la semana.

El valor predeterminado es el siguiente: **Lunes**.

© Acronis International GmbH, 2003-2025

Registro de eventos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción define si los agentes tienen que recopilar los eventos de las operaciones de copia de seguridad en el registro de eventos de aplicación de Windows (para ver este registro, ejecute eventvwr.exe o seleccione **Panel de control** > **Herramientas administrativas** > **Visor de eventos**). Puede filtrar los sucesos a ser recopilados.

El valor predeterminado es el siguiente: **Deshabilitado**.

Recuperación

Recuperación de apuntes

La siguiente tabla resume los métodos de recuperación disponibles. Use la tabla para elegir el método de recuperación que más le convenga.

Nota
En la consola de Cyber Protect no puede recuperar copias de seguridad en inquilinos en modo cumplimiento. Consulte "Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento" (p. 1570).

Qué recuperar	Método de recuperación
Máquina física (Windows o Linux)	Uso de la consola de Cyber Protect Uso de dispositivos de arranque
Máquina física (Mac)	Uso de dispositivos de arranque
Máquina virtual (Como VMware, Hyper-V, Red Hat Virtualization (oVirt), Scale Computing HC3 o Proxmox)	Uso de la consola de Cyber Protect Uso de dispositivos de arranque
Máquina virtual (Virtuozzo Hybrid Server, Virtuozzo Hybrid Infrastructure)	Uso de la consola de Cyber Protect
Contenedor (Virtuozzo Hybrid Server, Proxmox)	Uso de la consola de Cyber Protect
Configuración de ESXi	Uso de dispositivos de arranque
Archivos/Carpetas	Uso de la consola de Cyber Protect

© Acronis International GmbH, 2003-2025

	Descargar archivos del almacenamiento en la cloud Uso de dispositivos de arranque Extraer archivos de copias de seguridad locales
Estado del sistema	Uso de la consola de Cyber Protect
Bases de datos SQL	Uso de la consola de Cyber Protect
Bases de datos de Exchange	Uso de la consola de Cyber Protect
Buzones de correo de Exchange	Uso de la consola de Cyber Protect
Sitios web	Uso de la consola de Cyber Protect
Microsoft 365	
Buzones de correo (Agente local para Microsoft 365)	Uso de la consola de Cyber Protect
Buzones de correo (Agente en la nube para Microsoft 365)	Uso de la consola de Cyber Protect
Carpetas públicas	Uso de la consola de Cyber Protect
Archivos de OneDrive	Uso de la consola de Cyber Protect
Datos de SharePoint Online	Uso de la consola de Cyber Protect
Google Workspace	
Buzones de correo	Uso de la consola de Cyber Protect
Archivos de Google Drive	Uso de la consola de Cyber Protect
Archivos de unidades compartidas	Uso de la consola de Cyber Protect

Recuperación multiplataforma

La recuperación multiplataforma está disponible para las copias de seguridad de equipos completos y de discos que contengan un sistema operativo.

Se lleva a cabo una recuperación multiplataforma en los siguientes casos:

- Un tipo de agente crea una copia de seguridad, pero la recupera otro tipo de agente.

© Acronis International GmbH, 2003-2025

- Se recupera una copia de seguridad basada en agente a nivel de hipervisor (recuperación sin agente) o un agente recupera una copia de seguridad sin agente (recuperación basada en agente).
- Se recupera una copia de seguridad en hardware diferente (incluido hardware virtual).

Nota
Es posible que algunos dispositivos periféricos, como las impresoras, no se recuperen correctamente si realiza una recuperación multiplataforma.

Para obtener más información acerca de las posibles combinaciones para la recuperación entre plataformas, consulte "Recuperación multiplataforma" (p. 655).

Nota para los usuarios de Mac

- A partir de El Capitan 10.11, ciertos archivos de sistema, carpetas y procesos se marcan para su protección con el atributo de archivo extendido com.apple.rootless. Esta característica se llama Protección de integridad del sistema (SIP, por sus siglas en inglés). Los archivos protegidos incluyen aplicaciones previamente instaladas y la mayoría de carpetas en las ubicaciones /system, /bin, /sbin, /usr.

  Los archivos y carpetas protegidos no pueden sobrescribirse durante una recuperación realizada mediante el sistema operativo. Si necesita sobrescribir los archivos protegidos, realice la recuperación mediante dispositivos de arranque.
- A partir de macOS Sierra 10.12, puede mover los archivos que raramente utiliza a iCloud con la función Almacenar en la cloud. Se conservan espacios físicos reducidos de estos archivos en el sistema de archivos. Estos espacios se incluyen en la copia de seguridad en lugar de los archivos originales.

  Cuando se recupera un espacio en la ubicación original, este se sincroniza con iCloud y, por lo tanto, el archivo original está disponible. Cuando se recupera un espacio en una ubicación diferente, este no se puede sincronizar y, por lo tanto, el archivo original no está disponible.

Recuperación multiplataforma

Puede recuperar una copia de seguridad a nivel de disco en un equipo físico o en una máquina virtual. Por ejemplo, una copia de seguridad a nivel de disco es una copia de seguridad de **todo el equipo** o una copia de seguridad de **discos/volumen** que contiene el disco del sistema y el disco de arranque.

Se lleva a cabo una recuperación multiplataforma (migración de máquinas) en los siguientes casos:

- Cuando recupera una copia de seguridad de un equipo físico en una máquina virtual.
- Cuando recupera una copia de seguridad de una máquina virtual en un equipo físico.
- Cuando recupera una copia de seguridad de una máquina virtual en una máquina virtual en un tipo diferente de hipervisor.

© Acronis International GmbH, 2003-2025

Nota
Si una máquina virtual es objeto de una copia de seguridad por un agente de protección instalado en el sistema operativo invitado, la copia de seguridad se trata como una copia de seguridad de un equipo físico.

Las siguientes tablas resumen las opciones disponibles para la recuperación multiplataforma según el recurso informático respaldado.

Equipo físico

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Máquina virtual Broadcom (VMware) ESXi

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No

© Acronis International GmbH, 2003-2025

Carga de trabajo de destino	Compatible
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Máquina virtual de Microsoft Azure

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Máquina virtual Microsoft Hyper-V

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*

© Acronis International GmbH, 2003-2025

Carga de trabajo de destino	Compatible
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Máquina virtual de Virtuozzo Hybrid Server

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Contenedor de Virtuozzo Hybrid Server

Carga de trabajo de destino	Compatible
Equipo físico	No
Máquina virtual Broadcom (VMware) ESXi	No

© Acronis International GmbH, 2003-2025

Carga de trabajo de destino	Compatible
Máquina virtual de Microsoft Azure	No
Máquina virtual Microsoft Hyper-V	No
Máquina virtual de Virtuozzo Hybrid Server	No
Contenedor de Virtuozzo Hybrid Server	Sí
Equipo virtual de Virtuozzo Hybrid Infrastructure	No
Máquina virtual de Scale Computing HyperCore	No
Máquina virtual de RHV/oVirt	No
Equipo virtual Nutanix	No
Máquina virtual de Proxmox	No
Contenedor de Proxmox	No

Equipo virtual de Virtuozzo Hybrid Infrastructure

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

© Acronis International GmbH, 2003-2025

Máquina virtual de Scale Computing HyperCore

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Máquina virtual de Red Hat Virtualization/oVirt

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

© Acronis International GmbH, 2003-2025

Equipo virtual Nutanix

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

Máquina virtual de Proxmox

Carga de trabajo de destino	Compatible
Equipo físico	Sí
Máquina virtual Broadcom (VMware) ESXi	Sí
Máquina virtual de Microsoft Azure	Sí
Máquina virtual Microsoft Hyper-V	Sí*
Máquina virtual de Virtuozzo Hybrid Server	Sí
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	Sí
Máquina virtual de Scale Computing HyperCore	Sí
Máquina virtual de RHV/oVirt	Sí
Equipo virtual Nutanix	Sí
Máquina virtual de Proxmox	Sí
Contenedor de Proxmox	No

© Acronis International GmbH, 2003-2025

Contenedor de Proxmox

Carga de trabajo de destino	Compatible
Equipo físico	No
Máquina virtual Broadcom (VMware) ESXi	No
Máquina virtual de Microsoft Azure	No
Máquina virtual Microsoft Hyper-V	No
Máquina virtual de Virtuozzo Hybrid Server	No
Contenedor de Virtuozzo Hybrid Server	No
Equipo virtual de Virtuozzo Hybrid Infrastructure	No
Máquina virtual de Scale Computing HyperCore	No
Máquina virtual de RHV/oVirt	No
Equipo virtual Nutanix	No
Máquina virtual de Proxmox	No
Contenedor de Proxmox	Sí

Nota
No se hace copia de seguridad de la configuración de Arranque seguro. Si Arranque seguro está habilitado en el equipo original, la máquina virtual recuperada como un nuevo equipo no se iniciará. Para iniciar el equipo recuperado, deshabilite Arranque seguro en la consola de la MV después de la recuperación.

Nota

- * Los equipos basados en EFI se recuperan como máquinas virtuales de segunda generación.
- * No puede recuperar máquinas virtuales macOS en servidores Hyper-V porque Hyper-V no es compatible con macOS. Puede recuperar equipos virtuales MacOS en servidores VMware que estén instalados en un hardware de Mac.

Recuperación multiplataforma mediante dispositivos de arranque

Puede realizar una recuperación multiplataforma mediante el uso de dispositivos de arranque.

Le recomendamos que utilice el dispositivo de arranque en lugar de la consola de Cyber Protect en los siguientes casos:

- Realizar una migración que no es compatible a nivel nativo.

© Acronis International GmbH, 2003-2025

Por ejemplo, utilice un medio de arranque para recuperar una máquina física o una máquina virtual que no sea Virtuozzo Hybrid Server como una máquina virtual Virtuozzo Hybrid Server en un host Virtuozzo.

- Realizar la migración de un equipo Linux que contenga volúmenes lógicos (LVM).
  Utilice Agente para Linux o un dispositivo de arranque para crear la copia de seguridad y utilice dispositivos de arranque para recuperar la copia de seguridad.
- Proporcionar los controladores del hardware específico que sea fundamental para la capacidad de arranque del sistema.
  Cree un dispositivo de arranque que pueda utilizar los controladores necesarios. Para obtener más información, consulte "Bootable Media Builder" (p. 985).

Recuperación de equipos físicos

Puede recuperar una copia de seguridad a nivel de disco de un equipo físico a otro equipo físico o a una máquina virtual. Por ejemplo, una copia de seguridad a nivel de disco es una copia de seguridad de **todo el equipo** o una copia de seguridad de **discos/volúmenes** que contiene el disco del sistema y el disco de arranque.

Limitaciones

- En la consola de Cyber Protect no puede recuperar copias de seguridad de equipos que están registrados en inquilinos de clientes en el modo de cumplimiento. Consulte "Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento" (p. 1570).
- En la consola de Cyber Protect, no puede recuperar copias de seguridad de equipos físicos de macOS en otro equipo físico.
- No puede recuperar copias de seguridad de equipos físicos de macOS a una máquina virtual.
- Durante una recuperación a una máquina virtual, Cyber Protect detiene la máquina virtual de destino sin un aviso. Después de la recuperación, debe reiniciar esta máquina manualmente. Puede cambiar el comportamiento predeterminado en **Opciones de recuperación** > **Administración de energía de máquina virtual**.

Si desea recuperar uno de los siguientes, utilice el dispositivo de arranque en lugar de la consola de Cyber Protect:

- Un equipo físico que ejecute macOS.

  Nota
  No puede recuperar copias de seguridad a nivel de disco de equipos Mac basados en Intel en equipos Mac que usen procesadores Apple Silicon, ni viceversa. Puede recuperar archivos y carpetas.

- Un equipo en un inquilino de cliente en el modo de cumplimiento.
- Cualquier sistema operativo en un equipo desde cero o en un equipo offline.

© Acronis International GmbH, 2003-2025

- La estructura de los volúmenes lógicos. Por ejemplo, los volúmenes creados por Logical Volume Manager en Linux. Con el dispositivo de arranque, puede volver a crear automáticamente la estructura del volumen lógico.

Para obtener más información acerca de la recuperación de equipos mediante un dispositivo de arranque, consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

Recuperación de un equipo físico como un equipo físico

Puede recuperar una copia de seguridad a nivel de disco de un equipo físico al equipo original o a un equipo nuevo.

Este procedimiento describe la recuperación desde la consola de Cyber Protect. De forma alternativa, puede utilizar un dispositivo de arranque para recuperar una copia de seguridad (incluida una copia de seguridad de un equipo offline) en un equipo físico. Para obtener más información, consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

Pasos para recuperar un equipo físico como un equipo físico

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
     - Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
     - Seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona un equipo de destino de forma automática.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. Seleccione un equipo en línea y haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025

5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] Configure la asignación de discos entre el equipo incluido en la copia de seguridad y el de destino.
   a. [Pasos para configurar la asignación a nivel de disco]
      i. Haga clic en **Asignación de discos**.
      ii. Configure la asignación de discos entre el equipo incluido en la copia de seguridad y el de destino.
      iii. Haga clic en **Listo**.
   b. [Pasos para configurar la asignación a nivel de volumen]
      i. Haga clic en **Asignación de discos** y, a continuación, en la esquina superior derecha, haga clic en **Cambiar a asignación de volúmenes**.
      ii. Configure la asignación de volumenes entre el equipo incluido en la copia de seguridad y el de destino.
      iii. Haga clic en **Listo**.
7. [Opcional] [Sólo disponible para equipos Windows] Para asegurarse de que los datos recuperados estén libres de malware, active el interruptor **Recuperación segura**. Para obtener más información, consulte "Recuperación segura" (p. 719).
8. Haga clic en **Iniciar recuperación**.
9. [Opcional] Si prefiere reiniciar el equipo manualmente después de la recuperación, desactive la casilla de verificación **Reinicie el equipo automáticamente, si es necesario**. Para obtener, consulte "Recuperación con reinicio" (p. 704).
10. Para confirmar que desea sobrescribir los discos del equipo de destino, haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Recuperación de un equipo físico en una máquina virtual

Puede recuperar una copia de seguridad a nivel de disco de un equipo físico a una máquina virtual. Esta operación se denomina recuperación multiplataforma (migración de equipos). Para obtener más información, consulte "Recuperación multiplataforma" (p. 655).

Requisitos previos

- Un agente para el hipervisor correspondiente está instalado en su entorno. Por ejemplo, la recuperación a una máquina virtual de VMware ESXi requiere un agente para VMware que está instalado y registrado en la consola de Cyber Protect.

Para recuperar un equipo físico como un equipo virtual

Los procedimientos se enumeran según el tipo de la máquina virtual de destino.

VMware ESXi

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
     - Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
     - Seleccione un punto de recuperación.

     Nota
     También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Broadcom (VMware) ESXi**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025

6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Almacén de datos** y seleccione un almacén de datos.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Azure

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
     - Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
     - Seleccione un punto de recuperación.

     Nota
     También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

© Acronis International GmbH, 2003-2025

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Microsoft Azure**.
      a. [Realizar una recuperación en un equipo nuevo]
         i. Seleccione **Equipo nuevo**.
         ii. Seleccione una suscripción de Azure, una región y un grupo de recursos.
         iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
         iv. Haga clic en **Aceptar**.
      b. [Pasos para realizar la recuperación al equipo original]
         i. Seleccione **Equipo original**.
         ii. Haga clic en **Aceptar**.
6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el tipo de almacenamiento de cada disco de destino, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Seleccione el tipo de almacenamiento.
      El almacenamiento con redundancia local (LRS) y el almacenamiento con redundancia de zona (ZRS) están disponibles.
      iv. Haga clic en **Listo**.
   b. Para cambiar el tipo y la zona de disponibilidad, el tamaño de la memoria y las conexiones de red (incluidas las subredes y los grupos de seguridad) de la máquina virtual, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en el equipo original] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Hyper-V

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
     - Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
     - Seleccione un punto de recuperación.

     Nota
     También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Microsoft Hyper-V**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025

6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Ruta** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el almacenamiento, la interfaz o el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Configure de los ajustes.
      iv. Haga clic en **Listo**.
   d. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Virtuozzo Hybrid Infrastructure

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.

© Acronis International GmbH, 2003-2025

- Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
- Seleccione un punto de recuperación.

Nota
También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Virtuozzo Hybrid Infrastructure**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales.
   a. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   b. Para cambiar la directiva de almacenamiento del disco de destino, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Seleccione la directiva de almacenamiento para el disco.
      iv. Haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

c. Para cambiar los adaptadores de red, haga clic en **Configuración de la máquina virtual**.
   i. Configure de los ajustes.
   ii. Haga clic en **Aceptar**.

8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Scale Computing HC3

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
     - Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
     - Seleccione un punto de recuperación.

     Nota
     También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Scale Computing HC3**.
   c. [Realizar una recuperación en un equipo nuevo]

© Acronis International GmbH, 2003-2025

i. Seleccione **Equipo nuevo**.

ii. Seleccione un host.

iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.

iv. Haga clic en **Aceptar**.

d. [Pasos para realizar la recuperación en un equipo existente]

i. Seleccione **Equipo existente**.

ii. Seleccione el equipo de destino.

iii. Haga clic en **Aceptar**.

6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales.
   a. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   b. Para cambiar el contenedor de almacenamiento, la interfaz o el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Configure de los ajustes.
      iv. Haga clic en **Listo**.
8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

oVirt

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]

© Acronis International GmbH, 2003-2025

- En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
- Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
- Seleccione un punto de recuperación.

Nota
También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **oVirt**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Dominio de almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

© Acronis International GmbH, 2003-2025

Nutanix

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]
     - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
     - Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
     - Seleccione un punto de recuperación.

     Nota
     También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Nutanix**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.

© Acronis International GmbH, 2003-2025

ii. Seleccione el equipo de destino.

iii. Haga clic en **Aceptar**.

6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales.
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Contenedor de almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el contenedor de almacenamiento o la interfaz, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Configure de los ajustes.
      iv. Haga clic en **Listo**.
   d. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Proxmox

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - [Para equipos en línea] En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

     Nota
     Los puntos de recuperación se filtran por almacenamiento de copia de seguridad.

   - [Para equipos en línea y offline] En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
   - [Para equipos sin conexión] [Si la ubicación de la copia de seguridad es el almacenamiento en la nube o un almacenamiento compartido al que otros agentes pueden acceder]

© Acronis International GmbH, 2003-2025

- En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar y haga clic en **Recuperación**.
- Haga clic en **Seleccionar equipo**, seleccione un equipo de destino que esté en línea y, a continuación, haga clic en **Aceptar**.
- Seleccione un punto de recuperación.

Nota
También puede recuperar un equipo offline mediante el uso de un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo virtual**.
5. Seleccione un equipo de destino.
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Proxmox**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Nota

- Para recuperar un disco como disco de tipo VirtIO, en las opciones de recuperación, seleccione NVME.
- Durante una recuperación a un nuevo equipo, los discos VDMK se recuperan como discos QCOW2 o discos RAW (si cambia el tipo de aprovisionamiento a grueso).

c. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
   i. Configure de los ajustes.
   ii. Haga clic en **Aceptar**.

8. Haga clic en **Iniciar recuperación**
9. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Recuperación del equipos virtuales

Puede recuperar una copia de seguridad a nivel de disco de una máquina virtual a un equipo físico o a otra máquina virtual. Por ejemplo, una copia de seguridad a nivel de disco es una copia de seguridad de **todo el equipo** o una copia de seguridad de **discos/volumen** que contiene el disco del sistema y el disco de arranque.

Limitaciones

- En la consola de Cyber Protect no puede recuperar copias de seguridad de equipos que están registrados en inquilinos de clientes en el modo de cumplimiento. Consulte "Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento" (p. 1570).
- Durante una recuperación a una máquina virtual, Cyber Protect detiene la máquina virtual de destino sin un aviso. Después de la recuperación, debe reiniciar esta máquina manualmente. Puede cambiar el comportamiento predeterminado en **Opciones de recuperación** > **Administración de energía de máquina virtual**.
- Puede recuperar una copia de seguridad de una máquina virtual en un equipo físico si la configuración de disco del equipo de destino coincide exactamente con la configuración de disco de la copia de seguridad. De forma alternativa, puede realizar una migración de virtual a físico mediante un dispositivo de arranque. Consulte "Recuperar discos usando dispositivos de arranque" (p. 693).
- No puede recuperar máquinas virtuales macOS en servidores Hyper-V porque Hyper-V no es compatible con macOS. Puede recuperar equipos virtuales MacOS en un servidor VMware que esté instalado en un hardware de Mac.

© Acronis International GmbH, 2003-2025

Recuperación de una máquina virtual como un equipo físico

Puede recuperar una copia de seguridad a nivel de disco de una máquina virtual a un equipo físico. Esta operación se denomina recuperación multiplataforma (migración de equipos). Para obtener más información, consulte "Recuperación multiplataforma" (p. 655).

El siguiente procedimiento describe la recuperación desde la consola de Cyber Protect. De forma alternativa, puede utilizar un dispositivo de arranque para recuperar una copia de seguridad de una máquina virtual en un equipo físico. Para obtener más información, consulte "Recuperar discos usando dispositivos de arranque" (p. 693).

Pasos para recuperar una máquina virtual como un equipo físico

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. En **Recuperar a**, seleccione **Equipo físico**.
   Se selecciona un equipo de destino de forma automática.
5. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. Seleccione un equipo en línea y haga clic en **Aceptar**.
6. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
7. [Opcional] Configure la asignación de discos entre el equipo incluido en la copia de seguridad y el de destino.
   a. [Pasos para configurar la asignación a nivel de disco]
      i. Haga clic en **Asignación de discos**.
      ii. Configure la asignación de discos entre el equipo incluido en la copia de seguridad y el de destino.
      iii. Haga clic en **Listo**.
   b. [Pasos para configurar la asignación a nivel de volumen]
      i. Haga clic en **Asignación de discos** y, a continuación, en la esquina superior derecha, haga clic en **Cambiar a asignación de volúmenes**.
      ii. Configure la asignación de volumenes entre el equipo incluido en la copia de seguridad y el de destino.
      iii. Haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Nota
Puede seleccionar discos o volúmenes individuales para la recuperación. Asegúrese de que la configuración del disco o volúmen del equipo incluido en la copia de seguridad coincida exactamente con la configuración del disco o volúmen del equipo de destino.

8. [Opcional] [Sólo disponible para equipos Windows] Para asegurarse de que los datos recuperados estén libres de malware, active el interruptor **Recuperación segura**. Para obtener más información, consulte "Recuperación segura" (p. 719).
9. Haga clic en **Iniciar recuperación**
10. [Opcional] Si prefiere reiniciar el equipo manualmente después de la recuperación, desactive la casilla de verificación **Reinicie el equipo automáticamente, si es necesario**. Para obtener, consulte "Recuperación con reinicio" (p. 704).
11. Para confirmar que desea sobrescribir los discos del equipo de destino, haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Recuperación de una máquina virtual como máquina virtual

Puede recuperar una copia de seguridad de una máquina virtual al hipervisor original o a un tipo diferente de hipervisor. La recuperación a un tipo diferente de hipervisor se denomina recuperación multiplataforma (migración de máquinas). Para obtener más información, consulte "Recuperación multiplataforma" (p. 655).

La recuperación a una máquina virtual en la que no está instalado un agente de protección se realiza a nivel del hipervisor. Esta es una recuperación sin agente.

La recuperación a una máquina virtual en la que se ha instalado un agente de protección es una recuperación basada en agente. Este tipo de recuperación es igual que una recuperación a un equipo físico.

Requisitos previos

- Un agente para el hipervisor correspondiente está instalado en su entorno. Por ejemplo, la recuperación a una máquina virtual de VMware ESXi requiere un agente para VMware que está instalado y registrado en la consola de Cyber Protect.

Pasos para recuperar una máquina virtual como una máquina virtual

Los procedimientos se enumeran según el tipo de la máquina virtual de destino.

VMware ESXi

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).

© Acronis International GmbH, 2003-2025

- En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).

2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **VMware ESXi**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Almacén de datos** y seleccione un almacén de datos.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Azure

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Microsoft Azure**.
      a. [Realizar una recuperación en un equipo nuevo]
         i. Seleccione **Equipo nuevo**.
         ii. Seleccione una suscripción de Azure, una región y un grupo de recursos.
         iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
         iv. Haga clic en **Aceptar**.
      b. [Pasos para realizar la recuperación al equipo original]
         i. Seleccione **Equipo original**.
         ii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el tipo de almacenamiento de cada disco de destino, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Seleccione el tipo de almacenamiento.
      El almacenamiento con redundancia local (LRS) y el almacenamiento con redundancia de zona (ZRS) están disponibles.
      iv. Haga clic en **Listo**.
   b. Para cambiar el tipo y la zona de disponibilidad, el tamaño de la memoria y las conexiones de red (incluidas las subredes y los grupos de seguridad) de la máquina virtual, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**

© Acronis International GmbH, 2003-2025

8. [Al recuperar en el equipo original] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Hyper-V

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Microsoft Hyper-V**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Ruta** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el almacenamiento, la interfaz o el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.

© Acronis International GmbH, 2003-2025

iii. Configure de los ajustes.

iv. Haga clic en **Listo**.

d. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.

i. Configure de los ajustes.

ii. Haga clic en **Aceptar**.

7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Virtuozzo

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Virtuozzo**.

   Nota
   Solo se puede recuperar una máquina virtual de Virtuozzo a una máquina virtual de Virtuozzo.

   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025

5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Ruta** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el almacenamiento, la interfaz o el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Configure de los ajustes.
      iv. Haga clic en **Listo**.
   d. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Virtuozzo Hybrid Infrastructure

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.

   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Virtuozzo Hybrid Infrastructure**.
   c. [Realizar una recuperación en un equipo nuevo]

© Acronis International GmbH, 2003-2025

i. Seleccione **Equipo nuevo**.

ii. Seleccione un host.

iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.

iv. Haga clic en **Aceptar**.

d. [Pasos para realizar la recuperación en un equipo existente]

i. Seleccione **Equipo existente**.

ii. Seleccione el equipo de destino.

iii. Haga clic en **Aceptar**.

5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales.
   a. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   b. Para cambiar la directiva de almacenamiento del disco de destino, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Seleccione la directiva de almacenamiento para el disco.
      iv. Haga clic en **Listo**.
   c. Para cambiar los adaptadores de red, haga clic en **Configuración de la máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Scale Computing HC3

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.

© Acronis International GmbH, 2003-2025

3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Scale Computing HC3**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales.
   a. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   b. Para cambiar el contenedor de almacenamiento, la interfaz o el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Configure de los ajustes.
      iv. Haga clic en **Listo**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

oVirt

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).

© Acronis International GmbH, 2003-2025

2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **oVirt**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Dominio de almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Nutanix

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona la máquina virtual original como equipo de destino.

© Acronis International GmbH, 2003-2025

3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Nutanix**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales.
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Contenedor de almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el contenedor de almacenamiento o la interfaz, haga clic en **Asignación de discos**.
      i. En la sección disco de destino, haga clic en **Modificar**.
      ii. Haga clic en el icono de engranaje.
      iii. Configure de los ajustes.
      iv. Haga clic en **Listo**.
   d. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

© Acronis International GmbH, 2003-2025

Proxmox

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.

   Se selecciona la máquina virtual original como equipo de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Pasos para cambiar el equipo de destino:
   a. Haga clic en **Equipo de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Proxmox**.
   c. [Realizar una recuperación en un equipo nuevo]
      i. Seleccione **Equipo nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del equipo**, especifique un nombre para el equipo nuevo.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un equipo existente]
      i. Seleccione **Equipo existente**.
      ii. Seleccione el equipo de destino.
      iii. Haga clic en **Aceptar**.
5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.

Nota
- Para recuperar un disco como disco de tipo VirtIO, en las opciones de recuperación, seleccione NVME.
- Durante una recuperación a un nuevo equipo, los discos VDMK se recuperan como discos QCOW2 o discos RAW (si cambia el tipo de aprovisionamiento a grueso).

© Acronis International GmbH, 2003-2025

c. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de máquina virtual**.
   i. Configure de los ajustes.
   ii. Haga clic en **Aceptar**.

7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un equipo existente] Para confirmar que desea sobrescribir el equipo de destino, haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Recuperación de contenedores

Puede recuperar un contenedor respaldado en el contenedor original o en un nuevo contenedor en el mismo hipervisor.

La recuperación multiplataforma no es compatible con los contenedores.

Para recuperar un contenedor

Contenedor Virtuozzo

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona el contenedor original como contenedor de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Para cambiar el contenedor de destino:
   a. Haga clic en **Contenedor de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Virtuozzo**.
   c. [Para realizar la recuperación en un nuevo contenedor]
      i. Seleccione **Contedor nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del contenedor**, especifique un nombre para el nuevo contenedor.
      iv. Haga clic en **Aceptar**.
   d. [Pasos para realizar la recuperación en un contenedor existente]
      i. Seleccione **Contenedor existente**.

© Acronis International GmbH, 2003-2025

ii. Seleccione el contenedor de destino.

iii. Haga clic en **Aceptar**.

5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de contenedor**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un contenedor existente] Para confirmar que desea sobrescribir el contenedor de destino, haga clic en **Iniciar recuperación**.

Contenedor de Proxmox

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - En la pestaña **Dispositivos**, seleccione un equipo cuya copia de seguridad desee restaurar, haga clic en **Recuperación** y seleccione una copia de seguridad (punto de recuperación).
   - En la pestaña **Almacenamiento de la copia de seguridad**, seleccione un archivo de copia de seguridad y después seleccione una copia de seguridad (punto de recuperación).
2. Haga clic en **Recuperar** > **Todo el equipo**.
   Se selecciona el contenedor original como contenedor de destino.
3. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
4. [Opcional] Para cambiar el contenedor de destino:
   a. Haga clic en **Contenedor de destino**.
   b. [Si hay varios hipervisores disponibles] Seleccione **Proxmox**.
   c. [Para realizar la recuperación en un nuevo contenedor]
      i. Seleccione **Contedor nuevo**.
      ii. Seleccione un host.
      iii. En **Nombre del contenedor**, especifique un nombre para el nuevo contenedor.
      iv. Haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025

d. [Pasos para realizar la recuperación en un contenedor existente]
   i. Seleccione **Contenedor existente**.
   ii. Seleccione el contenedor de destino.
   iii. Haga clic en **Aceptar**.

5. [Si se le solicita] Especifique las credenciales para acceder al almacenamiento de copia de seguridad y haga clic en **Aceptar**.
6. [Opcional] [Al recuperar en un equipo nuevo] Configure las opciones adicionales:
   a. Para cambiar el almacenamiento de la máquina virtual, haga clic en **Almacenamiento** y seleccione un almacenamiento.
   b. Para cambiar la asignación de disco o excluir algunos de los discos incluidos en la copia de seguridad de la recuperación, haga clic en **Asignación de discos**.
      i. Configure la asignación de discos o seleccione los discos que desea recuperar.
      ii. Haga clic en **Listo**.
   c. Para cambiar el tamaño de la memoria, el número de procesadores virtuales o las conexiones a redes virtuales del equipo de destino, haga clic en **Configuración de contenedor**.
      i. Configure de los ajustes.
      ii. Haga clic en **Aceptar**.
7. Haga clic en **Iniciar recuperación**
8. [Al recuperar en un contenedor existente] Para confirmar que desea sobrescribir el contenedor de destino, haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Recuperar discos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de inicio, consulte "Creación de un dispositivo de arranque físico" (p. 984).

Nota
No puede recuperar copias de seguridad a nivel de disco de equipos Mac basados en Intel en equipos Mac que usen procesadores Apple Silicon, ni viceversa. Puede recuperar archivos y carpetas.

Para recuperar discos usando dispositivos de arranque.

1. Inicie el equipo de destino usando dispositivos de arranque.
2. [Solo cuando se recupera un Mac] Si recupera volúmenes o discos con formato APFS a un equipo no original o en una recuperación completa, vuelva a crear la configuración del disco original manualmente:

© Acronis International GmbH, 2003-2025

a. Haga clic en **Disk Utility**.

b. Borre y dé formato al disco de destino como APFS. Para obtener instrucciones, consulte https://support.apple.com/en-us/HT208496#erasedisk.

c. Vuelva a crear la configuración del disco original. Para obtener instrucciones, consulte https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.

d. Haga clic en **Disk Utility** > **Salir de Disk Utility**.

3. Haga doble clic en **Gestionar este equipo a nivel local** o en **Dispositivos de rescate de arranque**, dependiendo del tipo de dispositivo que use.
4. Si en la red hay un servidor proxy habilitado, haga clic en **Herramientas** > **Servidor proxy** y, a continuación, especifique el nombre de servidor/dirección IP, el puerto y las credenciales del servidor proxy. De lo contrario, omita este paso.
5. [Opcional] Al recuperar Windows o Linux, haga clic en **Herramientas** > **Registrar equipo en el servicio de Cyber Protection** y especifique el token de registro que haya obtenido al descargar el medio. Si lleva a cabo esta acción, no tendrá que introducir ninguna credencial ni ningún código de registro para acceder al almacenamiento en la nube, como se describe en el paso 8.
6. En la pantalla de inicio, haga clic en **Recuperar**.
7. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
8. Especifique la ubicación de la copia de seguridad:
   - Para recuperar datos desde un almacenamiento en la cloud, seleccione **Almacenamiento en la nube**. Especifique las credenciales de la cuenta a la que está asignado el equipo del que se hizo la copia de seguridad.

     Al recuperar Windows o Linux, tiene la opción de solicitar un código de registro y usarlo en lugar de las credenciales. Haga clic en **Utilizar código de registro** > **Solicitar el código**. El software muestra el vínculo y el código de registro. Puede copiar esta información y llevar a cabo los pasos de registro en un equipo distinto. El código de registro tiene una validez de una hora.
   - Para recuperar datos desde una carpeta local o de red, vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.
   - Para llevar a cabo la recuperación desde las ubicaciones de copia de seguridad en el almacenamiento en la nube pública como Microsoft Azure, Amazon S3, Wasabi o compatible con S3, primero haga clic en **Registrar medios en el servicio Cyber Protection** y luego configure la recuperación utilizando la interfaz web. Para obtener más información sobre la gestión de medios de forma remota a través de la interfaz web, consulte "Operaciones remotas con soportes de arranque" (p. 1003).

   Haga clic en **Aceptar** para confirmar su selección.
9. Seleccione la copia de seguridad desde la que desea recuperar los datos. Si se le pide, escriba la contraseña para la copia de seguridad.
10. En **Contenido de las copias de seguridad**, seleccione los discos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.

© Acronis International GmbH, 2003-2025

11. En **Dónde recuperar**, el software asigna automáticamente los discos seleccionados a los discos de destino.
    Si la asignación no se realiza con éxito o si no queda satisfecho con el resultado de asignación, puede volver a asignar los discos manualmente.

    Nota
    Cambiar la distribución de discos puede afectar a la capacidad de arranque del sistema operativo. Utilice la distribución del disco del equipo original, a menos que esté completamente seguro de que se realizará correctamente.

12. [Al recuperar un equipo Linux] Si el equipo incluido en la copia de seguridad tenía volúmenes lógicos (LVM) y quiere reproducir la estructura LVM original:
    a. Asegúrese de que el número y capacidad de los discos en el equipo de destino igualan o exceden los del equipo original. A continuación, haga clic en **Aplicar RAID/LVM**.
    b. Revise la estructura de volumen y luego haga clic en **Aplicar RAID/LVM** para crearla.
13. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
14. Haga clic en **Aceptar** para comenzar la recuperación.

Recuperación de archivos

Recuperación de archivos en la consola de Cyber Protect

Nota
En la consola de Cyber Protect no puede recuperar copias de seguridad en inquilinos en modo cumplimiento. Consulte "Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento" (p. 1570).

1. Seleccione el equipo que contenía originalmente los datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione el punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
   Si el equipo seleccionado es físico y no está conectado a Internet, no se muestran los puntos de recuperación. Realice una de las siguientes operaciones:
   - [Recomendado] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo de destino que tenga conexión a Internet y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.
   - Descargue los archivos desde el almacenamiento en la cloud.
   - Use dispositivos de arranque.

© Acronis International GmbH, 2003-2025

4. Haga clic en **Recuperar** > **Archivos/carpetas**.
5. Vaya hasta la carpeta requerida o utilice la barra de búsqueda para obtener la lista de los archivos y carpetas deseados.

   La búsqueda es independiente del idioma.

   Puede utilizar uno o más caracteres comodín (* y ?). Para obtener más información sobre el uso de los caracteres comodín, consulte la sección "Filtros de archivo (inclusiones y exclusiones)" (p. 607).

   Nota
   La búsqueda no está disponible para las copias de seguridad a nivel de disco que se guardan en el almacenamiento en la nube.
6. Seleccione los archivos que desea recuperar.
7. Si desea guardar los archivos en un archivo .zip, haga clic en **Descargar**, seleccione la ubicación en la que se guardarán los datos y, a continuación, haga clic en **Guardar**. De lo contrario, omita este paso.

   La acción de descarga no está disponible si su selección incluye carpetas o si el tamaño total de los archivos seleccionados supera los 100 MB. Para recuperar mayores cantidades de datos de la nube, utilice el procedimiento "Descarga de archivos en la consola de Web Restore" (p. 697).
8. Haga clic en **Recuperar**.

   En **Recuperar a**, haga clic para seleccionar el destino de la operación de recuperación o deje el destino predeterminado. El destino predeterminado varía según el origen de la copia de seguridad.

   Los siguientes destinos están disponibles:
   - El equipo de origen (si un agente de protección está instalado en él).

     Es el equipo que contenía originalmente los archivos que desea recuperar.
   - Otros equipos en los que está instalado un agente de protección: equipos físicos, máquinas virtuales y host de virtualización en los que está instalado un agente de protección, o dispositivos virtuales.

     Puede recuperar archivos en equipos físicos, máquinas virtuales y host de virtualización en los que está instalado un agente de protección. No puede recuperar archivos en máquinas virtuales en las que no esté instalado un agente de protección (excepto en máquinas virtuales Virtuozzo).
   - Contenedores o máquinas virtuales Virtuozzo.

     Puede recuperar archivos en contenedores y máquinas virtuales Virtuozzo con algunas limitaciones. Para obtener más información acerca de ellas, consulte "Limitaciones para recuperar archivos en la consola de Cyber Protect" (p. 702).
9. En **Ruta**, seleccione el destino de la recuperación. Puede seleccionar una de las siguientes opciones:
   - [Al recuperar en el equipo original] La ubicación original.
   - Una carpeta local o el almacenamiento adjunto de forma local en un equipo de destino.

© Acronis International GmbH, 2003-2025

Nota
No se pueden usar vínculos simbólicos.

- Una carpeta de red accesible desde el equipo de destino
  Por ejemplo, al recuperar archivos de una máquina virtual de Microsoft Azure, la carpeta de red debe ser accesible para el agente para Azure desplegado en la máquina virtual.

10. Haga clic en **Iniciar recuperación**.
11. Seleccione una de las opciones de sobreescritura de archivos:
    - **Sobrescribir archivos existentes**
    - **Sobrescribir un archivo existente si es más antiguo**
    - **No sobrescribir archivos existentes**

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Descarga de archivos en la consola de Web Restore

En la consola de Web Restore, puede navegar por el almacenamiento en la nube, ver el contenido de las copias de seguridad, y descargar archivos y carpetas con copia de seguridad.

La consola de Web Restore solo es accesible para las cuentas de usuario de nivel de cliente con los siguientes roles:

- Administrador de la empresa
- Administrador de Protección
- Usuario de Protección

Todas las cuentas pueden acceder únicamente a sus propias copias de seguridad.

Las cuentas de usuario de nivel de partner no pueden acceder a la consola de Web Restore.

Limitaciones

- No puede descargar discos con copia de seguridad, volúmenes ni puntos de recuperación completos.
- Cuando navega por las copias de seguridad a nivel de disco, no se muestran los volúmenes lógicos (como LVM y LDM).
- No puede navegar por las copias de seguridad del estado del sistema, las bases de datos SQL ni las bases de datos de Exchange.

Para descargar archivos y carpetas del almacenamiento en la nube

1. En la consola de Cyber Protection, seleccione la carga de trabajo requerida y haga clic en **Recuperación**.
2. [Si hay varias ubicaciones de copia de seguridad disponibles] Seleccione la ubicación de la copia de seguridad y haga clic en **Otras formas de recuperar**.

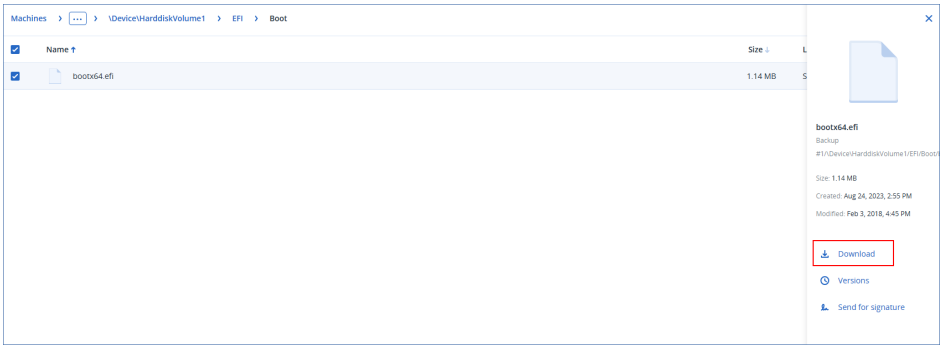
© Acronis International GmbH, 2003-2025

3. Haga clic en **Descargar archivos**.
4. En **Equipos**, haga clic en el nombre del recurso informático y, luego, en el archivo de copia de seguridad.

   Un archivo de copia de seguridad contiene una o más copias de seguridad (puntos de recuperación).
5. Haga clic en el número de copia de seguridad (punto de recuperación) desde el que desea descargar archivos o carpetas y, luego, navegue hasta los elementos requeridos.
6. Seleccione las casillas de verificación junto a los elementos que desee descargar.

   Nota
   Si selecciona varios elementos, se descargarán como archivo ZIP.

7. Haga clic en **Descargar**.



Verificar la autenticidad del archivo con Notary Service

Si se ha habilitado la notarización durante la copia de seguridad, puede verificar la autenticidad de un archivo del que se ha realizado la copia de seguridad.

Para verificar la autenticidad del archivo

1. Seleccione el archivo tal como se describe en los pasos 1 a 6 de la sección "Recuperación de archivos usando la interfaz", o los pasos 1 a 5 de la sección "Descarga de archivos desde el almacenamiento en la nube".
2. Asegúrese de que el archivo seleccionado esté marcado con el siguiente icono:  . Esto significa que el archivo está notarizado.
3. Realice uno de los siguientes procedimientos:
   - Haga clic en **Verificar**.

     El software comprueba la autenticidad del archivo y muestra el resultado.
   - Haga clic en **Obtener certificado**.

     Se abre un certificado que confirma la notarización del archivo en una ventana de navegador web. La ventana también incluye instrucciones que le permiten verificar la autenticidad del archivo manualmente.

© Acronis International GmbH, 2003-2025

Firma de un archivo con ASign

Nota
Esta función está disponible con el paquete Advanced Backup.

ASign es un servicio que permite que diversas personas puedan firmar de forma electrónica un archivo del que se ha realizado una copia de seguridad. Esta función solo está disponible para copias de seguridad a nivel de archivo almacenadas en el almacenamiento en la cloud.

Solo puede firmarse una versión del archivo al mismo tiempo. Si la copia de seguridad del archivo se ha realizado varias veces debe elegir la versión que firmará, y solo se firmará esta versión.

Por ejemplo, se puede usar ASign para firmar electrónicamente los siguientes archivos:

- Contratos de concesión o de alquiler
- Contratos de ventas
- Contratos de adquisición de activos
- Contratos de préstamos
- Formularios de permisos
- Documentos financieros
- Documentos del seguro
- Exenciones de responsabilidad
- Documentos de salud
- Documentos de investigación
- Certificados de autenticidad del producto
- Acuerdos de confidencialidad
- Cartas de oferta
- Acuerdos de confidencialidad
- Acuerdos de contratista independiente

Para firmar una versión del archivo

1. Seleccione el archivo tal como se describe en los pasos 1 a 6 de la sección "Recuperación de archivos usando la interfaz", o los pasos 1 a 5 de la sección "Descarga de archivos desde el almacenamiento en la nube".
2. Asegúrese de que la fecha y la hora seleccionadas en el panel de la izquierda son correctas.
3. Haga clic en **Firmar esta versión del archivo**.
4. Especifique la contraseña de la cuenta de almacenamiento en la nube en la que se ha guardado la copia de seguridad. El inicio de sesión de la cuenta aparece en la ventana emergente.
   La interfaz del servicio ASign se abrirá en una ventana del navegador web.

© Acronis International GmbH, 2003-2025

5. Agregue otras firmas especificando sus direcciones de correo electrónico. No es posible añadir o eliminar firmas después de enviar las invitaciones, así que compruebe que la lista incluye todas las firmas que necesita.
6. Haga clic en **Invitar a firmar** para enviar invitaciones a los firmantes.

   Cada firmante recibe un mensaje de correo electrónico con la solicitud de la firma. Cuando todos los firmantes requeridos firman el archivo, este se certifica y firma mediante el servicio de notaría.

   Recibirá una notificación cuando cada firmante firme el archivo y cuando todo el proceso se haya completado. Puede acceder a la página web de ASign haciendo clic en **Ver detalles** en cualquiera de los mensajes de correo electrónico que reciba.
7. Una vez completado el proceso, vaya a la página web de ASign y haga clic en **Obtener documento** para descargar un documento .pdf que contiene:
   - La página del certificado de la firma con las firmas reunidas.
   - La página Seguimiento de control con historial de actividades: cuándo se envió la invitación a los firmantes, cuándo firmó el archivo cada firmante y otros datos.

Recuperación de archivos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de arranque, consulte "Crear dispositivos de arranque".

Para recuperar archivos mediante un dispositivo de arranque

1. Inicie el equipo de destino usando el dispositivo de arranque.
2. Haga doble clic en **Gestionar este equipo a nivel local** o en **Dispositivos de rescate de arranque**, dependiendo del tipo de dispositivo que use.
3. Si en la red hay un servidor proxy habilitado, haga clic en **Herramientas** > **Servidor proxy** y, a continuación, especifique el nombre de servidor/dirección IP, el puerto y las credenciales del servidor proxy. De lo contrario, omita este paso.
4. [Opcional] Al recuperar Windows o Linux, haga clic en **Herramientas** > **Registrar equipo en el servicio de Cyber Protection** y especifique el token de registro que haya obtenido al descargar el medio. Si lleva a cabo esta acción, no tendrá que introducir ninguna credencial ni ningún código de registro para acceder al almacenamiento en la nube, como se describe en el paso 7.
5. En la pantalla de inicio, haga clic en **Recuperar**.
6. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
7. Especifique la ubicación de la copia de seguridad:
   - Para recuperar datos desde un almacenamiento en la cloud, seleccione **Almacenamiento en la nube**. Especifique las credenciales de la cuenta a la que está asignado el equipo del que se hizo la copia de seguridad.

     Al recuperar Windows o Linux, tiene la opción de solicitar un código de registro y usarlo en lugar de las credenciales. Haga clic en **Utilizar código de registro** > **Solicitar el código**. El software muestra el vínculo y el código de registro. Puede copiar esta información y llevar a

© Acronis International GmbH, 2003-2025

cabo los pasos de registro en un equipo distinto. El código de registro tiene una validez de una hora.

- Para recuperar datos desde una carpeta local o de red, vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.
- Para llevar a cabo la recuperación desde las ubicaciones de copia de seguridad en el almacenamiento en la nube pública como Microsoft Azure, Amazon S3, Wasabi o compatible con S3, primero haga clic en **Registrar medios en el servicio Cyber Protection** y luego configure la recuperación utilizando la interfaz web. Para obtener más información sobre la gestión de medios de forma remota a través de la interfaz web, consulte "Operaciones remotas con soportes de arranque" (p. 1003).

Haga clic en **Aceptar** para confirmar su selección.

8. Seleccione la copia de seguridad desde la que desea recuperar los datos. Si se le pide, escriba la contraseña para la copia de seguridad.
9. En **Contenido de la copia de seguridad**, seleccione **Carpetas/archivos**.
10. Seleccione los datos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.
11. En **Dónde recuperar**, especifique una carpeta. Opcionalmente, puede prohibir la sobrescritura de versiones de archivos más recientes o excluir algunos archivos de la recuperación.
12. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
13. Haga clic en **Aceptar** para comenzar la recuperación.

Extraer archivos de copias de seguridad locales

Puede examinar el contenido de las copias de seguridad y extraer los archivos que necesite.

Requisitos

- Esta funcionalidad solo está disponible en Windows utilizando el Explorador de archivos.
- El sistema de archivos a los que se ha realizado una copia de seguridad debe ser uno de los siguientes: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS o HFS+.

Requisitos previos

- Debe instalarse un agente de protección en el equipo desde donde buscará una copia de seguridad.
- La copia de seguridad debe almacenarse en una carpeta local o una red compartida (SMB/CIFS).

Para extraer archivos desde una copia de seguridad

1. Busque la ubicación de la copia de seguridad utilizando el Explorador de archivos.
2. Haga doble clic en el archivo de copia de seguridad. Los nombres de los archivos se basan en la siguiente plantilla:

   ```
   <machine name> - <protection plan GUID>
   ```


© Acronis International GmbH, 2003-2025

3. Si la copia de seguridad está cifrada, introduzca la contraseña de cifrado. De lo contrario, omita este paso.
   El Explorador de archivos muestra los puntos de recuperación.
4. Haga doble clic en el punto de recuperación.
   El Explorador de archivos muestra los datos objeto de la copia de seguridad.
5. Busque la carpeta requerida.
6. Copie los archivos requeridos en cualquier carpeta del sistema de archivos.

Limitaciones para recuperar archivos en la consola de Cyber Protect

Inquilinos en el modo de cumplimiento

En la consola de Cyber Protect no puede recuperar copias de seguridad en inquilinos en modo cumplimiento. Consulte "Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento" (p. 1570).

Recuperación a contenedores o máquinas virtuales Virtuozzo

- El agente invitado QEMU se debe instalar en la máquina virtual de destino.
- [Solo aplicable en la recuperación en contenedores] Los puntos de montaje dentro de los contenedores no puede utilizarse como destino de la recuperación. Por ejemplo, no puede recuperar archivos en un segundo disco duro o un recurso NFS compartido montado en un contenedor.
- Al recuperar archivos en una máquina virtual de Windows, y si está habilitada la opción de recuperación de "Seguridad a nivel de archivo" (p. 715), el atributo de bit de archivo se configura para los archivos recuperados.
- Los archivos con caracteres que no son ANSI en el nombre se recuperan con nombres incorrectos en los equipos que ejecutan Windows Server 2012 o anterior y equipos con Windows 7 o anterior.
- Para recuperar archivos en máquinas virtuales de CentOS o Red Hat Enterprise Linux que ejecuten Virtuozzo Hybrid Server, debe editar el archivo `qemu-ga` como se indica a continuación:
  - En la máquina virtual de destino, vaya a `/etc/sysconfig/` y abra el archivo `qemu-ga` para editarlo.
  - Vaya a la siguiente línea y borre todo lo que aparece después del signo de igual (=):

    ```
    BLACKLIST_RPC=
    ```

  - Reinicie el agente invitado QEMU. Para ello, ejecute el siguiente comando:

    ```
    systemctl restart qemu-guest-agent
    ```


© Acronis International GmbH, 2003-2025

Recuperación del estado del sistema

Nota
En la consola de Cyber Protect no puede recuperar copias de seguridad en inquilinos en modo cumplimiento. Consulte "Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento" (p. 1570).

1. Seleccione el equipo para el que desea recuperar el estado del sistema.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación del estado del sistema. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar el estado del sistema**.
5. Confirme si desea sobrescribir el estado del sistema con su respectiva copia de seguridad.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Recuperación de la configuración de ESXi

Para recuperar una configuración de ESXi, se necesita un dispositivo de arranque basado en Linux. Para obtener información sobre cómo crear dispositivos de inicio, consulte "Creación de un dispositivo de arranque físico" (p. 984).

Si quiere recuperar una configuración de ESXi en un servidor que no es el original y el servidor ESXi original sigue conectado a vCenter Server, desconecte y elimine este servidor de vCenter Server para evitar problemas inesperados durante la recuperación. Si quiere conservar el servidor original con el que ha recuperado, puede volver a añadirlo una vez completada la recuperación.

Los equipos virtuales que se ejecutan en el servidor no se incluyen en una copia de seguridad de configuración de ESXi. Se puede hacer una copia de seguridad de ellos y se pueden recuperar por separado.

Para recuperar una configuración de ESXi

1. Inicie el equipo de destino usando el dispositivo de arranque.
2. Haga clic en **Gestionar este equipo localmente**.
3. En la pantalla de inicio, haga clic en **Recuperar**.
4. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
5. Especifique la ubicación de la copia de seguridad:
   - Vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.

   Haga clic en **Aceptar** para confirmar su selección.
6. En **Mostrar**, seleccione **Configuración de ESXi**.

© Acronis International GmbH, 2003-2025

7. Seleccione la copia de seguridad desde la que desea recuperar los datos. Si se le pide, escriba la contraseña para la copia de seguridad.
8. Haga clic en **Aceptar**.
9. En **Discos que se usarán para almacenes de datos nuevos**, haga lo siguiente:
   - En **Recuperar ESXi en**, seleccione el disco donde se recuperará la configuración del servidor. Si quiere recuperar la configuración en el servidor original, se selecciona el disco original de forma predeterminada.
   - [Opcional] En **Usar para almacén de datos nuevo**, seleccione los discos donde se crearán los almacenes de datos nuevos. Debe tener cuidado, ya que se borrarán todos los datos del disco seleccionado. Si quiere conservar los equipos virtuales en los almacenes de datos existentes, no seleccione ningún disco.
10. Si se selecciona algún disco para los almacenes de datos nuevos, seleccione el método de creación de almacenes de datos de **Cómo crear almacenes de datos nuevos**: **Crear un almacén de datos por disco** o **Crear un almacén de datos en todos los discos duros seleccionados**.
11. [Opcional] En **Asignación de red**, cambie el resultado de la asignación automática de los conmutadores virtuales presentes en la copia de seguridad a los adaptadores de red físicos.
12. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
13. Haga clic en **Aceptar** para comenzar la recuperación.

Recuperación con reinicio

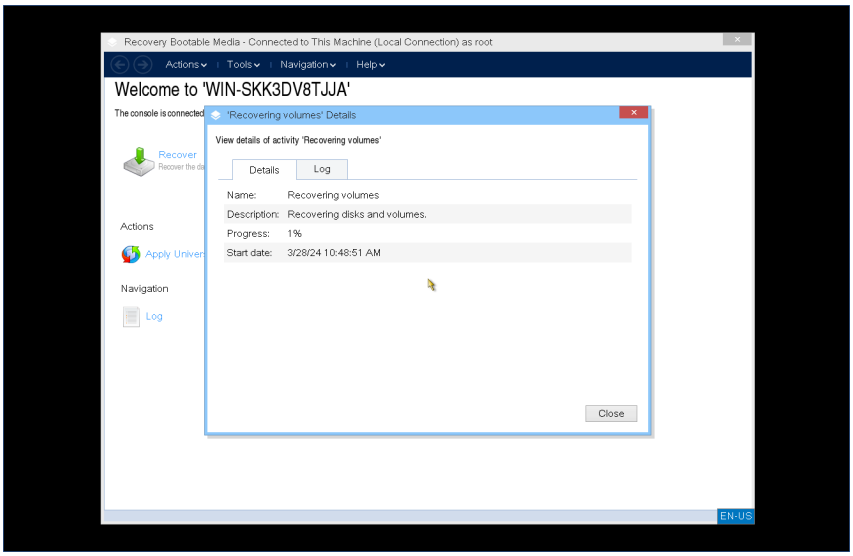
Es necesario reiniciar al recuperar lo siguiente:

- Un sistema operativo
  Por ejemplo, cuando recupera un equipo entero o el volumen del sistema de un equipo.
- Volúmenes cifrados
  Por ejemplo, cuando recupera volúmenes cifrados con BitLocker o cifrados con CheckPoint.

Importante
Los volúmenes no cifrados de los que se haya hecho una copia de seguridad se recuperan como no cifrados.

Un entorno de recuperación se prepara automáticamente en el equipo recuperado. Cuando el entorno está listo, el equipo se reinicia y luego se abre el entorno de recuperación. Cuando se completa la recuperación, se inicia el sistema operativo.

© Acronis International GmbH, 2003-2025



Nota
La preparación del entorno de recuperación de WinRE puede tardar hasta tres minutos.

Para obtener más información sobre los entornos de recuperación disponibles, consulte "Entornos de recuperación" (p. 705).

Entornos de recuperación

Puede utilizar el entorno de recuperación de WinRE o Linux.

La tabla siguiente resume las opciones disponibles.

Equipo recuperado	Entorno de recuperación	
	WinRE	Linux
Windows	Sí (predeterminado)*	Sí
Linux	N/D	Sí

Nota
* Si el entorno de recuperación WinRE predeterminado no puede iniciarse, la operación de recuperación cambiará automáticamente al entorno de Linux. Si establece explícitamente el entorno de recuperación en WinRE o Linux, solo se utilizará el entorno seleccionado. Para obtener más información, consulte "Cambio del entorno de recuperación" (p. 706).

La preparación del entorno de recuperación de WinRE puede tardar hasta tres minutos.

Requisitos de espacio en disco

El entorno de recuperación requiere espacio en disco para archivos temporales. Los requisitos varían dependiendo del equipo recuperado.

La tabla siguiente resume las opciones disponibles.

© Acronis International GmbH, 2003-2025

Modo de arranque	Equipo con volumen de sistema no cifrado	Equipo con volumen de sistema cifrado
BIOS	1 GB en la carpeta `Windows\Temp`	1 GB en la carpeta `Windows\Temp`
UEFI	1 GB en la carpeta `Windows\Temp`	1 GB en la carpeta `Windows\Temp`
BIOS	200 MB en el volumen del sistema	400 MB en un volumen sin cifrar
UEFI	200 MB en la partición del sistema EFI (ESP)	Uno de los siguientes: • 400 MB en la partición del sistema EFI (ESP) • 200 MB en la partición del sistema EFI (ESP) y 200 MB en una partición no cifrada que es accesible durante el proceso de arranque

* La recuperación de un equipo con volumen de sistema cifrado requiere al menos un volumen no cifrado en el mismo equipo.

Limitaciones

- Antes de la recuperación debe bloquear todos los volúmenes cifrados ajenos al sistema cifrados. Puede bloquear un volumen abriendo un archivo que reside en él. Si el volumen no está bloqueado, la recuperación continuará sin reiniciar, y el sistema operativo puede que no reconozca el volumen.

  No necesita bloquear un volumen de sistema cifrado.

Solución de problemas

Si una recuperación falla y el error `No se puede obtener el archivo de la partición` se muestra después de reiniciar, desactive el arranque seguro. Para obtener más información, consulte Cómo desactivar el arranque seguro en la documentación de Microsoft.

Cambio del entorno de recuperación

Puede cambiar el entorno de recuperación predeterminado en las cargas de trabajo de Windows.

En las cargas de trabajo de Linux, solo está disponible el entorno de recuperación de Linux.

Para configurar WinRE

1. En Windows, abra **Regedit**.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Cree un nuevo valor de cadena y, a continuación, asígnele el nombre **RebootEnvironmentType**.
4. Abra el valor de cadena para su edición.

© Acronis International GmbH, 2003-2025

5. En **Datos del valor**, especifique `Windows`.
6. Haga clic en **Aceptar**.

Para configurar Linux

1. En Windows, abra **Regedit**.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Cree un nuevo valor de cadena y, a continuación, asígnele el nombre **RebootEnvironmentType**.
4. Abra el valor de cadena para su edición.
5. En **Datos del valor**, especifique `Linux`.
6. Haga clic en **Aceptar**.

Para restablecer la configuración predeterminada

1. En Windows, abra **Regedit**.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Elimine el valor de cadena **RebootEnvironmentType**.
4. Para confirmar su elección, haga clic en **Sí**.

Uso de Universal Restore

Los sistemas operativos más recientes siguen pudiendo arrancarse cuando se recuperan en un hardware diferente, incluidas las plataformas VMware o Hyper-V. Si un sistema operativo recuperado no arranca, utilice la herramienta Universal Restore para actualizar los controladores y los módulos que sean críticos para el inicio del sistema operativo.

Universal Restore se puede aplicar a Windows y Linux.

Para aplicar Universal Restore

1. Inicie el equipo desde el dispositivo de arranque.
2. Haga clic en **Aplicar Universal Restore**.
3. Si existen varios sistemas operativos en el equipo, escoja aquel donde desea aplicar Universal Restore.
4. [Solo para Windows] Configure los ajustes adicionales.
5. Haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025

Universal Restore en Windows

Preparación

Preparar los controladores

Antes de aplicar Universal Restore a un sistema operativo de Windows, asegúrese de contar con los controladores para el nuevo controlador HDD y el conjunto de chips. Estos controladores son críticos para iniciar el sistema operativo. Utilice el CD o DVD suministrado por el proveedor del hardware o descargue los controladores del sitio web del proveedor. Los archivos de controlador deben tener la extensión *.inf. Si descarga los controladores en el formato *.exe, *.cab o *.zip, extráigalos con una aplicación de terceros.

Se recomienda almacenar los controladores para todo el hardware utilizado en su organización en un mismo depósito, ordenados según el tipo de dispositivo o las configuraciones de hardware. Puede conservar una copia del depósito en un DVD o una unidad de memoria flash; elija algunos controladores y añádalos al dispositivo de arranque; cree un dispositivo de inicio personalizado con los controladores necesarios (y la configuración de red necesaria) para cada uno de sus servidores. O bien, simplemente especifique la ruta al depósito cada vez que utilice Universal Restore.

Compruebe el acceso a los controladores en el entorno de inicio

Asegúrese de tener acceso al dispositivo con controladores cuando trabaje con el dispositivo de arranque. Utilice el dispositivo basado en WinPE si el dispositivo está disponible en Windows, pero el dispositivo basado en Linux no lo detecta.

Configuración de Universal Restore

Búsqueda automática de controladores

Especifique el lugar donde el programa debe buscar los controladores de la capa de abstracción del hardware (HAL), el controlador de disco duro y los adaptadores de red:

- Si los controladores se encuentran en el disco de un proveedor u otro medio extraíble, active la opción **Buscar en medios extraíbles**.
- Si los controladores se encuentran en una carpeta en red o en el soporte de arranque, especifique la ruta a la carpeta al hacer clic en **Añadir carpeta**.

Además, Universal Restore buscará la carpeta de almacenamiento de controladores predeterminada de Windows. Su ubicación está determinada en el valor de registro **DevicePath**, que se puede encontrar en la clave de registro **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Esta carpeta de almacenamiento generalmente es WINDOWS/inf.

Universal Restore ejecutará la búsqueda recursiva en todas las subcarpetas de la carpeta especificada, encontrará los controladores de HAL y de disco duro más apropiados entre todos los

© Acronis International GmbH, 2003-2025

que estén disponibles y los instalará en el sistema. Universal Restore también busca el controlador de adaptadores de red; luego, Universal Restore transmite al sistema operativo la ruta al controlador encontrado. Si el hardware cuenta con varias tarjetas de interfaz de red, Universal Restore intentará configurar los controladores de todos las tarjetas.

Instalar de todos maneras los controladores de los dispositivos de almacenamiento masivo

Necesita este ajuste si:

- El hardware posee un controlador de almacenamiento masivo como RAID (en especial NVIDIA RAID) o un adaptador de canal de fibra.
- Ha migrado un sistema a un equipo virtual que utiliza un controlador de disco duro SCSI. Utilice los controladores SCSI incluidos con el software de virtualización o descargue las últimas versiones de los controladores del sitio web del fabricante del software.
- Si la búsqueda automática de controladores no ayuda a iniciar el sistema.

Especifique los controladores adecuados al hacer clic en **Añadir controlador**. Los controladores definidos aquí se instalarán, con las advertencias adecuadas, incluso si el programa encuentra un controlador mejor.

Proceso de Universal Restore

Después de especificar los ajustes necesarios, haga clic en **Aceptar**.

Si Universal Restore no encuentra un controlador compatible en las ubicaciones especificadas, mostrará un mensaje sobre el dispositivo problemático. Realice uno de los siguientes procedimientos:

- Añada el controlador a cualquiera de las ubicaciones especificadas anteriormente y haga clic en **Reintentar**.
- Si no recuerda la ubicación, haga clic en **Ignorar** para continuar con la recuperación. Si el resultado no es satisfactorio, vuelva a aplicar Universal Restore. Al configurar la operación, especifique el controlador necesario.

Una vez que Windows se inicie, ejecutará el procedimiento estándar para instalar un nuevo hardware. El controlador de adaptadores de red se instalará silenciosamente si el controlador tiene la firma de Microsoft Windows. De lo contrario, Windows solicitará confirmación para instalar el controlador sin firma.

Después, podrá configurar la conexión de red y especificar los controladores para el adaptador de vídeo, USB y otros dispositivos.

Universal Restore en Linux

Universal Restore puede aplicarse a los sistemas operativos de Linux con una versión de kernel 2.6.8 o superior.

© Acronis International GmbH, 2003-2025

Cuando Universal Restore se aplica a un sistema operativo de Linux, actualiza un sistema de archivos temporal conocido como el disco RAM inicial (initrd). Esto garantiza que el sistema operativo pueda iniciarse en el nuevo hardware.

Universal Restore añade módulos para el nuevo hardware (incluyendo los controladores de dispositivo) al disco RAM inicial. Como regla general, localiza los módulos necesarios en el directorio **/lib/modules**. Si Universal Restore no puede encontrar un módulo que necesita, registra el nombre de archivo del módulo en el registro.

Universal Restore puede modificar la configuración del cargador de arranque GRUB. Esto puede ser necesario, por ejemplo, para garantizar la capacidad de arranque cuando el nuevo equipo posee una distribución del volumen diferente al equipo original.

Universal Restore nunca modifica el kernel Linux.

Reversión al disco RAM inicial original

Puede revertir al disco RAM inicial original, si fuera necesario.

El disco RAM inicial está almacenado en el equipo en un archivo. Antes de actualizar el disco RAM inicial por primero vez, Universal Restore guarda una copia del mismo en el mismo directorio. El nombre de la copia es el nombre del archivo seguido del sufijo **_acronis_backup.img**. Esta copia no se sobrescribirá si ejecuta Universal Restore más de una vez (por ejemplo, después de añadir controladores faltantes).

Para volver al disco RAM inicial original, realice cualquiera de las siguientes acciones:

- Cambie el nombre de la copia adecuadamente. Por ejemplo, ejecute un comando similar al siguiente:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Especifique la copia en la línea **initrd** de la configuración del cargador de inicio GRUB.

Opciones de recuperación

Para modificar las opciones de recuperación, haga clic en **Opciones de recuperación** al configurar la recuperación.

Disponibilidad de las opciones de recuperación

El conjunto de opciones de recuperación disponibles depende de:

- El entorno en el que opera el agente que efectúa la recuperación (Windows, Linux, macOS o dispositivo de arranque).
- El tipo de datos que se va a recuperar (discos, archivos, equipos virtuales, datos de aplicación).

La siguiente tabla resume la disponibilidad de las opciones de recuperación.

© Acronis International GmbH, 2003-2025

	Discos			Archivos				Equipos virtuales		SQL y Exchange
	Windows	Linux	Dispositivo de arranque	Windows	Linux	macOS	Dispositivo de arranque	ESXi, Hyper-V, Scale Computing, oVirt y Virtuozzo	Azure	Windows
Validación de la copia de seguridad	+	+	+	+	+	+	+	+	-	+
Modo de arranque	+	-	-	-	-	-	-	+	-	-
Fecha y hora de los archivos	-	-	-	+	+	+	+	-	-	-
Control de errores	+	+	+	+	+	+	+	+	+	+
Exclusiones de archivos	-	-	-	+	+	+	+	-	-	-
Seguridad a nivel de archivo	-	-	-	+	-	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-	-
Recuperación de ruta completa	-	-	-	+	+	+	+	-	-	-
Puntos de montaje	-	-	-	+	-	-	-	-	-	-
Rendimiento	+	+	-	+	+	+	-	+	-	+
Comandos previos/posteriores	+	+	-	+	+	+	-	+	-	+
Cambios en el identificador	+	-	-	-	-	-	-	-	-	-

© Acronis International GmbH, 2003-2025

de seguridad (SID)										
Gestión de energía de VM	-	-	-	-	-	-	-	+	+	-
Registro de eventos de Windows	+	-	-	+	-	-	-	Solo Hyper-V	-	+

Validación de la copia de seguridad

Esta opción define si se valida la copia de seguridad para garantizar que no se corrompió la copia de seguridad, antes de recuperar los datos. Esta operación la realiza el agente de protección.

El valor predeterminado es el siguiente: **Deshabilitado**.

Si quiere obtener más información acerca de la validación por suma de comprobación, acceda a "Verificación de suma de comprobación" (p. 266).

Nota
En función de la configuración que elija su proveedor de servicios, es posible que la validación no esté disponible al realizar una copia de seguridad en el almacenamiento en la nube.

Modo de arranque

Esta opción funciona al recuperar un equipo físico o virtual desde una copia de seguridad de disco que contenga un sistema operativo de Windows.

Esta opción le permite seleccionar el modo de arranque (BIOS o UEFI) que utilizará Windows tras la recuperación. Si el modo de arranque del equipo original difiere del modo de arranque seleccionado, el software:

- Inicializará el disco en el que recupera el volumen del sistema de acuerdo con el modo de arranque seleccionado (MBR para BIOS, GPT para UEFI).
- Ajustará el sistema operativo Windows para que pueda empezar a utilizar el modo de arranque seleccionado.

El valor predeterminado es el siguiente: **Como en el equipo de destino.**

Puede escoger una de las siguientes acciones:

- **Como en el equipo de destino**
  El agente que se ejecuta en el equipo de destino detecta el modo de arranque utilizado actualmente por Windows y realiza los ajustes en función del modo de arranque detectado.
  Este es el valor más seguro que automáticamente da lugar a un sistema de arranque, a menos que se apliquen las limitaciones indicadas a continuación. Puesto que la opción **Modo de**

© Acronis International GmbH, 2003-2025

arranque no está disponible para los dispositivos de arranque, el agente del dispositivo siempre actúa como si se seleccionara este valor.

- **Como en el equipo del que se ha realizado la copia de seguridad**

  El agente que se ejecuta en el equipo de destino lee el dispositivo de arranque de la copia de seguridad y realiza los ajustes en función de dicho dispositivo. Esto le ayuda a recuperar un sistema en un equipo diferente, incluso si este utiliza otro modo de arranque, y reemplazar el disco en el equipo del que se ha realizado la copia de seguridad.
- **BIOS**

  El agente que se ejecuta en el equipo de destino realiza los ajustes para usar BIOS.
- **UEFI**

  El agente que se ejecuta en el equipo de destino realiza los ajustes para usar UEFI.

Una vez que se haya cambiado un ajuste, se repetirá el procedimiento de asignación de discos. Este procedimiento tardará un tiempo.

Recomendaciones

Si necesita transferir Windows entre UEFI y BIOS:

- Recupere el disco completo en el que se encuentra el volumen del sistema. Si recupera solo el volumen del sistema sobre un volumen existente, el agente no podrá inicializar correctamente el disco de destino.
- Recuerde que BIOS no permite usar más de 2 TB de espacio de disco.

Limitaciones

- La transferencia entre UEFI y BIOS se admite para:
  - Los sistemas operativos Windows de 64 bits a partir de Windows 7
  - Los sistemas operativos de Windows Server de 64 bits a partir de Windows Server 2008 SP1

Si no se admite la transferencia de un sistema entre UEFI y BIOS, el agente actúa como si se seleccionara la configuración **Como en el equipo del que se ha realizado la copia de seguridad**. Si el equipo de destino admite tanto UEFI como BIOS, debe habilitar manualmente el modo de arranque correspondiente en el equipo original. De lo contrario, el sistema no arrancará.

Fecha y hora de los archivos

Esta opción es eficaz sólo con los archivos de recuperación.

Esta opción define si recuperar la fecha y hora de los archivos a partir de la copia de seguridad o si asignar a los archivos la fecha y hora actuales.

Si esta opción está habilitada, se asignará a los archivos la fecha y hora actuales.

El valor predeterminado es el siguiente: **Habilitado**.

© Acronis International GmbH, 2003-2025

Control de errores

Estas opciones le permiten que establezca como se manejarán los errores que puedan suceder durante la recuperación.

Reintentar si se produce un error

El valor predeterminado es el siguiente: **Habilitado. Número de intentos: 30. Intervalo entre intentos: 30 segundos**.

Cuando se produce un error recuperable, el programa vuelve a intentar para realizar la operación fallida. Puede establecer el intervalo temporal y el número de intentos. Se detendrán los intentos tan pronto como la operación se lleve a cabo correctamente O se realice el número de intentos especificados, lo que suceda primero.

No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)

El valor predeterminado es el siguiente: **Deshabilitado**.

Con el modo silencioso habilitado, el programa manejará automáticamente las situaciones que requieran de la interacción con el usuario cuando sea posible. Si una operación no puede continuar sin la acción del usuario, ésta fallará. Los detalles de la operación, incluyendo los errores, si los hubiera, pueden encontrarse en el registro de la operación.

Ignorar errores

Esta opción es eficaz para la recuperación a nivel de archivo.

El valor predeterminado es el siguiente: **Habilitado**.

Cuando esta opción esté habilitada y la recuperación de un archivo falle, la operación de recuperación continuará para el resto de los archivos. Se mostrará una advertencia en la pantalla **Actividades**. La opción **Reintentar si se produce un error** no se activará porque no se registrará un error.

Cuando esta opción esté deshabilitada y la recuperación de un archivo falle, la operación de recuperación fallará. Se mostrará un error en la pantalla **Actividades**.

Guardar información del sistema si falla una acción de recuperación con reinicio

Esta opción sirve para la recuperación de un disco o volumen en un equipo físico que ejecute Windows o Linux.

El valor predeterminado es el siguiente: **Deshabilitado**.

Cuando esta opción está habilitada, usted puede especificar una carpeta del disco local (incluidas las unidades flash y unidades de disco duro conectadas al equipo de destino) o de una red compartida en la que se guardarán los archivos de registro, de información del sistema y de volcado de memoria. Este archivo ayudará al personal de soporte técnico a identificar el problema.

© Acronis International GmbH, 2003-2025

Exclusiones de archivos

Esta opción es eficaz sólo con los archivos de recuperación.

La opción define qué archivos y carpetas deben omitirse durante el proceso de recuperación y, por lo tanto, quedar excluidos de la lista de elementos recuperados.

Nota
Las exclusiones anulan la selección de los elementos de datos que se van a recuperar. Por ejemplo, si selecciona recuperar el archivo MyFile.tmp y excluir todos los archivos .tmp, no se podrá recuperar el archivo MyFile.tmp.

Seguridad a nivel de archivo

Esta opción es eficaz a la hora de recuperar archivos de copias de seguridad a nivel de archivo y archivo de volúmenes formateados con NTFS.

Esta opción define si realiza la recuperación de permisos para archivos NTFS junto a los archivos.

El valor predeterminado es el siguiente: **Habilitado**.

Puede elegir entre recuperar los permisos o permitir que los archivos hereden los permisos NTFS de la carpeta desde donde se recuperan.

Flashback

Esta opción es efectiva cuando se recuperan discos y volúmenes en equipos físicos y virtuales, excepto para Mac.

Esta opción solo funciona si el diseño del volumen del disco que se está recuperando coincide exactamente con el del disco de destino.

Si esta opción está habilitada, solo se recuperan las diferencias entre los datos en la copia de seguridad y los datos en el disco de destino. Esto acelera la recuperación de los equipos físicos y virtuales. Los datos se comparan a nivel de bloque.

Cuando se recupera un equipo físico, el valor predeterminado es: **Deshabilitado**.

Cuando se recupera un equipo virtual, el valor predeterminado es: **Habilitado**.

Recuperación de ruta completa

Esta opción solo sirve para la recuperación de datos desde una copia de seguridad a nivel de archivos.

Si esta opción está habilitada, la ruta completa al archivo se volverá a crear en la ubicación de destino.

El valor predeterminado es el siguiente: **Deshabilitado**.

© Acronis International GmbH, 2003-2025

Puntos de montaje

Esta opción es en Windows para la recuperación de datos desde una copia de seguridad a nivel de archivos.

Habilite esta opción para recuperar los archivos y las carpetas que se almacenaron en los volúmenes montados y que se incluyeron en la copia de seguridad con la opción Puntos de montaje habilitada.

El valor predeterminado es el siguiente: **Deshabilitado**.

Esta opción solo funciona cuando selecciona para la recuperación una carpeta que se encuentra en un nivel superior al punto de montaje en la jerarquía. Si selecciona las carpetas de recuperación dentro del punto de montaje mismo, los elementos seleccionados se recuperarán sin importar el valor de la opción de **Puntos de montaje**.

Nota
Tenga en cuenta que si el volumen no está montado en el momento de la recuperación, los datos se recuperarán directamente a la carpeta que había sido el punto de montaje en el momento de la copia de seguridad.

Rendimiento

Esta opción define la prioridad del proceso de recuperación en el sistema operativo.

Los ajustes disponibles son: **Baja**, **Normal**, **Alta**.

El valor predeterminado es el siguiente: **Normal**.

La prioridad de un proceso que se ejecute en un sistema determina la cantidad de uso de la CPU y los recursos del sistema que se asignan a dicho proceso. La disminución de la prioridad de la recuperación liberará más recursos para otras aplicaciones. El aumento de la prioridad de la recuperación puede acelerar el proceso de recuperación al solicitar que el sistema operativo asigne más recursos por la aplicación que realizará la recuperación. Sin embargo, el efecto resultante dependerá del uso total del CPU y otros factores como la velocidad de salida o entrada del disco o el tráfico en la red.

Comandos previos/posteriores

Esta opción le permite definir los comandos a ejecutar automáticamente antes y después del proceso de recuperación de datos.

Ejemplos de como se pueden usar los comandos pre/post:

- Use el comando **Checkdisk** para buscar y reparar los errores en el sistema de archivos lógicos, los errores físicos o los sectores defectuosos que se iniciarán antes del comienzo de la recuperación o cuando finalice.

© Acronis International GmbH, 2003-2025

El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pausa”).

No se ejecutará un comando de recuperación posterior si la recuperación sucede como reinicio.

Comandos antes de la recuperación

Para especificar un comando o archivo por lotes para su ejecución antes de comenzar el proceso de copia de seguridad

1. Habilite el conmutador **Ejecutar un comando antes de la recuperación**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes. El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pausa”).
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Listo**.

Casilla de verificación	**Selección**			
Hacer que la recuperación falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No recuperar hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Realizar la recuperación solo después de que se ejecute el comando correctamente. Hacer que la recuperación falle si falla la ejecución del comando.	Realizar la recuperación después de que se ejecute el comando a pesar del éxito o fallo de la ejecución.	N/D	Realizar la recuperación al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

© Acronis International GmbH, 2003-2025

* Un comando se considerará fallido si su código de salida no es igual a cero.

Comandos posteriores a la recuperación

Para especificar un comando o archivo ejecutable después de completar la recuperación

1. Habilite el conmutador **Ejecutar un comando tras la recuperación**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes.
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Active la casilla de verificación **Hacer que la recuperación falle si falla la ejecución del comando** si cree que la ejecución correcta del comando es fundamental. El comando se considerará fallido si su código de salida no es igual a cero. Si la ejecución del comando falla, el estado de la recuperación será **Error**.

   Cuando no se activa la casilla de verificación, el resultado de la ejecución del comando no afecta al éxito o fallo de la recuperación. Puede realizar un seguimiento de la ejecución de comandos desde la pestaña **Actividades**.
6. Haga clic en **Listo**.

Nota
No se ejecutará un comando de recuperación posterior si la recuperación sucede como reinicio.

Cambios en el identificador de seguridad (SID)

Esta opción funciona al recuperar Windows 8.1/Windows Server 2012 R2 o versiones anteriores.

Esta opción no funciona cuando Agente para VMware, Agente para Hyper-V, Agente para Scale Computing HC3 o Agente para oVirt realizan la recuperación en una máquina virtual.

El valor predeterminado es el siguiente: **Deshabilitado**.

El software puede generar un identificador de seguridad (SID del equipo) único para el sistema operativo recuperado. Solo necesita esta opción para garantizar la operatividad del software de terceros que depende del SID del equipo.

Microsoft no ofrece soporte técnico para cambiar el SID de un sistema implementado o recuperado. Deberá usar esta opción bajo su propia cuenta y riesgo.

Gestión de energía de VM

Estas opciones son efectivas cuando el agente para VMware, agente para Azure, agente para Hyper-V, agente para Virtuozzo, agente para Scale Computing HC3 o agente para oVirt realizan la recuperación en una máquina virtual.

© Acronis International GmbH, 2003-2025

Apagar máquinas virtuales de destino al iniciar la recuperación

El valor predeterminado es el siguiente: **Habilitado**.

La recuperación en un equipo virtual existente no es posible si el equipo está en línea, por lo que este se apaga una vez comenzada la recuperación. Se desconectará a los usuarios de los equipos y se perderán los datos que no se hayan guardado.

Desmarque la casilla de verificación para esta opción si prefiere apagar el equipo virtual antes de la recuperación.

Encienda el equipo virtual de destino cuando haya finalizado la recuperación.

El valor predeterminado es el siguiente: **Deshabilitado**.

Después de recuperar un equipo con una copia de seguridad de otro equipo, es posible que la réplica del equipo existente aparecerá en la red. Para tener seguridad, encienda la máquina virtual manualmente, después de tomar las precauciones necesarias.

Registro de eventos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción define si los agentes tienen que recopilar los eventos de las operaciones de recuperación en el registro de eventos de aplicación de Windows (para ver este registro, ejecute eventvwr.exe o seleccione **Panel de control** > **Herramientas administrativas** > **Visor de eventos**). Puede filtrar los sucesos a ser recopilados.

El valor predeterminado es el siguiente: **Deshabilitado**.

Recuperación segura

Utilice la recuperación segura con copias de seguridad de **Todo el equipo** o **Discos/volúmenes** de cargas de trabajo de Windows para garantizar que solo recupera datos libres de malware, incluso si la copia de seguridad contiene archivos infectados.

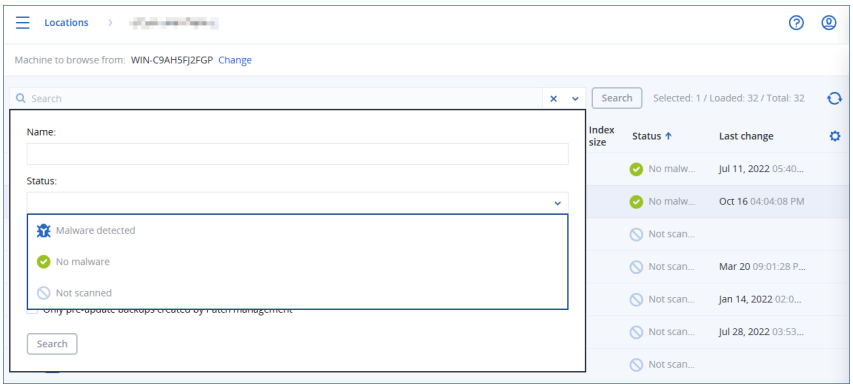
Durante una operación de recuperación segura, la copia de seguridad se analiza automáticamente en busca de malware. A continuación, el agente de protección recupera la copia de seguridad en la carga de trabajo de destino y elimine cualquier archivo infectado. Como resultado, se recupera una copia de seguridad libre de malware.

Asimismo, a la copia de seguridad se le asignará uno de los siguientes estados:

- Malware detectado
- Sin malware
- No analizado

Puede utilizar el estado para filtrar los archivos de copia de seguridad.

© Acronis International GmbH, 2003-2025



Limitaciones

- La recuperación segura se admite en equipos físicos y máquinas virtuales de Windows en los que hay instalado un agente de protección.
- La recuperación segura es compatible con las copias de seguridad de **Todo el equipo** o **Discos/volúmenes**.
- Solo se analizan los volúmenes NTFS en busca de malware. Los volúmenes que no son NTFS se recuperan sin realizar ningún análisis antimalware.
- La recuperación segura no es compatible con la copias de seguridad de la protección continua de datos (CDP) del archivo. Para recuperar los datos de la copia de seguridad CDP, ejecute una operación de recuperación de **archivos/carpetas**. Para obtener más información sobre las copias de seguridad CDP, consulte "Protección continua de datos (CDP)" (p. 552).

Operaciones con copias de seguridad

Almacenamiento de copias de seguridad

La pestaña **Almacenamiento de la copia de seguridad** le permite acceder a todas las copias de seguridad, incluidas las de las cargas de trabajo no conectadas, las de cargas de trabajo que ya no estén registradas en la consola de Cyber Protect y las de nubes públicas como Microsoft Azure.

Las copias de seguridad se organizan en archivos comprimidos de copia de seguridad. Los archivos se nombran según la siguiente plantilla:

```
<workload name> - <protection plan name>
```

Los siguientes archivos comprimidos están huérfanos:

- Archivos que ya no están asociados a un plan de protección o plan de copias de seguridad en la nube.
- Archivos que ya no están asociados a una carga de trabajo registrada.

© Acronis International GmbH, 2003-2025

Nota
Las copias de seguridad huérfanas utilizan espacio de almacenamiento y se facturan en consecuencia.

Las copias de seguridad que se almacenan en una ubicación compartida (como un recurso compartido SMB o NFS) son visibles para todos los usuarios que tienen permisos de lectura para esa ubicación. Recomendamos que restrinja los permisos de lectura para las ubicaciones en las que almacena las copias de seguridad.

Nota
Le recomendamos que utilice la replicación de copia de seguridad en lugar de mover los archivos de la copia de seguridad de forma manual.

Advertencia.
No edite los archivos de la copia de seguridad manualmente. Esto podría resultar en la corrupción de archivos y hacer que las copias de seguridad sean inutilizables. En la consola de Cyber Protect, las copias de seguridad dañadas se marcan como **Desconocido** y solo puede eliminarlas. Puede que no sea posible recuperar datos de ellas. Para obtener asistencia con copias de seguridad dañadas, póngase en contacto con el equipo de soporte.

En el almacenamiento en la nube, el acceso a las copias de seguridad depende del rol del usuario:

- Las cuentas con el rol de administrador pueden acceder a todas las copias de seguridad en su inquilino o unidad.
- Las cuentas con el rol de usuario solo pueden acceder a sus propias copias de seguridad.

Las ubicaciones de copia de seguridad que se utilizan en los planes de protección se añaden automáticamente a la pestaña **Almacenamiento de la copia de seguridad**. Las copias de seguridad de la nube a la nube se muestran en **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones en la nube**.

Una ubicación de copia de seguridad (excepto el almacenamiento en la nube) desaparece de la pestaña **Almacenamiento de la copia de seguridad** si se eliminan todos las cargas de trabajo que se han respaldado en esa ubicación de la consola de Cyber Protect. Si se realiza una nueva copia de seguridad en esta ubicación, se vuelve a añadir la ubicación con todas las copias de seguridad que se almacenan en ella.

Puede añadir manualmente la ubicación de la copia de seguridad. Por ejemplo, una memoria USB o un disco duro externo.

Para añadir manualmente una ubicación de copia de seguridad

Nota
Esta operación solo está disponible si tiene un agente en línea.

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a la pestaña **Almacenamiento de la copia de seguridad** y haga clic en **Añadir ubicación**.
3. Seleccione el tipo de ubicación:
   - Carpeta local
   - Carpeta de red
   - Secure Zone
   - Carpeta NFS
   - Nube pública
4. Configure la ubicación y haga clic en **Listo**.

Para actualizar una ubicación de copia de seguridad

Si ha añadido o eliminado copias de seguridad manualmente, debe actualizar la ubicación para sincronizar el cambio con la consola de Cyber Protect.

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a la pestaña **Almacenamiento de la copia de seguridad** y seleccione una ubicación de copia de seguridad.
3. [No aplicable a las **Copias de seguridad de aplicaciones en la nube**] En **Equipo en el que explorar**, seleccione un equipo en línea.
4. En el panel de **Acciones**, haga clic en **Actualizar**.

Cómo filtrar los archivos comprimidos de copias de seguridad

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a la pestaña **Almacenamiento de la copia de seguridad** y seleccione una ubicación de copia de seguridad.
3. En la cuadrícula principal, haga clic en el ícono de engranaje y active las columnas que desea ver.
4. Para filtrar las copias de seguridad, pulse en el nombre de la columna.

Para seleccionar una copia de seguridad (punto de recuperación)

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a la pestaña **Almacenamiento de la copia de seguridad** y seleccione una ubicación de copia de seguridad.
   Solo se muestran las copias de seguridad a las que puede acceder.
3. [No aplicable a las copias de seguridad de aplicaciones en la nube] En **Equipo en el que explorar**, seleccione un equipo en línea.
   El acceso a algunas copias de seguridad requiere un agente específico. Por ejemplo, para examinar las copias de seguridad de bases de datos SQL, debe seleccionar un equipo que esté ejecutando el Agente para SQL.

© Acronis International GmbH, 2003-2025

Importante
El equipo con el agente de protección (**Equipo en el que explorar**) es el destino de recuperación predeterminado para las copias de seguridad de equipos físicos. Si desea recuperar dicha copia de seguridad en un equipo diferente, seleccione ese equipo en **Equipo en el que explorar**.

4. Seleccione un archivo comprimido desde el que desea recuperar los datos.
5. Haga clic en **Mostrar copias de seguridad**.
6. Seleccione la copia de seguridad (punto de recuperación).

Montaje de volúmenes desde una copia de seguridad

El montaje de volúmenes a nivel de la copia de seguridad del disco le permite acceder a los volúmenes como si se tratara de discos físicos.

El montaje de volúmenes en el modo de lectura/escritura le permite modificar el contenido de la copia de seguridad, es decir, guardar, mover, crear o eliminar archivos o carpetas, y ejecutar ejecutables que consten de un archivo. En este modo, el software crea una copia de seguridad incremental que contiene los cambios realizados en el contenido de la copia de seguridad. Tenga en cuenta que ninguna de las copias de seguridad posteriores contendrá estos cambios.

Requisitos

- Esta funcionalidad solo está disponible en Windows utilizando el Explorador de archivos.
- Debe instalarse Agente para Windows en el equipo que realice la operación de montaje.
- El sistema de archivos a los que se ha realizado una copia de seguridad debe ser compatible con la versión de Windows instalada en el equipo.
- La copia de seguridad debe almacenarse en una carpeta local, en una red compartida (SMB/CIFS) o en Secure Zone (zona segura).

Escenarios de usos

- Compartir datos
  Los volúmenes montados se pueden compartir fácilmente en la red.
- Solución de recuperación de base de datos "Band-aid"
  Para montar un volumen que contenga una base de datos SQL desde un equipo que falló recientemente. Esto dará acceso a la base de datos hasta que se recupere la máquina que falló. Este enfoque también se puede utilizar para la recuperación granular de los datos de Microsoft SharePoint utilizando SharePoint Explorer.
- Limpieza de virus fuera de línea
  Si un equipo está infectado, monte su copia de seguridad, límpielo con un programa antivirus (o busque la última copia de seguridad que no esté infectada) y, a continuación, recupere el equipo desde esta copia de seguridad.

© Acronis International GmbH, 2003-2025

- Comprobación de errores

  Si ha fallado una recuperación con cambio en el tamaño del volumen, la razón podría deberse a un error en el sistema de archivos a los que se ha realizado una copia de seguridad. Monte la copia de seguridad en el modo de lectura/escritura. Luego, compruebe si hay errores en el volumen montado por medio del comando `chkdsk /r`. Una vez que se hayan solucionado los errores y se haya creado una nueva copia de seguridad incremental, recupere el sistema desde esta copia de seguridad.

Para montar un volumen desde una copia de seguridad

1. Busque la ubicación de la copia de seguridad utilizando el Explorador de archivos.
2. Haga doble clic en el archivo de copia de seguridad. Los nombres de los archivos se basan en la siguiente plantilla:

   `<machine name> - <protection plan GUID>`
3. Si la copia de seguridad está cifrada, introduzca la contraseña de cifrado. De lo contrario, omita este paso.

   El Explorador de archivos muestra los puntos de recuperación.
4. Haga doble clic en el punto de recuperación.

   El Explorador de archivos muestra los volúmenes objeto de la copia de seguridad.

   Nota
   Haga doble clic en un volumen para buscar su contenido. Puede copiar archivos y carpetas desde la copia de seguridad a cualquier carpeta del sistema de archivos.
5. Haga clic con el botón derecho en un volumen que desee montar y, a continuación, seleccione una de las siguientes opciones:
   a. **Montar**

      Nota
      La última copia de seguridad en el archivo comprimido (cadena de copia de seguridad) solo se puede montar en el modo de lectura y escritura.

   b. **Montar en modo de solo lectura**.
6. Si la copia de seguridad se almacena en una red compartida, proporcione las credenciales de acceso. De lo contrario, omita este paso.

   El software monta el volumen seleccionado. La primera letra que no esté en uso se asignará al volumen.

Para desmontar un volumen

1. Busque el **Equipo** (**Este PC** en Windows 8.1 y versiones posteriores) utilizando el Explorador de archivos.
2. Haga clic con el botón derecho en el volumen montado.
3. Haga clic en **Desmontar**.

© Acronis International GmbH, 2003-2025

4. [Opcional] Si el volumen se montó en modo de lectura/escritura, y se modificó su contenido, seleccione si crear una copia de seguridad incremental que contenga los cambios. De lo contrario, omita este paso.

El software desmonta el volumen seleccionado.

Validación de copias de seguridad

Puede validar una copia de seguridad para verificar que puede recuperar los datos. Para obtener más información sobre esta operación, consulte "Validación" (p. 264).

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

Validar una copia de seguridad

1. Seleccione la carga de trabajo con copia de seguridad.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
   Si la carga de trabajo está offline, no se mostrarán los puntos de recuperación. Realice una de las siguientes operaciones:
   - Si la ubicación de la copia de seguridad se encuentra en la nube o en un almacenamiento compartido (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, elija una carga de trabajo de destino que esté en línea y después un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad. Para obtener más información sobre las copias de seguridad ahí, consulte "Almacenamiento de copias de seguridad" (p. 720).
4. Haga clic en el icono de engranaje y, a continuación, en **Validar**.
5. Seleccione el agente que llevará a cabo la validación.
6. Seleccione el método de validación.
7. Si la copia de seguridad está cifrada, indique la contraseña de cifrado.
8. Haga clic en **Iniciar**.

Exportación de copias de seguridad

La operación de exportación crea una copia autosuficiente de la copia de seguridad en la ubicación que especifique. La copia de seguridad original permanece intacta. La exportación de copias de seguridad permite separar una copia de seguridad específica de una cadena de copias de seguridad incrementales y diferenciales para una rápida recuperación, escribir sobre medios extraíbles u otros propósitos.

© Acronis International GmbH, 2003-2025

Nota
Esta funcionalidad está disponible en los inquilinos de cliente para los que se ha habilitado la cuota de **Advanced Backup – Servers** o la cuota de **Advanced Backup – NAS** como parte del paquete de Advanced Backup.

El resultado de una operación de exportación es siempre una copia de seguridad completa. Si quiere replicar toda la cadena de copia de seguridad en una ubicación diferente y conservar varios puntos de recuperación, use un plan de réplica de copia de seguridad. Para obtener más información sobre este plan, consulte "Réplica de copia de seguridad" (p. 261).

El nombre del archivo de la copia de seguridad exportada es el mismo que el de la copia de seguridad original, excepto en el número de secuencia. Si se exportan varias copias de seguridad de la misma cadena de copia de seguridad en la misma ubicación, se añade una secuencia de números de cuatro dígitos a los nombres de los archivos de todas las copias de seguridad, excepto al primero.

La copia de seguridad exportada hereda la contraseña y la configuración de cifrado de la copia de seguridad original. Al exportar una copia de seguridad cifrada, debe especificar la contraseña.

Pasos para exportar una copia de seguridad

1. Seleccione la carga de trabajo con copia de seguridad.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
   Si la carga de trabajo está offline, no se mostrarán los puntos de recuperación. Realice una de las siguientes operaciones:
   - Si la ubicación de la copia de seguridad se encuentra en la nube o en un almacenamiento compartido (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, elija una carga de trabajo de destino que esté en línea y después un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad. Para obtener más información sobre las copias de seguridad ahí, consulte "Almacenamiento de copias de seguridad" (p. 720).
4. Haga clic en el icono de engranaje y, a continuación, en **Exportar**.
5. Seleccione el agente que llevará a cabo la exportación.
6. Si la copia de seguridad está cifrada, indique la contraseña de cifrado. De lo contrario, omita este paso.
7. Especifique el destino de la exportación.
8. Haga clic en **Iniciar**.

© Acronis International GmbH, 2003-2025

Eliminación de copias de seguridad

Un archivo de copia de seguridad contiene una o más copias de seguridad. Puede eliminar copias de seguridad específicas (puntos de recuperación) en un archivo o su totalidad.

Eliminar el archivo de copia de seguridad elimina todas las copias de seguridad en él. Eliminar todas las copias de seguridad de una carga de trabajo elimina los archivos de copia de seguridad que contienen estas copias de seguridad.

Nota
La protección continua de datos (CDP) evita la eliminación de archivos de copia de seguridad. Si desea eliminar manualmente una copia de seguridad que se crea con la CDP habilitada, debe revocar o eliminar el plan de protección correspondiente.

Puede eliminar copias de seguridad utilizando la consola de Cyber Protect en la pestaña **Dispositivos** y en la pestaña **Almacenamiento de la copia de seguridad**. Además, puede eliminar copias de seguridad del almacenamiento en la nube utilizando la consola de Web Restore.

Advertencia.
Si el almacenamiento inmutable está desactivado, los datos con copia de seguridad se eliminan permanentemente y no se pueden recuperar.

Para eliminar copias de seguridad o archivos de copia de seguridad

En la pestaña Dispositivos

Este procedimiento solo se aplica a las cargas de trabajo en línea.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las copias de seguridad de la carga de trabajo que desea eliminar.
3. Haga clic en **Recuperación**.
4. [Si hay disponible más de una ubicación para las copias de seguridad] Seleccione la ubicación de la copia de seguridad.
5. [Para eliminar todas las copias de seguridad de la carga de trabajo] Haga clic en **Eliminar todo**. Eliminar todas las copias de seguridad también elimina los archivos de copia de seguridad que contienen estas copias de seguridad.
6. [Para eliminar una copia de seguridad específica] Seleccione la copia de seguridad (punto de recuperación) que desea eliminar y haga clic en **Acciones** > **Eliminar**.
7. [Al eliminar todas las copias de seguridad] Seleccione la casilla de verificación y haga clic en **Eliminar** para confirmar su decisión.
8. [Al eliminar una copia de seguridad específica] Haga clic en **Eliminar** para confirmar su decisión.

En la pestaña Almacenamiento de la copia de seguridad

Este procedimiento se aplica a cargas de trabajo online y offline.

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación de la que desea eliminar las copias de seguridad.
3. Seleccione el archivo de copia de seguridad del que desea eliminar copias de seguridad.
   El nombre del archivo utiliza la siguiente plantilla:
   - Archivos de copia de seguridad no de nube a nube: <workload name> - <protection plan name>
   - Archivos de copia de seguridad de nube a nube: <user name> o <drive name> o <team name> - <cloud service> - <protection plan name>
4. [Para eliminar todo el archivo de copia de seguridad] Haga clic en **Eliminar**.
   Eliminar un archivo de copia de seguridad borra todas las copias de seguridad en ese archivo.
5. [Para eliminar una copia de seguridad específica en el archivo de copia de seguridad] Haga clic en **Mostrar copias de seguridad**.
   a. Seleccione la copia de seguridad (punto de recuperación) que desee eliminar.
   b. Haga clic en **Acciones** > **Eliminar**.
6. [Al eliminar un archivo de copia de seguridad] Seleccione la casilla de verificación y haga clic en **Eliminar** para confirmar su decisión.
7. [Al eliminar una copia de seguridad específica] Haga clic en **Eliminar** para confirmar su decisión.

En la consola de Web Restore

Este procedimiento solo se aplica a los archivos de copia de seguridad en el almacenamiento en la nube.

1. En la consola de Cyber Protection, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las copias de seguridad de la carga de trabajo que desee eliminar y luego haga clic en **Recuperación**.
3. [Si hay varias ubicaciones de copia de seguridad disponibles] Seleccione la ubicación de la copia de seguridad y haga clic en **Otras formas de recuperar**.
4. Haga clic en **Descargar archivos**.
   Se le redirige a la consola de Web Restore.
5. En la consola de Web Restore, en **Equipos**, haga clic en el nombre de la carga de trabajo.
6. En **Última versión**, haga clic en la fecha y, luego, en **Eliminar**.
   Esta acción solo está disponible a nivel de archivo de copia de seguridad. No puede profundizar en el archivo y eliminar copias de seguridad específicas en él.
7. Haga clic en **Eliminar** para confirmar su decisión.

Eliminación de copias de seguridad fuera de la consola de Cyber Protect

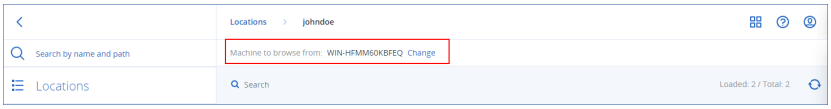
Recomendamos que elimine las copias de seguridad utilizando la consola de Cyber Protect. Si elimina las copias de seguridad del almacenamiento en la nube utilizando la consola de Web Restore o elimina las copias de seguridad locales utilizando un administrador de archivos, debe

© Acronis International GmbH, 2003-2025

actualizar la ubicación de la copia de seguridad para sincronizar los cambios con la consola de Cyber Protect.

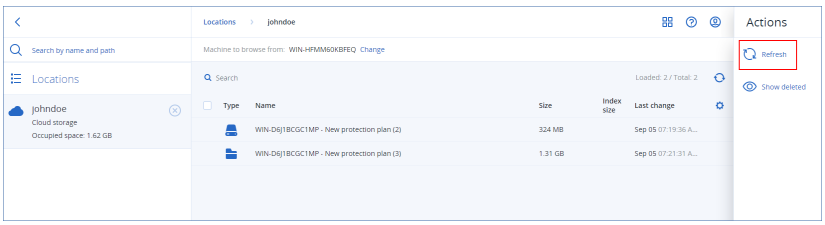
Prerrequisito

- Debe seleccionarse un agente en línea que pueda acceder a la ubicación de la copia de seguridad como **Equipo desde el cual examinar** en la consola de Cyber Protect.



Para actualizar una ubicación de copia de seguridad

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación de la copia de seguridad en la que se almacenaron las copias de seguridad eliminadas.
3. En el panel de **Acciones**, haga clic en **Actualizar**.



Descripción de la detección de atascos

La función de detección de atascos le ayuda a entender cómo puede mejorar el rendimiento al destacar qué componente de su sistema fue más lento durante una copia de seguridad o proceso de recuperación.

Dado que *siempre* ocurren atascos en cualquier evento de transmisión, no es necesario resolverlos. Sus copias de seguridad pueden ser ya lo suficientemente rápidas y ajustarse a la perfección a las copias de seguridad de Windows, así como a sus acuerdos de nivel de servicio, por lo que no suele haber nada que deba resolverse.

Puede ver los atascos y seguirlos fácilmente en la pestaña **Detalles de actividad**. Para ello, en la consola de Cyber Protect, vaya a **Supervisión > Actividades** y, a continuación, haga clic en la actividad correspondiente. Para obtener más información sobre cómo ver los atascos, consulte "Visualización de detalles de atasco" (p. 731) y "¿Se muestran los atascos en las cargas de trabajo, los agentes y las ubicaciones de copia de seguridad?" (p. 733).

¿Qué es un atasco?

Los atascos suelen estar causados por un componente lento de la cadena de procesamiento, es decir, un componente al que tienen que esperar el resto de componentes.

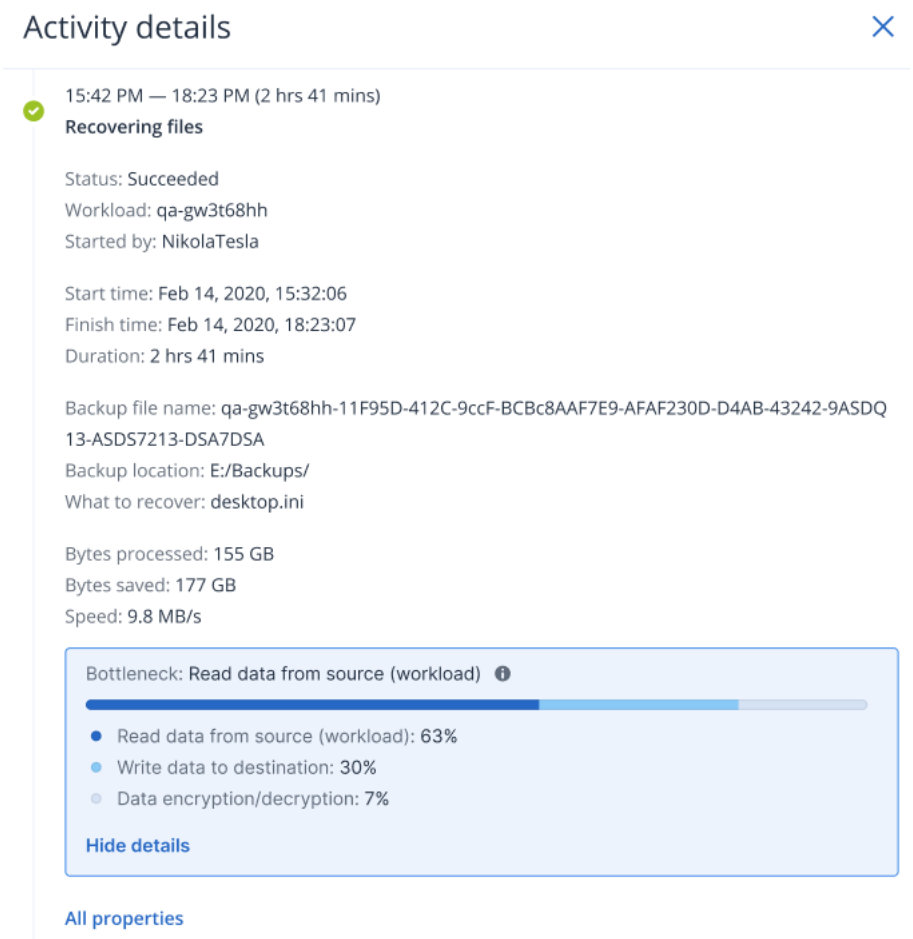
© Acronis International GmbH, 2003-2025

La función de detección de atascos le permite hacer un seguimiento de estos componentes lentos durante la copia de seguridad y el proceso de recuperación, lo que le ayuda a entender qué tipo de componente de entre los siguientes es el más lento:

- **Origen**: Puede determinar de un vistazo si la velocidad de lectura del origen de la copia de seguridad o recuperación está provocando un atasco.
- **Destino**: Conozca si la velocidad de escritura en el destino de la copia de seguridad o la recuperación está afectando al rendimiento.
- **Agente**: Conozca si el agente procesa los datos lo suficientemente rápido.

El tipo de atasco, tanto del origen, del destino o del agente, puede cambiar varias veces durante la actividad de copia de seguridad o recuperación. Los porcentajes que se muestran en la sección **Atasco** de la pestaña **Detalles de actividad** a continuación (por ejemplo, **Datos de lectura del origen (carga de trabajo): 63 %**) representan el porcentaje de tiempo cuando se encuentra este tipo de atasco. En este caso, para el 63 % del tiempo de actividad de recuperación, el tipo de atasco fue de datos de lectura, es decir, la velocidad lenta de los datos de lectura desde el archivo de copia de seguridad por el agente.

De manera similar, en cuanto al 30 % del tiempo, el atasco se debió a la velocidad lenta de los datos de escritura hasta el destino de la recuperación (**Escribir datos en el destino: 30 %**).



© Acronis International GmbH, 2003-2025

Nota
Es normal ver estadísticas de atascos en la pestaña **Detalles de actividad**. Estas estadísticas solo están disponibles para tareas de más de un minuto de duración.

Cómo reducir los atascos

Como se ha mencionado, la función de detección de atascos destaca el flujo de datos de *lectura* y *escritura* entre los componentes de la copia de seguridad. Las estadísticas de *lectura* hacen referencia al flujo de datos desde el origen de datos hasta el agente que ejecuta la copia de seguridad o la operación de recuperación, y las estadísticas de *escritura* hacen referencia al flujo de datos entre el agente y el archivo de copia de seguridad (el destino).

Para reducir los atascos y mejorar el rendimiento del flujo de datos de lectura o escritura, debe analizar el canal entre el agente y el origen de datos o el archivo de copia de seguridad. Por ejemplo, puede probar a hacer un análisis comparativo de sus discos duros si el agente realiza una copia de seguridad de algunos archivos locales.

Visualización de detalles de atasco

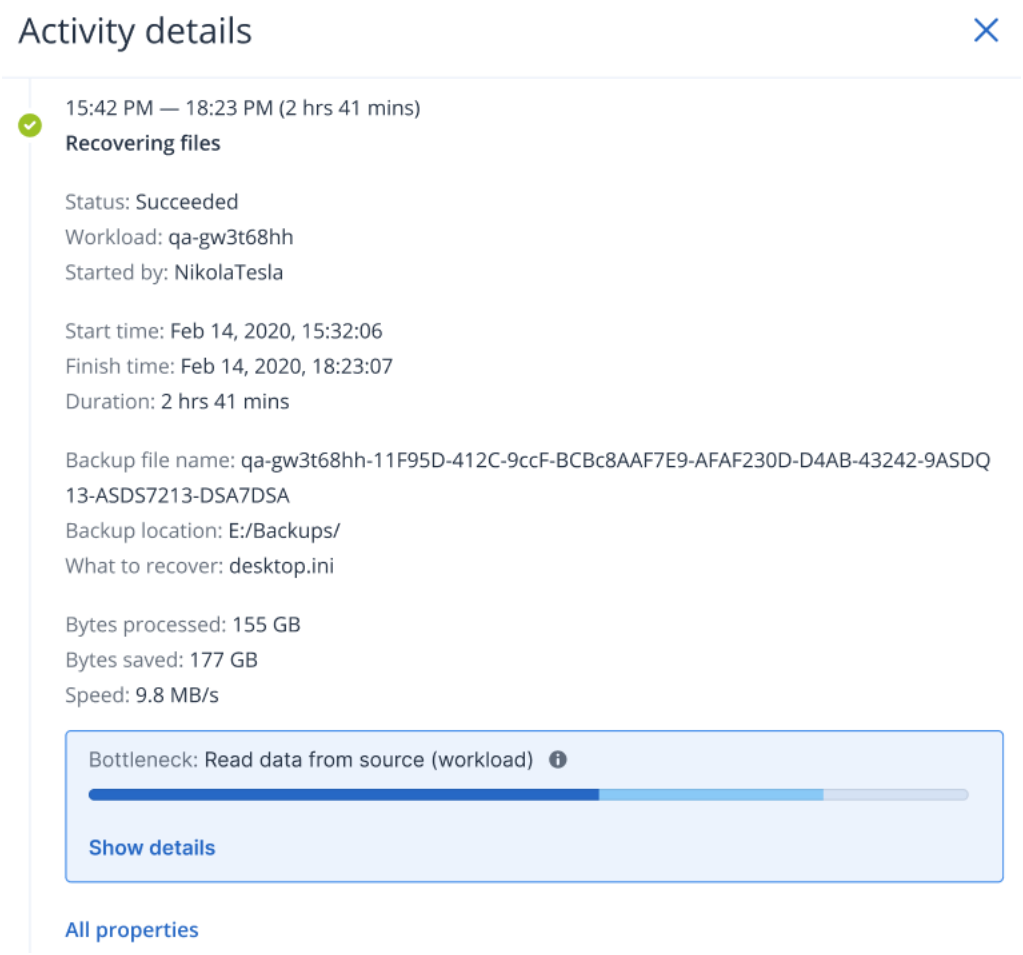
Puede ver los atascos detectados de cualquier tipo de copia de seguridad, replicación de copia de seguridad o proceso de recuperación (para cualquier tipo de carpeta o ubicación de destino), incluidas las copias de seguridad de máquinas virtuales, de equipos y de archivos o carpetas. También puede ver los atascos de la replicación de máquinas virtuales y las actividades de conmutación tras recuperación.

Para obtener más información sobre la definición y los conceptos básicos de los tipos de atascos, consulte "Descripción de la detección de atascos" (p. 729).

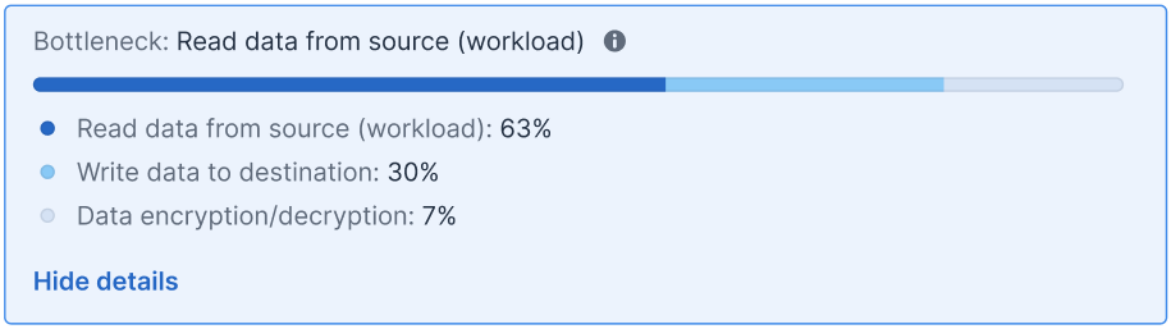
Pasos para ver los detalles del atasco

1. En la consola de Cyber Protect, vaya a **Supervisión > Actividades**.
2. Haga clic en la actividad correspondiente.
   En la pestaña **Detalles de actividad**, se mostrará la sección **Atasco** en azul.

© Acronis International GmbH, 2003-2025



3. Haga clic en **Mostrar detalles** para ver el atasco más frecuente encontrado durante la operación de copia de seguridad o recuperación.
   La sección **Atasco** se expande para mostrar un resumen de los tipos de atasco correspondientes.



   En el ejemplo anterior, el atasco, que suponía el 63 % de todo el tiempo de la operación, estaba causado por la operación de *Lectura* (ejecutada por el agente).

Nota
Los valores del atasco se actualizan dinámicamente cada minuto mientras que se ejecuta la actividad correspondiente.

© Acronis International GmbH, 2003-2025

¿Se muestran los atascos en las cargas de trabajo, los agentes y las ubicaciones de copia de seguridad?

La detección de atascos está disponibles para los siguientes tipos de cargas de trabajo, agentes y ubicaciones de copia de seguridad:

- Copias de seguridad a nivel de disco o imagen ejecutadas por:
  - Agente para Azure
  - Agente para Windows
  - Agente para Linux
  - Agente para Mac
  - Agente para VMware (tanto dispositivo virtual como Windows, incluidas las actividades de replicación de máquinas virtuales y conmutación tras error de la réplica [restauración desde réplica])
  - Agente para Hyper-V
  - Agent para Scale Computing HC3
  - Agente para oVirt (KVM)
  - Agente para la Plataforma de infraestructuras Virtuozzo
  - Agente para Virtuozzo
  - Agente para VMware Cloud Director (vCD-BA)
- Copias de seguridad a nivel de archivos
  - Agente para Windows
  - Agente para Linux
  - Agente para Mac
- Copias de seguridad a nivel de aplicación
  - Agente para SQL
  - Agente para Exchange
  - Agente para MySQL/MariaDB
  - Agente para Oracle
  - Agente para SAP HANA
- Ubicaciones de las copias de seguridad
  - Acronis Cloud Storage (incluido el almacenamiento alojado por el partner)
  - Almacenamiento en la nube pública
  - Recursos compartidos de red (SMB + NFS)
  - Carpetas locales

© Acronis International GmbH, 2003-2025

- Ubicaciones definidas por secuencia de comandos
- Acronis Secure Zone

Hacer copias de seguridad de cargas de trabajo en nubes públicas

Nota
Esta función forma parte del paquete Advanced Backup, que a su vez forma parte del servicio de Cyber Protection. Tenga en cuenta que cuando añade esta funcionalidad a un plan de protección, puede estar sujeta a cargos adicionales.

Importante
La copia de seguridad de los recursos informáticos en cualquiera de los servicios en la nube pública admitidos solo es posible para los agentes de protección que se ejecutan en Windows 7 o superior, y Windows Server 2008 R2 o superior. Además, los agentes que ejecutan planes de protección de datos fuera del host mientras se ejecutan en un sistema operativo desactualizado (como Windows Vista o Windows Server 2008 o inferior) no pueden trabajar con ubicaciones en nubes públicas.

Puede seleccionar servicios de nube pública, como Microsoft Azure y Amazon S3 (Simple Storage Service) y Wasabi como destinos de copia de seguridad en la consola de Cyber Protect.

Nota
El almacenamiento S3 no es compatible como destino de las copias de seguridad de Microsoft 365.

Para configurar ubicaciones de copia de seguridad en nubes públicas, debe ser un administrador de la empresa o administrador de la unidad, o tener uno de los siguientes roles definidos en el servicio de ciberprotección: Administrador de cibernética, administrador, o usuario.

Definir una ubicación de copia de seguridad en Microsoft Azure

Nota
Para configurar ubicaciones de copia de seguridad en Microsoft Azure, debe tener uno de los siguientes roles definidos en el servicio de ciberprotección: Administrador de la empresa, Usuario, Administrador de cibernética.

Puede definir ubicaciones de copia de seguridad en el servicio de Microsoft Azure Blob Storage, en uno de los siguientes tipos de cuenta de Microsoft Azure Storage:

- Uso general estándar v2 (StorageV2)
- Blobs en bloques Prémium

Para obtener más información sobre los tipos de cuentas de Microsoft Azure Storage, consulte la documentación de Microsoft.

© Acronis International GmbH, 2003-2025

Para hacer una copia de seguridad de una carga de trabajo en Microsoft Azure, debe definir la ubicación de copia de seguridad de Microsoft Azure en la consola de Cyber Protect y conectarse a la suscripción de Microsoft Azure correspondiente. Lo puede hacer de distintas formas:

- Al crear o editar un plan de protección.
- Al definir y gestionar ubicaciones de almacenamiento de copia de seguridad.

Importante
Tanto los usuarios administradores como los que no lo son pueden hacer copias de seguridad de cargas de trabajo en Microsoft Azure.

Los usuarios que no son administradores pueden añadir el acceso a una suscripción de Microsoft Azure (consulte "Gestionar el acceso a las suscripciones de Microsoft Azure" (p. 753)), pero solo pueden aplicar planes de protección en los que la ubicación de copia de seguridad esté conectada a la suscripción de Microsoft Azure que han añadido ellos mismos, y para cargas de trabajo que estén registradas a su nombre en la consola de Cyber Protect.

Los administradores pueden aplicar planes de protección en los que la ubicación de copia de seguridad esté conectada a suscripciones de Microsoft Azure que hayan añadido ellos mismos u otros administradores, y para cargas de trabajo que estén registradas a nombre de cualquier usuario en la consola de Cyber Protect.

Pasos para definir una ubicación de copia de seguridad en Microsoft Azure

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - Si quiere crear o editar un plan de protección, vaya a **Dispositivos** y selecciona la carga de trabajo de la que quiera hacer una copia de seguridad en Microsoft Azure. En la sección **Copia de seguridad** del plan de protección de la carga de trabajo seleccionada, haga clic en el enlace en la fila **Dónde guardar las copias de seguridad**.
     Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 249).
   - Si quiere gestionar sus ubicaciones de almacenamiento de copia de seguridad y añadir Microsoft Azure como una nueva ubicación, vaya a **Almacenamiento de la copia de seguridad**.
     Para obtener más información sobre cómo gestionar las ubicaciones de almacenamiento de copia de seguridad, consulte "Almacenamiento de copias de seguridad" (p. 720).
2. Haga clic en **Añadir ubicación**.
3. Desde la lista desplegable de **Nubes públicas**, seleccione **Microsoft Azure**.
4. Si la suscripción de Microsoft Azure correspondiente ya está registrada en la consola de Cyber Protect, selecciónela en la lista de suscripciones.
   Si la suscripción correspondiente no está registrada en la consola de Cyber Protect, haga clic en **Agregar** y, en el diálogo que se muestra, haga clic en **Iniciar sesión**. Se le redirigirá a la página de inicio de sesión de Microsoft. Para obtener información sobre cómo añadir y definir el acceso

© Acronis International GmbH, 2003-2025

a una suscripción de Microsoft Azure, consulte "Añadir el acceso a una suscripción de Microsoft Azure" (p. 754).

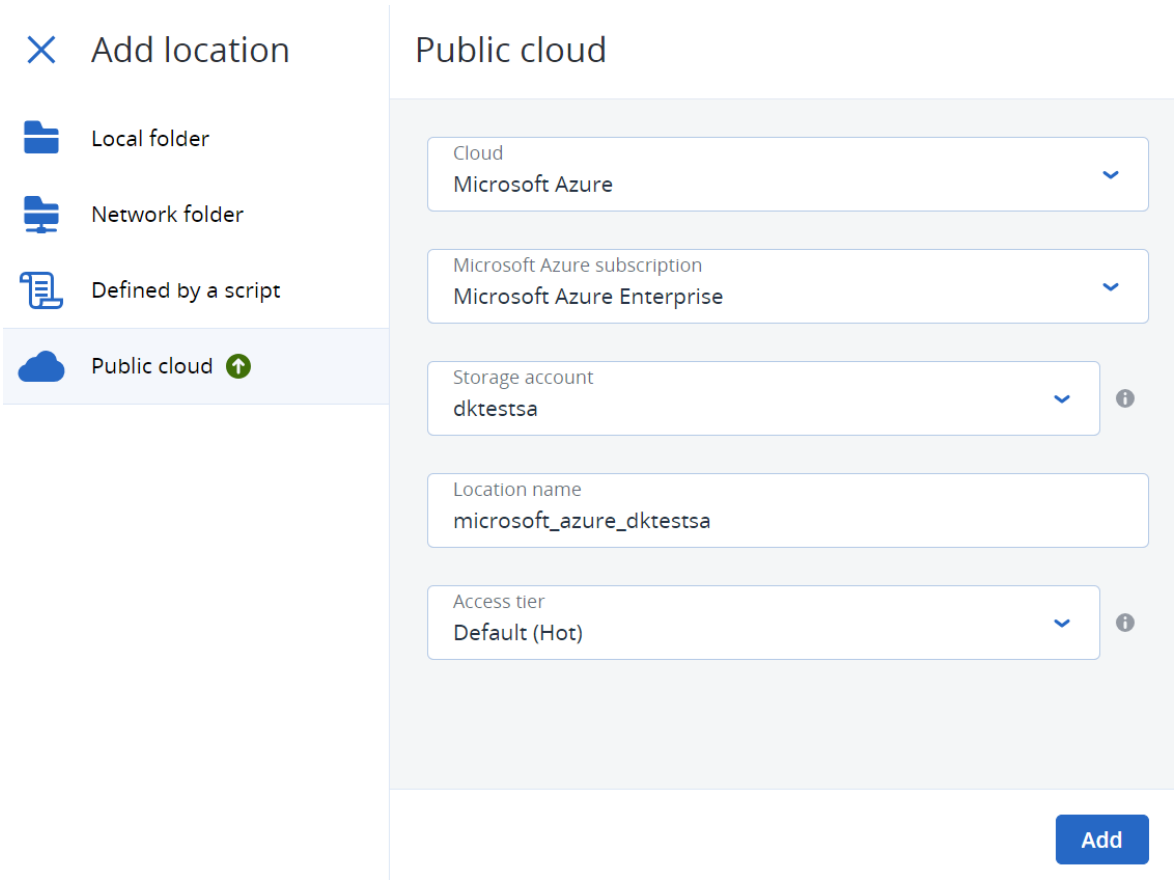
5. En el campo **Cuenta de almacenamiento**, seleccione la cuenta correspondiente.

Nota
Actualmente, solo se admiten las cuentas de almacenamiento de Microsoft Azure con sufijos de endpoint que contengan `core.windows.net`.

Los campos **Nombre de la ubicación** y **Nivel de acceso** se rellenan automáticamente según la cuenta de almacenamiento seleccionada. El nombre de la ubicación que se muestra es `microsoft_azure_[storage account]` y el nivel de acceso seleccionado es **Predeterminado (frecuente)**. Se pueden modificar ambos campos si es necesario.

Nota
Actualmente solo se admite el nivel de acceso Hot y Cool (para obtener más información sobre los niveles de acceso, consulte la documentación de Microsoft).

Nota
Si cambia el nombre de la ubicación, debe introducir uno que sea exclusivo del inquilino del cliente. Si el nombre que ha añadido ya existe en la cuenta de almacenamiento, Acronis añadirá un número al final. Por ejemplo, si **Microsoft Azure Storage** ya existe, el nombre se cambiará automáticamente a **Microsoft Azure Storage_01**.



© Acronis International GmbH, 2003-2025

6. Haga clic en **Agregar**.

   Si crea o edita un plan de protección, la ubicación de copia de seguridad de Microsoft Azure se establece en la ubicación de la fila **Dónde guardar las copias de seguridad**. Cuando se ejecute la copia de seguridad (ya sea manualmente o según la planificación), se guardará en la ubicación definida.

   Si está gestionando sus ubicaciones de almacenamiento de copia de seguridad, puede ver y actualizar los detalles de la ubicación según sea necesario. La ubicación de Microsoft Azure también está disponible al definir una ubicación de copia de seguridad para cargas de trabajo. Para obtener más información, consulte "Visualización y actualización de ubicaciones de copia de seguridad en la nube pública" (p. 747).

Definición de una ubicación de copia de seguridad en Amazon S3

Nota
Para configurar ubicaciones de copia de seguridad en Amazon S3, debe tener uno de los siguientes roles definidos en el servicio de ciberprotección: Administrador de la empresa, Usuario, Administrador de cibernética.

Para hacer una copia de seguridad de una carga de trabajo en Amazon S3, debe definir la ubicación de la copia de seguridad en la consola de Cyber Protect y, luego, conectarse a la conexión relevante de Amazon S3. Puede hacerlo de las siguientes maneras:

- Al crear o editar un plan de protección.
- Al definir y gestionar ubicaciones de almacenamiento de copia de seguridad.

Importante
Tanto los administradores como los usuarios no administradores pueden hacer copias de seguridad de las cargas de trabajo en Amazon S3.

Los usuarios no administradores pueden añadir acceso a una conexión de Amazon S3 (ver "Gestión del acceso a otros servicios de almacenamiento en la nube pública" (p. 757)), pero solo pueden aplicar planes de protección donde la ubicación de la copia de seguridad está conectada a la conexión de Amazon S3 que ellos mismos añadieron, y para las cargas de trabajo registradas en la consola de Cyber Protect bajo su nombre.

Los administradores pueden aplicar planes de protección donde la ubicación de la copia de seguridad está conectada a las conexiones de Amazon S3 que ellos mismos añadieron o a las suscripciones añadidas por cualquier otro administrador, y para las cargas de trabajo registradas en la consola de Cyber Protect bajo cualquier usuario.

Pasos para definir una ubicación de respaldo en Amazon S3

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - Si está creando o editando un plan de protección, vaya a **Dispositivos** y seleccione la carga de trabajo de la que quiera hacer una copia de seguridad en Amazon S3. En la sección de **Copia de seguridad** del plan de protección de la carga de trabajo seleccionada, haga clic en el enlace en la fila **Dónde guardar las copias de seguridad**.

     Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 249).
   - Si está gestionando sus ubicaciones de almacenamiento de la copia de seguridad y quiere añadir Amazon S3 como una nueva ubicación, vaya a **Almacenamiento de la copia de seguridad**.

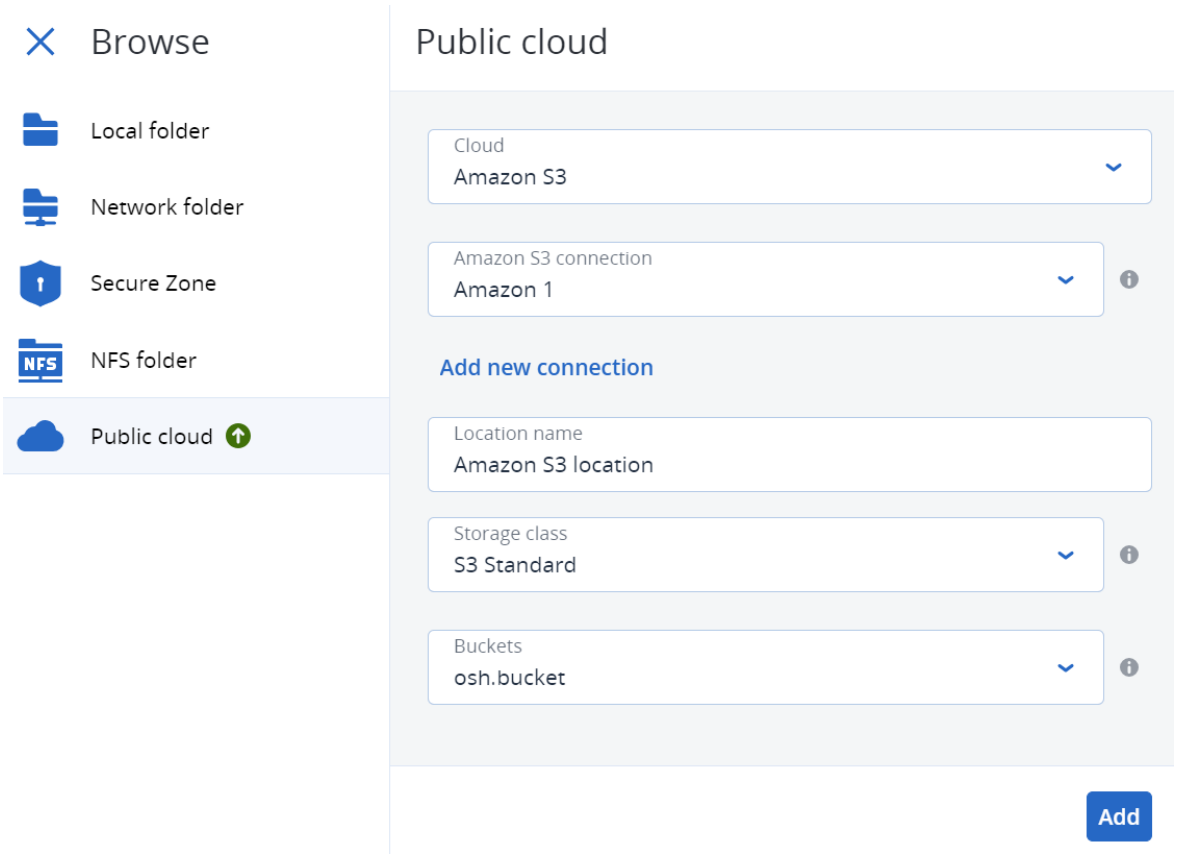
     Para obtener más información sobre cómo gestionar las ubicaciones de almacenamiento de copia de seguridad, consulte "Almacenamiento de copias de seguridad" (p. 720).
2. Haga clic en **Añadir ubicación**.
3. Desde la lista desplegable de **Nubes públicas**, seleccione **Amazon S3**.

   Nota
   Los buckets en regiones especiales de Government Cloud (por ejemplo, `us-gov-west-1`), no se admiten como ubicaciones de copia de seguridad.

4. Si la conexión relevante de Amazon S3 ya está registrada en la consola de Cyber Protect, selecciónela de la lista.

   Si la conexión relevante no está registrada en la consola de Cyber Protect, haga clic en **Añadir conexión nueva**. Para obtener más información sobre cómo añadir y definir el acceso a una conexión de Amazon S3, consulte "Añadir acceso a una conexión de nube pública" (p. 758). Cuando se añada la conexión, continúe al siguiente paso.

© Acronis International GmbH, 2003-2025



5. Defina lo siguiente:
   - En el campo **Nombre de la ubicación**, introduzca el nombre de la ubicación de la copia de seguridad.

     Nota
     El nombre de la ubicación debe ser único para el inquilino del cliente. Si el nombre que añade ya existe en la conexión, Acronis añade un número de sufijo al nombre. Por ejemplo, si **Almacenamiento de Amazon S3** ya existe, el nombre se actualizará automáticamente a **Almacenamiento de Amazon S3 1**.

   - En el campo **Clase de Almacenamiento**, seleccione una de las siguientes clases de almacenamiento admitidas:
     - S3 Standard
     - Standard: acceso poco frecuente (S3 Standard-IA)
     - One Zone: Acceso poco frecuente (S3 One Zone-IA)
     - S3 Intelligent Tiering

© Acronis International GmbH, 2003-2025

Nota
Al utilizar la clase de almacenamiento S3 Intelligent Tiering, los objetos de copia de seguridad antiguos se pueden mover automáticamente a los niveles de "Archive Access" o "Deep Archive Access" (para obtener más información acerca de estos niveles, consulte la documentación de Amazon S3). Los objetos en estos niveles no se pueden acceder de forma instantánea y requieren "re-hidratación", lo que significa que, cuando intente realizar la recuperación a partir de estas copias de seguridad antiguas, la recuperación fallará. Para realizar correctamente la recuperación a partir de estas copias de seguridad, primero recupere los objetos antiguos de los niveles de archivo comprimido relevantes. Para obtener más información acerca de la recuperación de datos de los niveles de archivo comprimido, consulte la documentación de Amazon S3.

- En el campo **Bucket**, selecciona el bucket relevante de Amazon S3.
  Si el bucket seleccionado está habilitado con las funciones Object Lock y Object Versioning (que están habilitadas en la Consola de Administración de AWS), se habilita la casilla de verificación **Periodo de inmutabilidad de la copia de seguridad (días)**. A continuación, puede definir el número de días para el periodo de inmutabilidad, que garantiza que los datos de la copia de seguridad no se eliminarán durante este periodo y se aplicará a todos los objetos de copia de seguridad creados por Acronis.
  Tenga en cuenta que, cuando establece el periodo de inmutabilidad como una propiedad de la ubicación de la copia de seguridad, se ignora el periodo de retención predeterminado definido para el bucket en la Consola de Administración de AWS. Para obtener más información sobre la función Object Lock y los periodos de retención, consulte la documentación de Amazon S3.

© Acronis International GmbH, 2003-2025

Nota
Se recomienda que configure la directiva de ciclo de vida para el bucket si ha establecido la opción de inmutabilidad al crear la ubicación de la copia de seguridad. Los buckets con las funciones de versionado de objetos y bloqueo de objetos habilitadas almacenarán versiones de objetos para siempre, lo que provocará que el consumo de almacenamiento crezca indefinidamente a menos que se configure una directiva de ciclo de vida.

Sin embargo, no se recomienda habilitar las funciones de versionado de objetos y bloqueo de objetos para los buckets utilizados por las ubicaciones de copia de seguridad y que están configurados sin la opción de inmutabilidad. Si se aplican directivas de ciclo de vida a estos buckets, pueden eliminar accidentalmente objetos relacionados con la cadena de archivos de copia de seguridad, lo que provocará la corrupción del archivo.

Con la opción de inmutabilidad configurada, el problema se resuelve ajustando el período de inmutabilidad para los objetos antiguos, de los que los objetos de copia de seguridad más nuevos aún tienen dependencias. Esto sucede automáticamente con cada copia de seguridad programada, donde el período de inmutabilidad de cada objeto que pertenece a la cadena de copia de seguridad se extiende mediante el agente de copia de seguridad que se comunica con el almacenamiento en la nube. Este período de inmutabilidad nunca es inferior al valor de días del período de inmutabilidad definido durante la creación de la ubicación de copia de seguridad. Para obtener más información sobre cómo configurar la directiva de ciclo de vida, consulte la documentación de Amazon S3.

Nota
Los agentes anteriores a la versión 24.05 pueden realizar copias de seguridad en Amazon S3, pero solo los agentes de la versión 24.05 o superior aplicarán Object Lock a los objetos creados en el almacenamiento de Amazon S3. Esto significa que solo los agentes más recientes pueden reconocer el periodo de inmutabilidad establecido como una propiedad de la ubicación de la copia de seguridad y administrarán este periodo para todas las copias de seguridad creadas. Los agentes anteriores a la versión 24.05 ignorarán esta configuración y las propiedades de Object Lock del depósito predeterminado (definidas en la consola de administración de AWS o mediante la API) se aplicarán a los objetos creados en Amazon S3.

6. Haga clic en **Agregar**.

   Si está creando o editando un plan de protección, la ubicación de la copia de seguridad de Amazon S3 se establece como la ubicación en la fila **Dónde guardar las copias de seguridad**. Cuando se ejecuta la copia de seguridad (ya sea manualmente o cuando está programada), la copia de seguridad se guarda en la ubicación definida.

   Si está gestionando sus ubicaciones de almacenamiento de copia de seguridad, puede ver y actualizar los detalles de la ubicación según sea necesario. La ubicación de Amazon S3 también está disponible al definir una ubicación de copia de seguridad para cargas de trabajo. Para

© Acronis International GmbH, 2003-2025

obtener más información, consulte "Visualización y actualización de ubicaciones de copia de seguridad en la nube pública" (p. 747).

Definición de una ubicación de copia de seguridad en un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3

Nota

- Para configurar ubicaciones de copia de seguridad en un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3, debe tener uno de los siguientes roles definidos en el servicio de ciberprotección: Administrador de empresa, Usuario o Administrador de cibernética.
- Los buckets en regiones especiales GovCloud (por ejemplo, `s3.eu-central-1.wasabisys.com` u otras URL de endpoint de proveedores de almacenamiento que admiten el concepto de GovCloud), no son compatibles como ubicaciones de copia de seguridad.

Para realizar una copia de seguridad de una carga de trabajo en Wasabi, IONOS Cloud, Impossible Cloud o un almacenamiento compatible con S3, debe definir la ubicación de la copia de seguridad en la consola de Cyber Protect y (solo para Wasabi) conectarse a la conexión de almacenamiento de Wasabi correspondiente. Puede hacerlo de las siguientes maneras:

- Al crear o editar un plan de protección.
- Al definir y gestionar ubicaciones de almacenamiento de copia de seguridad.

© Acronis International GmbH, 2003-2025

Importante
Tanto los administradores como los usuarios que no son administradores pueden realizar copias de seguridad de cargas de trabajo en almacenamientos compatibles con Wasabi, IONOS Cloud, Impossible Cloud o S3.

Los usuarios que no son administradores pueden añadir acceso a una conexión de almacenamiento de Wasabi (consulte "Gestión del acceso a otros servicios de almacenamiento en la nube pública" (p. 757)), pero solo pueden aplicar planes de protección en los que la ubicación de la copia de seguridad esté conectada a la conexión de almacenamiento de Wasabi que añadieron ellos mismos y para cargas de trabajo registradas en la consola de Cyber Protect a su nombre. Los usuarios que no son administradores también pueden aplicar planes de protección que utilicen las ubicaciones de copia de seguridad en un almacenamiento compatible con Impossible Cloud, IONOS Cloud o S3 creadas por ellos mismos y para cargas de trabajo registradas en la consola de Cyber Protect a su nombre.

Los administradores pueden aplicar planes de protección que utilicen la ubicación de copia de seguridad conectada a las conexiones de almacenamiento de Wasabi, IONOS Cloud, Impossible Cloud o compatibles con S3 que añadieron ellos mismos o cualquier otro administrador y para cargas de trabajo registradas en la consola de Cyber Protect a nombre de cualquier usuario.

Para definir una ubicación de copia de seguridad en un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3

1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - Si está creando o editando un plan de protección, vaya a **Dispositivos** y seleccione el recurso informático del que quiera hacer una copia de seguridad en un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3. En la sección de **Copia de seguridad** del plan de protección de la carga de trabajo seleccionada, haga clic en el enlace en la fila **Dónde guardar las copias de seguridad**.
     Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 249).
   - Si está gestionando sus ubicaciones de almacenamiento de copia de seguridad y quiere añadir un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3 como una nueva ubicación, vaya a **Almacenamiento de la copia de seguridad**.
     Para obtener más información sobre cómo gestionar las ubicaciones de almacenamiento de copia de seguridad, consulte "Almacenamiento de copias de seguridad" (p. 720).
2. Haga clic en **Añadir ubicación**.
3. En la lista desplegable **Nubes públicas**, seleccione una de los siguientes:
   - **Wasabi**
   - **Compatible con S3**

© Acronis International GmbH, 2003-2025

- **Impossible Cloud**
- **IONOS Cloud**

4. [Solo para Wasabi] Si la conexión relevante ya está registrada en la consola de Cyber Protect, selecciónela de la lista de conexiones.
   Si la conexión correspondiente no está registrada en la consola de Cyber Protect, haga clic en **Añadir conexión nueva**. Cuando se haya añadido la conexión, continúe con el siguiente paso.

   Importante
   Las claves de acceso para las cuentas de usuario raíz en Wasabi no se pueden utilizar porque los usuarios raíz no pueden llamar AssumeRole. Debería crear un usuario no raíz separado y generar claves de acceso para ese usuario.

5. Defina lo siguiente:
   - [Para compatible con S3, IONOS Cloud o Impossible Cloud] En el campo **Agente de gestión**, haga clic en **Examinar** para seleccionar el agente de gestión de una lista de agentes adecuados.
     Este agente establecerá la comunicación inicial con el almacenamiento compatible con S3 / IONOS Cloud / Impossible Cloud. Puede modificar los parámetros de la ubicación de la copia de seguridad más adelante, si es necesario.

     Este agente de gestión, que se puede seleccionar de cualquier tipo de agente compatible (incluido el Agente para Windows/Linux/VMware (dispositivo virtual)/Hyper-V/oVirt (pero no el Agente para Azure)), se utiliza solo durante la creación o edición de la ubicación de la copia de seguridad. El estado offline/online del agente no afectará a las copias de seguridad realizadas por otros agentes regulares.
   - En el campo **Nombre de la ubicación**, introduzca el nombre de la ubicación de la copia de seguridad.

     Nota
     El nombre de la ubicación debe ser único para el inquilino del cliente. Si el nombre que añade ya existe en la conexión, Cyber Protect Cloud añadirá un número de sufijo al nombre. Por ejemplo, si el **almacenamiento de Wasabi** ya existe, el nombre se actualizará automáticamente a **almacenamiento de Wasabi 1**.

   - En el campo **Celda**, seleccione el bucket de almacenamiento correspondiente compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3.
     Si el bucket seleccionado está habilitado con las funciones Object Lock y Versioning, se habilita la casilla de verificación **Periodo de inmutabilidad de la copia de seguridad (días)**. A continuación, puede definir la cantidad de días para el periodo de inmutabilidad, que garantiza que los datos de la copia de seguridad no se eliminarán durante este periodo y se aplicará a todos los objetos de copia de seguridad creados por Cyber Protect Cloud.

© Acronis International GmbH, 2003-2025

Nota
No puede establecer el período de inmutabilidad de las ubicaciones de copia de seguridad en Wasabi. Actualmente, solo se admiten los tipos compatibles con S3, IONOS Cloud, Impossible Cloud y Amazon S3 (consulte "Definición de una ubicación de copia de seguridad en Amazon S3" (p. 737)).

Tenga en cuenta que, cuando establece el periodo de inmutabilidad como una propiedad de la ubicación de la copia de seguridad, se ignora el periodo de retención predeterminado definido para el bucket. Para obtener más información sobre la función Object Lock y los periodos de retención, consulte la documentación correspondiente. Por ejemplo, consulte la documentación de Impossible Cloud.

Nota
Recomendamos que configure la directiva de ciclo de vida para el bucket si ha establecido la opción de inmutabilidad al crear la ubicación de copia de seguridad. Los buckets con las funciones de versionado de objetos y bloqueo de objetos habilitados almacenarán versiones de objetos para siempre, lo que provocará que el consumo de almacenamiento crezca indefinidamente a menos que se configure una directiva de ciclo de vida.

Sin embargo, no recomendamos habilitar las funciones de versionado de objetos y bloqueo de objetos para los buckets utilizados por las ubicaciones de copia de seguridad y que están configuradas sin la opción de inmutabilidad. Si se aplican directivas de ciclo de vida a estos buckets, pueden eliminar accidentalmente objetos relacionados con la cadena de archivos de copia de seguridad, lo que provocará la corrupción del archivo.

Con la opción de inmutabilidad configurada, el problema se resuelve ajustando el período de inmutabilidad para los objetos antiguos, de los que los objetos de copia de seguridad más recientes aún tienen dependencias. Esto sucede automáticamente con cada copia de seguridad programada, donde el período de inmutabilidad de cada objeto que pertenece a la cadena de copia de seguridad se extiende mediante el agente de copia de seguridad que se comunica con el almacenamiento en la nube. Este período de inmutabilidad nunca es inferior al valor de días del período de inmutabilidad definido durante la creación de la ubicación de copia de seguridad. Para obtener más información sobre cómo configurar la directiva de ciclo de vida, consulte la documentación de Wasabi (que también es aplicable cuando se agrega el almacenamiento en la nube pública de Wasabi como un tipo de ubicación de copia de seguridad "compatible con S3").

© Acronis International GmbH, 2003-2025

Nota
Los agentes anteriores a la versión 24.06 pueden realizar copias de seguridad en un almacenamiento compatible con Wasabi, Impossible Cloud o S3, pero solo los agentes de la versión 24.06 o superior aplicarán Obkect Lock a los objetos creados en un almacenamiento compatible con Wasabi, Impossible Cloud o S3. Esto significa que solo los agentes más recientes pueden reconocer el periodo de inmutabilidad establecido como una propiedad de ubicación de copia de seguridad y gestionarán este periodo para todas las copias de seguridad creadas. Los agentes anteriores a la versión 24.06 ignorarán esta configuración y las propiedades de Object Lock del bucket predeterminado se aplicarán a los objetos creados en un almacenamiento compatible con Wasabi, Impossible Cloud o S3.

[Solo para Impossible Cloud] La lista de buckets se recupera siempre de la URL del endpoint principal (`https://eu-central-2.storage.impossibleapi.net/`), que lista los buckets en todas las regiones. La URL del endpoint utilizada para leer y escribir datos en el bucket se calcula a partir de la región detectada del bucket y está en el siguiente formato: `https://[REGION_NAME].storage.impossibleapi.net`. Por ejemplo, si selecciona el bucket **eu-central-1**, la URL del endpoint sería `https://eu-central-1.storage.impossibleapi.net/`.

[Solo para IONOS Cloud] La lista de buckets se recupera siempre de la URL del endpoint principal (`https://s3.eu-central-4.ionoscloud.com`), que lista los buckets en todas las regiones. La URL del endpoint utilizada para leer y escribir datos en el bucket se calcula a partir de la región detectada del bucket y está en el siguiente formato: `https://s3.[REGION_NAME].ionoscloud.com`. Por ejemplo, si selecciona el bucket **eu-central-2**, la URL del endpoint sería `https://s3.eu-central-2.ionoscloud.com/`.

Nota
Los buckets de usuario en IONOS Cloud no se enumerarán porque requieren una URL de endpoint única para el acceso. Para utilizar los buckets de usuario como ubicaciones de copia de seguridad, debe configurar un tipo de ubicación de copia de seguridad **Compatible con S3**, en lugar de **IONOS Cloud**.

- [Solo para el almacenamiento compatible con S3] Seleccione la casilla de verificación **Permitir el uso de un certificado firmado automáticamente del endpoint (vulnerable a ataques MITM, no recomendado)** para omitir la validación de la cadena de certificados y aceptar los certificados firmados automáticamente para la URL del endpoint de S3.

  Tenga en cuenta que esta opción solo está disponible al crear la ubicación de copia de seguridad compatible con S3 y no se puede cambiar al editar la ubicación de copia de seguridad.

6. Haga clic en **Agregar**.

   Si está creando o editando un plan de protección, la ubicación de la copia de seguridad del almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3 se establece como la ubicación en la fila **Dónde guardar las copias de seguridad**. Cuando se ejecuta la

© Acronis International GmbH, 2003-2025

copia de seguridad (ya sea manualmente o cuando está programada), esta se guarda en la ubicación definida.

Si gestiona sus ubicaciones de almacenamiento de copia de seguridad, puede ver y actualizar la información de la ubicación cuando sea necesario. La ubicación del almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3 también está disponible cuando se define una ubicación de copia de seguridad para cargas de trabajo. Para obtener más información, consulte "Visualización y actualización de ubicaciones de copia de seguridad en la nube pública" (p. 747).

Visualización y actualización de ubicaciones de copia de seguridad en la nube pública

Puede ver y actualizar las ubicaciones de copia de seguridad de Microsoft Azure, Amazon S3 y Wasabi que defina en el módulo **Almacenamiento de la copia de seguridad**, o al crear o editar un plan de protección.

Para obtener información sobre cómo eliminar el acceso a una suscripción de Microsoft Azure desde la consola de Cyber Protect, consulte "Eliminar el acceso a una suscripción de Microsoft Azure" (p. 756). Para obtener información sobre cómo eliminar el acceso a otras conexiones de nube pública, consulte "Gestión del acceso a otros servicios de almacenamiento en la nube pública" (p. 757).

Nota
No puede actualizar manualmente ni eliminar una ubicación de copia de seguridad en la nube pública en el módulo de **Almacenamiento de la copia de seguridad**. El contenido de la ubicación de la copia de seguridad se actualiza automáticamente después de cada operación de copia de seguridad o recuperación.

Pasos para ver ubicaciones de copia de seguridad en la nube pública

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
   Se muestra una lista de ubicaciones de copia de seguridad, con detalles de la capacidad de almacenamiento y el número de copias de seguridad asignadas a cada ubicación.
   Para obtener más información sobre cómo trabajar con las ubicaciones de copia de seguridad de la lista, consulte "Almacenamiento de copias de seguridad" (p. 720).
2. Seleccione la ubicación correspondiente.
   Se incluyen las copias de seguridad que existan en la ubicación seleccionada.
3. (Opcional) Haga clic en una copia de seguridad para ver más detalles sobre la misma.

Pasos para actualizar una ubicación de copia de seguridad en la nube pública en un plan de protección

1. Vaya al plan de protección correspondiente y seleccione **Editar**.
2. Haga clic en el enlace en la fila **Dónde guardar las copias de seguridad**.

© Acronis International GmbH, 2003-2025

3. Seleccione una de las ubicaciones de copia de seguridad de la lista o haga clic en **Añadir ubicación** para añadir una nueva.

   Si la suscripción correspondiente de Microsoft Azure o la conexión a la nube pública ya está registrada en la consola de Cyber Protect, selecciónela de la lista que se muestra.

   Si añade una nueva suscripción de Microsoft Azure, se le pedirá que autentifique la información de su cuenta de Microsoft (consulte "Añadir el acceso a una suscripción de Microsoft Azure" (p. 754)). Para obtener más información sobre los permisos requeridos al conectarse a Microsoft Azure, consulte el artículo Seguridad y auditoría de conexión de Microsoft Azure (72684).

Gestionar el acceso a la cuenta de la nube pública

Para habilitar los servicios de Acronis Cyber Protection en las plataformas de nube pública, se debe configurar el acceso a las cuentas de Microsoft Azure, Amazon S3 y Wasabi correspondientes.

Por ejemplo, cuando se trabaja con Microsoft Azure, se requiere acceso a su suscripción de Microsoft Azure. Una vez añadida en la consola de Cyber Protect, la suscripción puede ser seleccionada cuando configure una copia de seguridad directa a Microsoft Azure. Igualmente, en el caso de Amazon S3 y Wasabi, se requieren las claves de acceso relevantes que están asociadas con políticas específicas relacionadas con la copia de seguridad.

El acceso a las nubes públicas se gestiona a través del menú **Infraestructura** en la consola de Cyber Protect.

Advertencia.
Después de añadir una ubicación, no puede quitarla. Solo puede eliminarla.

Importante
La validación de copia de seguridad está desactivada para las copias de seguridad en el almacenamiento en la nube pública para evitar costes excesivos de tráfico de salida. Además, actualmente no puede «volver a adjuntar» una ubicación de copia de seguridad en una nube pública al mismo inquilino de cliente o a uno diferente si la ubicación ha sido previamente eliminada.

Requisitos de acceso necesarios para hacer una copia de seguridad en el almacenamiento en la nube pública

Cuando se realiza una copia de seguridad directa en los servicios de almacenamiento en la nube pública, hay una serie de requisitos de acceso que considerar para cada plataforma:

- Microsoft Azure
- Amazon S3
- Almacenamiento compatible con S3 (incluye Wasabi, IONOS Cloud e Impossible Cloud)

© Acronis International GmbH, 2003-2025

Copia de seguridad en Microsoft Azure

Para conectarse a una suscripción de Microsoft Azure, debe tener varios permisos. Para obtener más información sobre ellos, consulte el artículo Seguridad y auditoría de conexión de Microsoft Azure (72684).

Nota
Debe tener asignado uno de los siguientes roles en Microsoft Azure AD para poder completar la conexión con la suscripción: Administrador de aplicaciones en la nube, administrador de aplicaciones o administrador general. También debe tener asignado el rol Propietario para cada suscripción seleccionada.

Copia de seguridad en Amazon S3

Cuando hace una copia de seguridad en Amazon S3, hay varios requisitos al definir las ubicaciones de copia de seguridad de Amazon S3:

- Clases de almacenamiento admitidas
- Permisos de directiva
- Claves de acceso
- Configuración del bucket

Clases de almacenamiento admitidas

Las siguientes clases de almacenamiento de Amazon S3 se admiten actualmente:

- S3 Standard
- Standard: acceso poco frecuente (S3 Standard-IA)
- One Zone: Acceso poco frecuente (S3 One Zone-IA)
- S3 Intelligent Tiering

Permisos de directiva

Cuando hace una copia de seguridad en Amazon S3, su cuenta de Amazon debe tener los permisos mínimos aplicados para asegurar que Cyber Protect Cloud pueda hacer una copia de seguridad de las cargas de trabajo relevantes en Amazon S3. Esto significa que los usuarios relevantes deberían tener acceso a la Consola de Administración de AWS y tener la política relevante aplicada a los grupo(s) a los que están asignados.

Nota
Los permisos de la directiva especificados para Amazon S3 pueden reutilizarse en otros servicios de almacenamiento compatibles con S3. Para obtener más información, consulte "Copia de seguridad en almacenamiento compatible con S3 (incluye Wasabi, IONOS Cloud e Impossible Cloud)" (p. 751).

Ejemplos

© Acronis International GmbH, 2003-2025

La siguiente directiva de ejemplo muestra el conjunto mínimo de permisos para un amplio ámbito de recursos al realizar copias de seguridad y recuperaciones a/desde un bucket específico (indicado por [BUCKETNAME]). Tenga en cuenta que * indica todos los recursos.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

La siguiente política de ejemplo muestra los permisos mínimos limitados a un bucket específico. Tenga en cuenta que `[BUCKETNAME]` debe remplazarse por el nombre del bucket.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::*" }, { "Effect": "Allow",
"Action": "sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::*" } ] }
```

Claves de acceso

Para cada conexión de Amazon S3, se requieren claves de acceso que se utilizan al definir la conexión de Amazon S3. Para obtener más información sobre cómo generar claves de acceso e ID de claves de acceso, consulte la documentación de Amazon S3.

Configuración del bucket

Al utilizar los buckets de Amazon S3 como ubicación de copia de seguridad, asegúrese de que el bucket esté configurado con los ajustes predeterminados, incluyendo el bloqueo de todo el acceso público (por defecto, esto está establecido en **Activado**). Para obtener más información sobre cómo trabajar con buckets, consulte la documentación de Amazon S3.

Nota

Los ejemplos en Permisos de directiva incluyen un conjunto completo de permisos. Si no necesita inmutabilidad en un bucket, puede excluir los permisos relacionados, como `s3:GetBucketObjectLockConfiguration` (que se utiliza para crear y editar la ubicación de la copia de seguridad) y `s3:GetObjectRetention` (que se utiliza para detectar la necesidad de actualizar el bloqueo de un objeto por un periodo reducido).

© Acronis International GmbH, 2003-2025

Copia de seguridad en almacenamiento compatible con S3 (incluye Wasabi, IONOS Cloud e Impossible Cloud)

Cuando hace una copia de seguridad en un almacenamiento compatible con S3, hay una serie de requisitos que debe tener en cuenta al definir las ubicaciones de copia de seguridad:

- Permisos de directiva
- Claves de acceso
- Configuración del bucket

Permisos de directiva

Cuando defina una ubicación de copia de seguridad en un almacenamiento compatible con S3, asegúrese de que las políticas relevantes se apliquen a los grupos y usuarios pertinentes.

Nota
Los permisos de directiva especificados para Amazon S3 (consulte arriba) pueden reutilizarse por otros servicios de almacenamiento compatibles con S3. Tenga en cuenta que el permiso `sts:GetFederationToken` solo es aplicable a Amazon S3 y no es necesario para otros servicios de almacenamiento compatibles con S3.

Importante
Cuando se crea la conexión a Wasabi por primera vez, se utilizan las credenciales temporales creadas con el permiso `AssumeRole`. Esto da como resultado permisos de acceso adicionales, lo que significa que, incluso si hay permisos en la directiva de Wasabi que restringen el trabajo con buckets específicos, estos buckets seguirán apareciendo en la lista desplegable de buckets disponibles. Las operaciones de copia de seguridad y recuperación funcionarán con cualquier bucket seleccionado de la lista.

Sin embargo, el token de acceso proporcionado al agente durante las operaciones de copia de seguridad/recuperación está limitado a operaciones en un único bucket específico: el bucket seleccionado al crear la ubicación de copia de seguridad en Wasabi en la consola de Cyber Protect. Como resultado, después de que se crea la ubicación de copia de seguridad, el sistema limitará las operaciones del agente únicamente al bucket seleccionado.

Ejemplos

El siguiente ejemplo de directiva es solo para Wasabi y muestra los permisos mínimos para cualquier bucket de la cuenta.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
```


© Acronis International GmbH, 2003-2025

```
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource": "*"
}, { "Effect": "Allow", "Action": [ "s3:ListBucket", "s3:ListBucketVersions" ],
"Resource": "*" }, { "Effect": "Allow", "Action": [ "iam:CreateRole",
"iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "*"
}, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject", "s3:GetObjectVersion", "s3:GetObjectRetention",
"s3:PutObjectRetention" ], "Resource": "*" } ] }
```

La siguiente directiva de ejemplo es para un almacenamiento compatible con S3, IONOS Cloud e Impossible Cloud y muestra permisos limitados con un ámbito limitado de recursos. Tenga en cuenta que `[BUCKETNAME]` debe reemplazarse con el nombre del bucket.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

El siguiente ejemplo de directiva es para el almacenamiento compatible con S3, IONOS Cloud e Impossible Cloud y muestra los permisos mínimos para cualquier bucket de la cuenta.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::*" } ] }
```

Claves de acceso

Se requieren claves de acceso para cada conexión compatible con S3, y se utilizan cuando se define la conexión.

Tenga en cuenta que las claves de acceso para las cuentas de usuario raíz en Wasabi no se pueden utilizar porque los usuarios raíz no pueden llamar AssumeRole. Debería crear un usuario no raíz separado y generar claves de acceso para ese usuario.

© Acronis International GmbH, 2003-2025

Para obtener más información sobre la generación de claves de acceso y claves de acceso ID, consulte la documentación correspondiente. Por ejemplo, consulte la documentación de Wasabi, la documentación de IONOS Cloud y la documentación de Impossible Cloud.

Configuración del bucket

Al utilizar los buckets como ubicación de la copia de seguridad, asegúrese de que el bucket esté configurado con los ajustes predeterminados. Para obtener más información sobre cómo trabajar con los buckets, consulte la documentación correspondiente. Por ejemplo, consulte la documentación de Wasabi, la documentación de IONOS Cloud y la documentación de Impossible Cloud.

Gestionar el acceso a las suscripciones de Microsoft Azure

Al conectarse a las suscripciones de Microsoft Azure correspondientes en la consola de Cyber Protect, puede hacer copias de seguridad directamente de las cargas de trabajo relevantes en Microsoft Azure.

Se puede configurar la conexión a una suscripción al crear una ubicación de copia de seguridad a través del menú **Dispositivos** o **Almacenamiento de la copia de seguridad**, tal y como se describe en "Definir una ubicación de copia de seguridad en Microsoft Azure" (p. 734).

Como alternativa, estas suscripciones de Microsoft Azure se pueden configurar en la pantalla **Nubes públicas** (vaya a **Infraestructura > Nubes públicas**). Aquí también puede gestionar sus suscripciones, incluyendo la renovación del acceso a la suscripción, la visualización de las propiedades y actividades de la suscripción o la eliminación de la suscripción. Tenga en cuenta que si está desplegando el agente para Azure para ejecutar copias de seguridad sin agente de máquinas virtuales de Microsoft Azure, se muestra una pestaña adicional donde puede visualizar y actualizar su despliegue. Para obtener más información, consulte "Visualización y actualización de un agente para Azure desplegado" (p. 169).

Según su rol de usuario asignado, podrá gestionar las suscripciones de Microsoft Azure añadidas por otros usuarios dentro de su organización. Por ejemplo, si es un administrador de la empresa o administrador de la unidad, o si se le ha asignado el rol de administrador de cibernética o administrador en el servicio de ciberprotección, podrá ver y gestionar las suscripciones de Microsoft Azure añadidas por otros administradores y las añadidas por usuarios que no son administradores. Los usuarios que no son administradores solo pueden ver y acceder a las suscripciones de Microsoft Azure que ellos mismos añadan a la consola de Cyber Protect.

Nota
Los partners pueden gestionar las suscripciones de Microsoft Azure de los clientes que estén bajo su nivel en la jerarquía. Sin embargo, cuando un partner selecciona **Todos los clientes**, el menú **Infraestructura** de la consola de Cyber Protect no está disponible.

© Acronis International GmbH, 2003-2025

Importante
Al conectarse a una suscripción de Microsoft Azure, Acronis requiere los permisos mínimos para conectarse a la suscripción. Para obtener más información sobre los permisos necesarios, consulte el artículo Seguridad y auditoría de la conexión de Microsoft Azure (72684).

Añadir el acceso a una suscripción de Microsoft Azure

Al añadir una suscripción de Microsoft Azure en la consola de Cyber Protect, Acronis puede acceder de forma segura a su suscripción y hacer copias de seguridad directamente de las cargas de trabajo correspondientes en Microsoft Azure.

Pasos para añadir el acceso a una suscripción de Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Haga clic en **Agregar**, y de la lista de opciones mostrada, seleccione **Microsoft Azure**.
3. En el diálogo mostrado, haga clic en **Iniciar sesión**. Se le redirigirá a la página de inicio de sesión de Microsoft.

   Nota
   Debe tener asignado uno de los siguientes roles en Microsoft Azure AD para poder completar la conexión con la suscripción: Administrador de aplicaciones en la nube, administrador de aplicaciones o administrador general. También debe tener asignado el rol Propietario para cada suscripción seleccionada.

4. En la pantalla de inicio de sesión de Microsoft, introduzca las credenciales de inicio de sesión y acepte los permisos solicitados. Se iniciará el proceso de conexión y puede tardar varios minutos.

   Para obtener más información sobre el acceso seguro a su suscripción de Microsoft Azure, consulte el artículo Auditoría y seguridad de conexión de Microsoft Azure (72684).
5. Cuando la conexión se haya completado, realice lo siguiente:
   a. En el campo **Suscripción de Microsoft Azure**, seleccione la suscripción correspondiente de la lista.
   b. [Opcional] En el campo **Región de Azure**, seleccione la región en la que desplegar los recursos del sistema.

      Nota
      El sistema preselecciona la región en la que se encuentran la mayoría de los grupos de recursos, pero puede cambiarla según su preferencia.

6. Haga clic en **Agregar suscripción**.

   Se añadirá la suscripción a la lista de nubes públicas.

   Para renovar el certificado de acceso anual de la suscripción, consulte "Renovar el acceso a una suscripción de Microsoft Azure" (p. 755).

© Acronis International GmbH, 2003-2025

Para eliminar el acceso a la suscripción, consulte "Eliminar el acceso a una suscripción de Microsoft Azure" (p. 756).

Nota
Si la cuenta de Microsoft Azure en la que ha iniciado sesión incluye acceso a varios Microsoft Azure AD, incluidos aquellos en los que es un usuario invitado, solo se seleccionará el directorio del usuario predeterminado. Si quiere usar un directorio en el que es un usuario invitado, deberá crear un nuevo usuario en ese Microsoft Azure AD específico. A continuación, puede iniciar sesión en esa cuenta y conectar la suscripción correspondiente.

Renovar el acceso a una suscripción de Microsoft Azure

Cuando un usuario se registra en la consola de Cyber Protect, Acronis le asigna automáticamente el acceso a una suscripción de Microsoft Azure durante un año con un certificado de acceso único y gratuito. Cuando se acerque la fecha de caducidad del certificado, puede renovarlo de forma rápida y fácil.

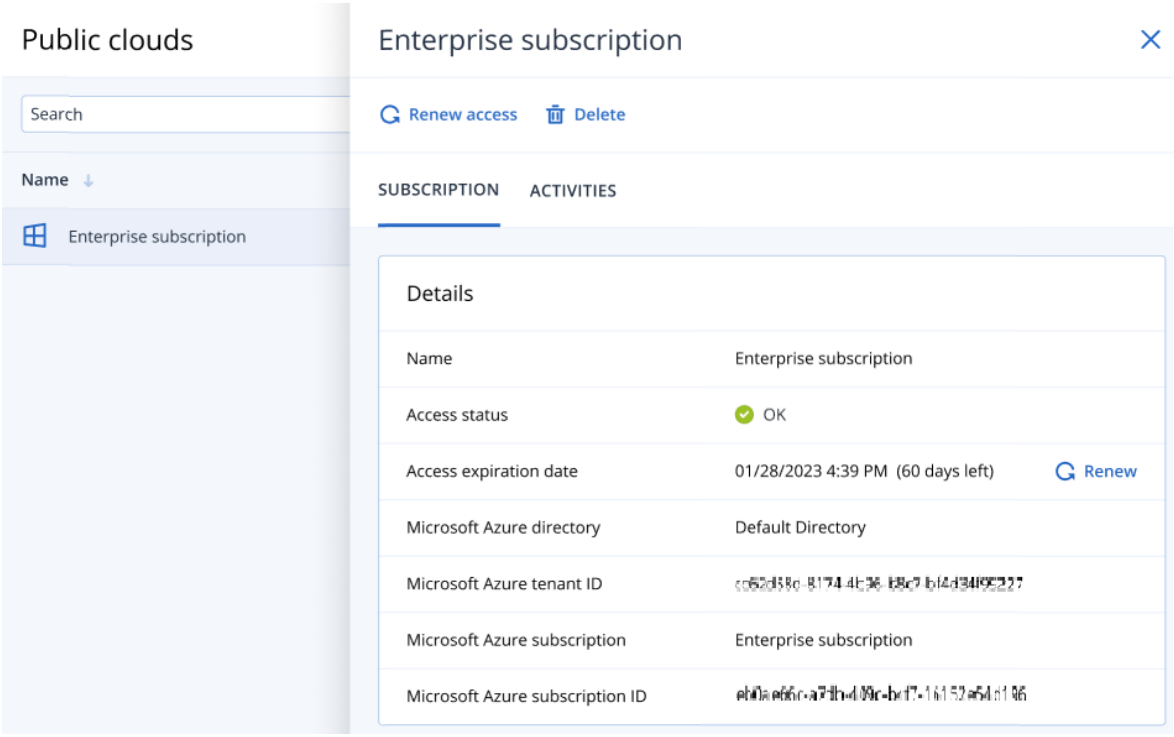
Pasos para renovar el certificado de acceso de la suscripción de Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la suscripción correspondiente en la lista que se muestra.

   Nota
   La columna **Estado del acceso** indica el estado actual del certificado de acceso de cada suscripción y muestra uno de estos dos estados: **OK** o **Caducado**.

3. En el panel derecho, haga clic en **Renovar acceso**.
   Otra opción es hacer clic en la pestaña **Suscripción** y, a continuación, en **Renovar** en el campo **Fecha de caducidad del acceso**.

© Acronis International GmbH, 2003-2025



4. En la pantalla de inicio de sesión de Microsoft, introduzca las credenciales de inicio de sesión y acepte los permisos solicitados. Se iniciará el proceso de conexión y puede tardar varios minutos.
   Si la autenticación es correcta, el acceso se renovará automáticamente durante un año.
   Para obtener más información sobre los permisos necesarios, consulte el artículo Auditoría y seguridad de conexión de Microsoft Azure (72684).

Eliminar el acceso a una suscripción de Microsoft Azure

Es recomendable eliminar el acceso a la suscripción de Microsoft Azure si no se realizan copias de seguridad de cargas de trabajo en Microsoft Azure.

Pasos para eliminar el acceso a una suscripción de Microsoft Azure

Importante
No puede eliminar una suscripción si se está utilizando para hacer copias de seguridad en Microsoft Azure.

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la suscripción correspondiente en la lista que se muestra.
3. En el panel derecho, haga clic en **Eliminar**.

Nota
Solo puede eliminar las suscripciones que haya añadido usted. También puede eliminar una suscripción si es un administrador de la empresa o de la unidad, o si tiene asignado el rol Administrador de cibernética o Administrador en el servicio de ciberprotección.

© Acronis International GmbH, 2003-2025

4. Haga clic en **Eliminar** en el mensaje de confirmación que se muestra.

Gestión del acceso a otros servicios de almacenamiento en la nube pública

Nota
Esta sección se refiere a la gestión del acceso a los servicios de almacenamiento de Amazon S3 o Wasabi. La gestión del acceso a Microsoft Azure se describe en "Gestionar el acceso a las suscripciones de Microsoft Azure" (p. 753).

Al conectarse a la cuenta de Amazon S3 o Wasabi correspondiente en la consola de Cyber Protect, puede hacer una copia de seguridad directamente de las cargas de trabajo al almacenamiento en la nube pública pertinente.

Puede configurar conexiones a cuentas de almacenamiento en la nube pública al crear una ubicación de copia de seguridad a través del menú **Dispositivos** o **Almacenamiento de la copia de seguridad**. De manera alternativa, puede configurar conexiones a la nube pública en la pantalla **Nubes públicas** (vaya a **Infraestructura > Nubes públicas**). Aquí también puede gestionar su conexión, incluyendo la renovación del acceso a la conexión, la visualización de las propiedades y actividades de la conexión, o la eliminación de la conexión.

Dependiendo de su rol de usuario asignado, es posible que pueda gestionar las conexiones a la nube pública añadidas por otros usuarios dentro de su organización. Por ejemplo, si es un administrador de la empresa o administrador de la unidad, o si se le ha asignado el rol de Administrador de cibernética o Administrador en el servicio de ciberprotección, puede ver y gestionar las conexiones a la nube pública añadidas por otros administradores, así como las conexiones añadidas por usuarios no administradores. Los usuarios no administradores solo pueden ver y acceder a las conexiones a la nube pública que ellos mismos añadieron a la consola de Cyber Protect.

Nota
Los partners pueden gestionar las conexiones de nube pública de los clientes que están por debajo de su nivel en la jerarquía. Sin embargo, cuando un partner selecciona **Todos los clientes**, el menú de **Infraestructura** en la consola de Cyber Protect no está disponible.

Importante
Al conectarse a una conexión de nube pública, Acronis requiere una serie de permisos. Para obtener más información, consulte "Requisitos de acceso necesarios para hacer una copia de seguridad en el almacenamiento en la nube pública" (p. 748).

© Acronis International GmbH, 2003-2025

Añadir acceso a una conexión de nube pública

Nota
Los buckets en regiones especiales GovCloud (por ejemplo, `s3.eu-central-1.wasabisys.com` u otras URL de endpoint de proveedores de almacenamiento que admiten el concepto de GovCloud), no son compatibles como ubicaciones de copia de seguridad.

Después de añadir una conexión a la nube pública para almacenamiento en la nube de Amazon S3 o Wasabi en la consola de Cyber Protect, puede acceder de manera segura a sus recursos en la nube y hacer copias de seguridad de las cargas de trabajo directamente en el almacenamiento en la nube pública correspondiente.

Advertencia.
Después de agregar una ubicación, no puede eliminar el acceso a la nube pública. Para eliminar el acceso, debe eliminar la ubicación. Consulte "Eliminación de una conexión a la nube pública" (p. 761).

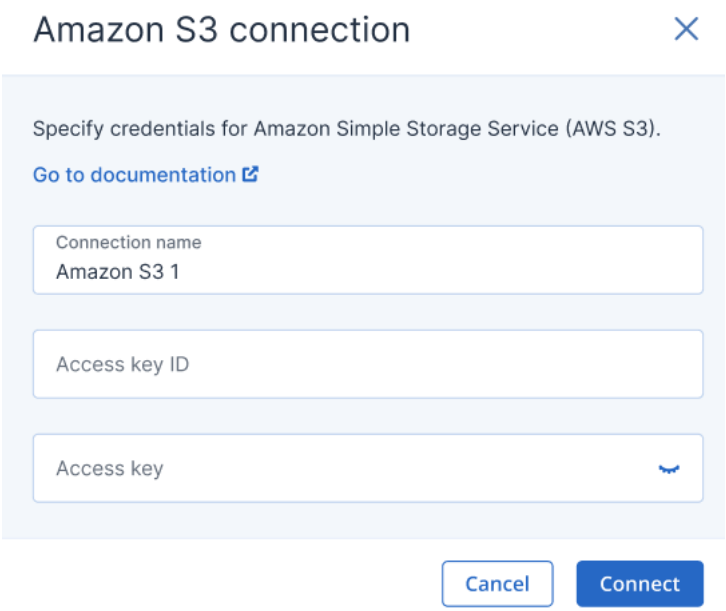
Para obtener más información sobre cómo añadir acceso al almacenamiento en la nube de Microsoft Azure, consulte "Gestionar el acceso a las suscripciones de Microsoft Azure" (p. 753).

Pasos para añadir acceso a una conexión de nube pública

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Haga clic en **Agregar** y seleccione una de las siguientes opciones:

   Amazon S3
   En el diálogo que se muestra, defina lo siguiente:
   - **Nombre de la conexión**: El nombre para la conexión de Amazon S3.
   - **ID de la clave de acceso**: El ID de clave de acceso del usuario para el servicio de Amazon S3.
   - **Clave de acceso**: La clave de acceso del usuario para el servicio de Amazon S3.
     La clave de acceso y el ID de la clave de acceso permiten acceder a las clases de almacenamiento y los buckets para la conexión relevante. Para obtener más información sobre las claves de acceso y los permisos, consulte "Requisitos de acceso necesarios para hacer una copia de seguridad en el almacenamiento en la nube pública" (p. 748).

© Acronis International GmbH, 2003-2025

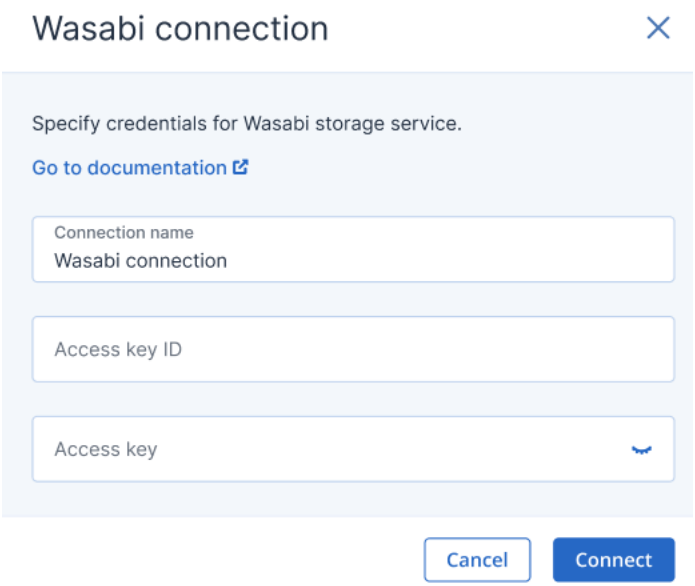


Nota
Para acceder al almacenamiento correctamente, la hora del sistema en el agente que realiza las operaciones de copia de seguridad y recuperación con el almacenamiento de Amazon S3 debe sincronizarse con los servidores NTP.

Wasabi
En el diálogo que se muestra, defina lo siguiente:

- **Nombre de la conexión**: El nombre para la conexión de Wasabi.
- **ID de la clave de acceso**: El ID de clave de acceso del usuario para el servicio de Wasabi.
- **Clave de acceso**: La clave de acceso del usuario para el servicio de Wasabi.
  La clave de acceso y el ID de la clave de acceso permiten acceder a las clases de almacenamiento y los buckets para la conexión relevante. Para obtener más información sobre las claves de acceso y los permisos, consulte "Requisitos de acceso necesarios para hacer una copia de seguridad en el almacenamiento en la nube pública" (p. 748).

© Acronis International GmbH, 2003-2025



Nota
Para acceder al almacenamiento correctamente, la hora del sistema en el agente que realiza las operaciones de copia de seguridad y recuperación con el almacenamiento de Wasabi debe sincronizarse con los servidores NTP.

3. Haga clic en **Conectar**.
   El proceso de conexión comienza y puede tardar varios minutos. Cuando se termina, la conexión se añade a la lista de nubes públicas.
   Para renovar el certificado de acceso anual para la conexión, consulte "Renovación del acceso a una conexión de nube pública" (p. 760).
   Para eliminar el acceso a la conexión, consulte "Eliminación de una conexión a la nube pública" (p. 761).

Renovación del acceso a una conexión de nube pública

Después de que se registre una conexión a la nube pública en la consola de Cyber Protect, Acronis asigna automáticamente un certificado de acceso gratuito y único que permite el acceso a la conexión a la nube pública. El certificado es válido por un año. Cuando el certificado se acerca a su fecha de vencimiento, puede renovarlo.

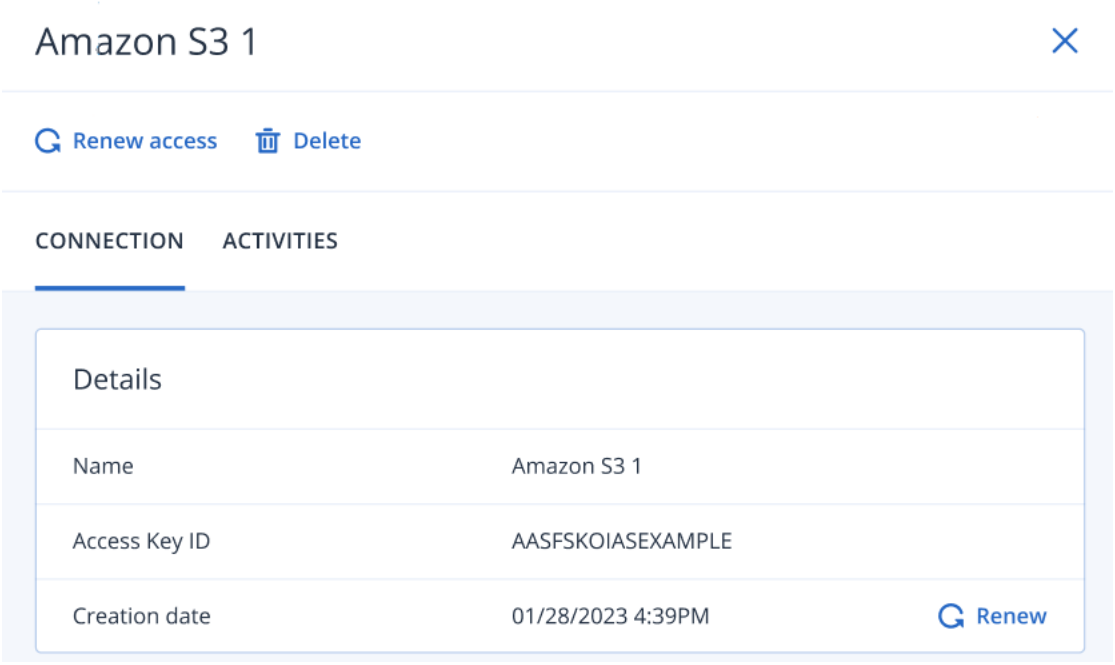
Pasos para renovar el certificado de acceso a su conexión a la nube pública

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la conexión relevante de la lista.

Nota
La columna **Estado de acceso** indica el estado actual del certificado de acceso para cada conexión y muestra uno de dos estados: **OK** o **Caducado**.

© Acronis International GmbH, 2003-2025

3. En el panel derecho, haga clic en **Renovar acceso**.
   De manera alternativa, haga clic en la pestaña **Conexión**, y luego haga clic en **Renovar** en la fila de **Fecha de creación**.



   Si la autenticación es correcta, el acceso se renovará automáticamente durante un año.

Eliminación de una conexión a la nube pública

Debería eliminar la conexión a una nube pública si no está realizando copias de seguridad de cargas de trabajo en ella. La eliminación de la conexión es la única forma de eliminar el acceso a la nube pública.

Nota
De forma predeterminada, solo puede eliminar las conexiones que ha añadido. Para eliminar la conexión de otro usuario a la nube pública, necesita uno de los siguientes roles: administrador de empresa, administrador de unidad, administrador de ciberseguridad o administrador en el servicio de ciberprotección.

Importante
Para eliminar una conexión que se utiliza actualmente para copias de seguridad a una nube pública, primero debe eliminar todas las ubicaciones de copia de seguridad que utilizan esta conexión.

Pasos para eliminar el acceso a una nube pública (eliminar una conexión)

1. En la consola de Cyber Protect, vaya a **Copias de seguridad** > **Almacenamiento de la copia de seguridad**.
2. Elimine todas las ubicaciones de copia de seguridad en nubes públicas que utilizan la conexión que desea eliminar.

© Acronis International GmbH, 2003-2025

Nota
Los objetos en el almacenamiento no se eliminarán. Esta operación solo elimina la ubicación de la lista de ubicaciones de copias de seguridad en la consola de Cyber Protect, sin afectar los datos.

3. Vaya a **Infraestructura** > **Nubes públicas**.
4. Seleccione la conexión de la lista.
5. En el panel derecho, haga clic en **Eliminar**.
6. Haga clic en **Eliminar** en el mensaje de confirmación que se muestra.

Archivado de correos electrónicos

Con el archivado de correos electrónicos, se conservan todos los correos electrónicos de su organización de Microsoft 365 en un archivo comprimido externo que se almacena en la nube, lo que le permite cumplir con las normativas y responder a las solicitudes de eDiscovery. Los nuevos correos electrónicos se agregan al archivo comprimido de forma continua, a medida que se envían o reciben, y no se pueden modificar ni eliminar manualmente.

Los correos electrónicos se muestran en dos carpetas para cada buzón de correo de usuario: **Entrantes** y **Salientes**. En cada carpeta, los correos electrónicos se ordenan cronológicamente, del más reciente al más antiguo.

El archivo está cifrado con el algoritmo AES-256. Solo los usuarios autorizados pueden acceder al archivo de acuerdo con su nivel de acceso y está disponible una pista de auditoría para todas las acciones.

Además de la funcionalidad relacionada con el cumplimiento, el archivado de correos electrónicos proporciona la funcionalidad de copia de seguridad y recuperación.

Puede realizar las siguientes acciones:

- Explorar del archivo comprimido
- Buscar mensajes específicos mediante consultas de búsqueda ad hoc y consultas de búsqueda guardadas
- Obtener una vista previa de correos electrónicos sin recuperarlos
- Recuperar correos electrónicos específicos, las carpetas **Entrantes** y **Salientes** y buzones de correo completos al buzón de correo original o a un buzón de correo no original
- Descarga de adjuntos de correo electrónico

De forma predeterminada, todos los correos electrónicos se conservan en el archivo indefinidamente. Para eliminar los correos electrónicos que ya no necesita, puede aplicar reglas de retención. Cuando finaliza el período de retención, los correos electrónicos se eliminan automáticamente. No puede eliminar manualmente los correos electrónicos del archivo.

© Acronis International GmbH, 2003-2025

Para mantener correos electrónicos específicos en el archivo, independientemente de cualquier regla de retención, puede aplicar reglas de retención legal. Durante el período de retención legal, no se pueden eliminar estos correos electrónicos.

Por ejemplo, puede configurar reglas de retención o reglas de retención legal para correos electrónicos de un remitente específico, correos a un destinatario específico o correos con una palabra concreta en el asunto.

Limitaciones

- El archivo comprimido solo incluye los buzones de correo con licencia. Los buzones de correo compartidos, a los que no se les asigna una licencia, no se incluyen en el archivo comprimido.
- El tamaño máximo de un correo electrónico que puede incluirse en el archivo comprimido es de 150 MB, debido a una limitación de Microsoft.
- Los correos electrónicos en borrador no se incluyen en el archivo comprimido.
- Puede aplicar un plan de archivado a un servidor de correo.

Configuración del archivado de correos electrónicos

Añadir un servidor de correo

Requisitos previos

Las siguientes cuotas deben estar habilitadas para el inquilino en el portal de administración:

- **Licencias de archivado de correo electrónico de Microsoft 365**
- **Almacenamiento de archivos comprimidos**

Nota
Ambas cuotas son obligatorias. Si alguna de ellas se elimina o se configura incorrectamente después de la configuración inicial, el archivado del correo electrónico se pausará para todos los planes del inquilino hasta que se restaure la cuota.

Pasos para añadir un servidor de correo

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** y haga clic en **Agregar** > **Microsoft 365 Business (archivado de correos electrónicos)**.
   Se le redirigirá a la página de inicio de sesión de Microsoft 365.
3. En la página de inicio de sesión de Microsoft, inicie sesión como administrador global.
4. Revise la lista de permisos necesarios y, a continuación, haga clic en **Aceptar**.
   El servidor de correo de Microsoft 365 aparece en la consola de Cyber Protect, en la pestaña **Dispositivos** > **Servidores de correo**.

© Acronis International GmbH, 2003-2025

5. En la pantalla que se abre, configure el plan de archivado como se describe en "Creación de un plan de archivado" (p. 767).

Ver actividades de archivado de correos electrónicos

Puede ver las siguientes actividades de archivado de correos electrónicos:

- Actividades que están relacionadas únicamente con servidores de correo.
- Todas las actividades, incluidas las actividades relacionadas con los servidores de correo y los archivos de correos electrónicos.

Para ver las actividades

Relacionadas con servidores de correo

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** > **Servidores de correo**.
3. En la pantalla principal, haga clic en el nombre del servidor de correo y, a continuación, en la pestaña **Actividades**.

Todas

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Supervisión** > **Actividades**.

Ver alertas de archivado de correos electrónicos

Puede ver las siguientes alertas de archivado de correos electrónicos:

- Alertas que están relacionadas únicamente con servidores de correo.
- Todas las alertas, incluidas las actividades que están relacionadas con los servidores de correo y los archivos de correos electrónicos.

Pasos para ver las alertas

Relacionadas con servidores de correo

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** > **Servidores de correo**.
3. En la pantalla principal, haga clic en el nombre del servidor de correo y, a continuación, en la pestaña **Alertas**.

Todas

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Supervisión** > **Alertas**.

© Acronis International GmbH, 2003-2025

Eliminar un servidor de correo

Puede eliminar un servidor de correo que se agregó a la consola de Cyber Protect.

Pasos para eliminar un servidor de correo

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** > **Servidores de correo**.
3. En la pantalla principal, haga clic en el nombre del servidor de correo y, a continuación, en **Eliminar**.
4. Para confirmar su elección, haga clic en **Eliminar**.

Como resultado, el servidor de correo se quitará de la consola de Cyber Protect. Se conservará el archivo comprimido de correos electrónicos, pero ya no se actualizará.

Descarga de un informe de licencias para el archivado de correos

Puede descargar un informe de licencias para el archivado de correo electrónico a nivel de partner y a nivel de cliente.

En clientes-inquilinos, este informe solo está disponible si se añade un servidor de correo de Microsoft 365.

Para descargar un informe de licencias

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Haga clic en el icono de la cuenta en la esquina superior derecha.
3. Haga clic en **Informe de licencias de archivado de correo electrónico**.
   Se descarga un archivo ZIP en su equipo. El archivo ZIP contiene el informe de licencias en formato CSV.

Archivo comprimido de correo electrónico en inquilinos deshabilitados o eliminados

El archivo comprimido de correo electrónico no está activado en los siguientes tipos de inquilinos:

- Deshabilitado
  Puede volver a habilitar un inquilino deshabilitado.
- Eliminación temporal (durante 30 días desde la eliminación)
  Puede recuperar un inquilino eliminado en un plazo de 30 días desde su eliminación.
- Eliminación permanente (pasados 30 días desde la eliminación)
  No puede recuperar un inquilino si se eliminó hace más de 30 días.

La tabla siguiente resume comportamiento del producto.

© Acronis International GmbH, 2003-2025

Tipo de inquilino		
Deshabilitado o eliminado (eliminación temporal)	**Habilitado nuevamente o recuperado**	**Eliminado (eliminación permanente)**
• Las operaciones de detección no se ejecutan. • Los nuevos correos electrónicos entrantes y salientes no se agregan al archivo comprimido de correo electrónico. • No se aplican las reglas de retención. • No se aplican las reglas de retención legal. • No se ejecutan las operaciones de indexación.	• Las operaciones de detección se ejecutan de nuevo. • Los nuevos correos electrónicos entrantes y salientes se agregan al archivo comprimido de correo electrónico. • Los metadatos de las licencias de Microsoft 365 se han actualizado. Por ejemplo, los cambios en la dirección de correo electrónico de los usuarios. • Los correos electrónicos del período en que el inquilino estaba deshabilitado o eliminado se importan al correo electrónico, de acuerdo con la configuración del plan de archivado. Por ejemplo, correos de todos los buzones de correo o correos de buzones de correo seleccionados. • Se aplican las reglas de retención. • Se aplican las reglas de retención legal. • Las operaciones de indexación se ejecutan de nuevo.	• Se eliminarán permanentemente todos los datos del inquilino, incluidos los archivos comprimidos de correo electrónico. Esta acción es irreversible.

Planes de archivos comprimidos

Con un plan de archivado, puede configurar qué correos electrónicos se importarán al archivo del correo electrónico.

La importación inicial afecta únicamente a los correos electrónicos que estaban en el servidor de correo antes de que se añadiera este servidor a la consola de Cyber Protect.

© Acronis International GmbH, 2003-2025

Después de agregar el servidor de correo a la consola de Cyber Protect, todos los nuevos correos electrónicos se añadirán automáticamente al archivo. No se trata de un ajuste configurable y no depende del ámbito de la importación inicial.

Puede aplicar un plan de archivado a un servidor de correo.

Creación de un plan de archivado

Puede crear un plan de archivado cuando añade un nuevo servidor de correo a la consola de Cyber Protect o crear un plan de archivado para un servidor de correo existente en la consola de Cyber Protect.

Nuevo servidor de correo

Pasos para crear un plan de archivado

1. Añada el servidor de correo a la consola de Cyber Protect, como se describe en "Añadir un servidor de correo" (p. 763).
   Se abre un plan de archivado.
2. [Opcional] Para cambiar el nombre del plan de archivado, haga clic en el icono del lápiz, especifique un nuevo nombre y después haga clic en **Aceptar**.
3. En **Qué importar**, seleccione **Todos los buzones de correo** y, a continuación, haga clic en **Listo**.
4. Haga clic en **Cifrado**, especifique y confirme la contraseña de cifrado y, a continuación, haga clic en **Guardar**.

   Advertencia.
   No hay manera de examinar el archivado de correos y recuperar datos de él si pierde u olvida esta contraseña.

5. Haga clic en **Crear**.

Servidor de correo existente

Prerrequisito

- Ya se ha añadido un servidor de correo a la consola de Cyber Protect, pero no se le ha aplicado ningún plan de archivado.

Pasos para crear un plan de archivado

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** y seleccione el servidor de correo para el que desea crear un plan.
3. Haga clic en el icono de puntos suspensivos (...) y luego en **Proteger**.
4. [Opcional] Para cambiar el nombre del plan de archivado, haga clic en el icono del lápiz, especifique un nuevo nombre y después haga clic en **Aceptar**.
5. En **Qué importar**, seleccione **Todos los buzones de correo** y, a continuación, haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

6. Haga clic en **Cifrado**, especifique y confirme la contraseña de cifrado y, a continuación, haga clic en **Guardar**.

   Advertencia.
   No hay manera de examinar el archivo comprimido y recuperar datos de él si pierde u olvida esta contraseña.

7. Haga clic en **Crear**.

Como resultado, se crea un plan de archivado de correos electrónicos y se aplica al servidor de correo, y se crea el archivo comprimido de correos electrónicos.

La importación inicial llevará algún tiempo, dependiendo del ámbito y el periodo de importación seleccionados. Todos los correos electrónicos nuevos se agregarán continuamente al archivo comprimido, a medida que se envíen o reciban.

Edición de un plan de archivado

Puede editar el nombre de un plan de archivado.

Pasos para editar un plan de archivado

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Planes de archivado de correo electrónico**.
3. Haga clic en el nombre del plan y luego en **Editar**.
4. Para cambiar el nombre del plan, haga clic en el icono del lápiz, especifique un nuevo nombre y, a continuación, haga clic en **Aceptar**.
5. Haga clic en **Guardar**.

Aplicación de un plan de archivado

Puede aplicar un plan de archivado a un servidor de correo.

Nota
Esta operación solo está disponible si aún no ha aplicado un plan de archivado al servidor de correo. Solo puede aplicar un plan de archivado a un servidor de correo.

Pasos para aplicar un plan de archivado

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** > **Servidores de correo**.
3. En la pantalla principal, haga clic en el nombre del servidor de correo y, a continuación, en **Proteger**.
4. Seleccione un plan de archivado y luego haga clic en **Aplicar**.

© Acronis International GmbH, 2003-2025

Como resultado, se aplica el plan de archivado de correos electrónicos al servidor de correo y se crea el archivo comprimido de correo electrónico.

La importación inicial llevará algún tiempo, dependiendo del ámbito y el periodo de importación seleccionados. Todos los correos electrónicos nuevos se agregarán continuamente al archivo comprimido, a medida que se envíen o reciban.

Revocar un plan de archivado

Puede revocar un plan de archivado sin eliminarlo.

Para revocar un plan de archivado

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Dispositivos** > **Servidores de correo**.
3. En la pantalla principal, haga clic en el nombre del servidor de correo.
4. En la pestaña **Proteger**, haga clic en el icono de los puntos suspensivos (...) junto al nombre del plan de archivo y luego en **Revocar**.

Como resultado, el plan ya no se aplicará al servidor de correo y el archivo de correos electrónicos ya no se actualizará.

Eliminación de un plan de archivado

Puede eliminar un plan de archivado.

Pasos para eliminar un plan de archivado

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivado** y haga clic en **Planes de archivado**.
3. En la pantalla principal, haga clic en el nombre del plan y luego en **Eliminar**.
4. Para confirmar su decisión, marque la casilla de verificación y haga clic en **Eliminar**.

Como resultado, se eliminará el plan de archivado. El archivo con los correos electrónicos no se eliminará, pero ya no se actualizará.

Importando correos electrónicos desde archivos PST

Puede utilizar archivos PST para importar correos electrónicos en un archivo comprimido de correos electrónicos.

Durante la importación, los correos electrónicos en el archivo PST son enumerados y se recopilan datos estadísticos sobre sus destinatarios. Los destinatarios más frecuentes se convierten en propietarios de buzones de correo, para quienes se crea un nuevo buzón de correo en **Todos los buzones de correo** > **Importados desde PST** en la consola de Cyber Protect. Los correos electrónicos importados se agrupan por hora de importación y propietario del buzón de correo. Los correos electrónicos que no se pueden asociar con un propietario del buzón de correo y los correos

© Acronis International GmbH, 2003-2025

electrónicos que no tienen campos "De" o "Para" (o están dañados), aparecen en **Importados desde PST** > **Otro**.

Nota
Los correos electrónicos importados no se añaden a los buzones de correo que se están archivando. Un buzón de correo que se está archivando aparece en **Todos los buzones de correo**. Los correos electrónicos importados se muestran en buzones de correo separados en **Todos los buzones de correo** > **Importados desde PST**.

Limitaciones

- En una tarea de importación, puede seleccionar archivos PST de una única cuenta personal de OneDrive.
  No se admite la importación desde una cuenta de SharePoint o de Grupo de OneDrive.
- El tiempo de importación depende de la velocidad de descarga permitida por OneDrive y puede variar considerablemente en diferentes ubicaciones y horas del día.
- Puede seleccionar hasta 100 000 archivos PST o una carpeta que contenga archivos PST.
  La carpeta seleccionada puede contener hasta 10 000 subcarpetas y hasta 100 000 archivos PST.
- El tamaño máximo permitido por archivo PST es de 50 GB.
  Si selecciona una carpeta, se omitirán los archivos PST de más de 50 GB.
- Solo se importan correos electrónicos de hasta 200 MB.
  Se omiten correos electrónicos, tareas, notas, invitaciones y otros elementos que ocupen más.
- Los archivos PST en unicode son totalmente compatibles. Es posible que no se procesen los archivos PST en ANSI o que se procesen incorrectamente.
- No se admite la deduplicación.
  Si utiliza el mismo archivo PST dos veces, los correos electrónicos importados se duplicarán.
- No se puede conservar el formato de texto enriquecido (RTF) en el cuerpo de un correo electrónico importado.
  Se conserva el cuerpo de texto sin formato o html de un correo electrónico con formato RTF. El cuerpo con formato RFT se adjunta al correo electrónico importado como un archivo `body.rtf` separado.
- Los archivos adjuntos OLE en línea se importan como archivos adjuntos de imagen con nombres asignados automáticamente y sin extensiones de archivo.
- No se requiere ninguna contraseña al importar archivos PST protegidos con contraseña creados en Microsoft Outlook.
- Los correos electrónicos que se importan desde archivos PST solo se pueden recuperar en nuevos destinos.

Para importar correos electrónicos desde archivos PST

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones en la nube** y seleccione el archivo comprimido en el que desee importar los correos electrónicos.

© Acronis International GmbH, 2003-2025

3. Haga clic en **Importar desde archivos PST**.
4. Indique la contraseña de cifrado para el archivo comprimido y luego haga clic en **Continuar**.
5. En **Organización**, seleccione la organización de Microsoft 365 de origen.
   - Si se añade una única organización de Microsoft 365 a la consola de Cyber Protect, esta organización se preselecciona. Puede utilizar esta organización como origen o añadir una nueva.
   - [Si se añaden varias organizaciones de Microsoft 365 a la consola de Cyber Protect] Haga lo siguiente:
     - Haga clic en **Seleccionar** y, a continuación, seleccione la organización de Microsoft 365 de origen.
     - Haga clic en **Seleccionar**.
   - [Si no se ha añadido ninguna organización de Microsoft 365 a la consola de Cyber Protect] Haga lo siguiente:
     - Haga clic en **Seleccionar** y, a continuación, en **Añadir organización**.
     - En la página de inicio de sesión de Microsoft 365, acceda con las credenciales de administrador global de Microsoft 365.

       Microsoft 365 muestra una lista con aquellos permisos que son necesarios para realizar copias de seguridad de los datos de su organización, además de recuperarlos.
     - Confirme que concede los permisos requeridos.
6. En **Qué importar**, seleccione uno o más archivos PST o carpetas que contengan archivos PST.
   - Haga clic en **Seleccionar**.
   - En la página de inicio de sesión de Microsoft 365, inicie sesión con las credenciales de administrador global de la organización de Microsoft 365 de origen.

     Microsoft 365 muestra una lista adicional de permisos.
   - Confirme que concede los permisos requeridos.
   - En la consola de Cyber Protect, navegue hasta el OneDrive de un usuario y, a continuación, seleccione uno o más archivos PST.
   - Haga clic en **Seleccionar**.
7. Haga clic en **Importar**.
8. Después de que se complete la operación de importación, compruebe su resultado.

   Después de una correcta importación, los correos electrónicos importados se muestran en **Todos los buzones de correo** > **Importados desde PST**.

   Después de una incorrecta importación, no se muestran correos electrónicos importados. Una importación fallida no se reanudará ni reiniciará automáticamente.

Consultas de búsqueda

Puede buscar correos electrónicos específicos en el archivo mediante consultas de búsqueda y, a continuación, guardar las consultas para su uso futuro.

Las consultas de búsqueda son la base para crear reglas de retención y reglas de retención legal.

© Acronis International GmbH, 2003-2025

Puede vincular una consulta de búsqueda guardada a un archivo de correos concreto. Esta consulta de búsqueda solo se puede ejecutar en el archivo de correos vinculado.

Si no vincula la consulta de búsqueda guardada a un archivo de correos, puede ejecutarse en cualquier archivo de correos. Puede utilizar consultas de búsqueda no vinculadas en reglas de retención y reglas de retención legal que se aplican a varios archivos de correos.

Búsqueda de correos electrónicos

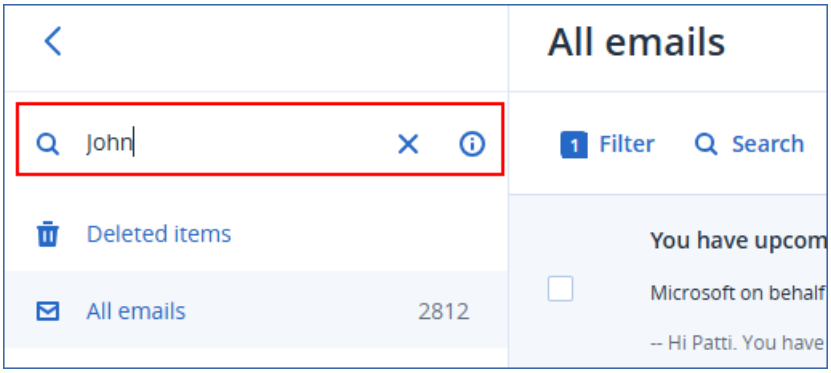
Puede buscar correos electrónicos específicos mediante consultas de búsqueda de texto completo en los siguientes niveles:

- El archivo comprimido de correos electrónicos (**Todos los correos electrónicos**)
- Un buzón de correo de usuario
- La carpeta **Entrantes** o **Salientes** en un buzón de correo de usuario

Pasos para buscar correos electrónicos

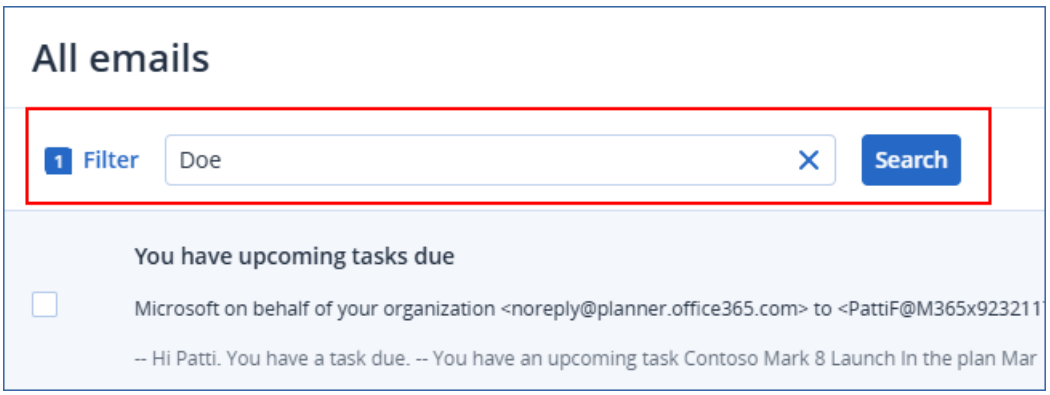
1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** > **Copias de seguridad de aplicaciones en la nube**.
3. [Si desea buscar en un archivo de correos en almacenamiento inmutable] Haga clic en **Mostrar elementos eliminados**.
4. Seleccione un archivo de correos y, a continuación, haga clic en **Examinar el archivo**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
7. Seleccione el nivel en el que desea llevar a cabo la búsqueda.

   Puede seleccionar **Todos los correos electrónicos**, un buzón de correo de usuario o la carpeta **Entrantes** o **Salientes** en un buzón de correo de usuario.
8. [Opcional] Para buscar el buzón de correo de un usuario específico, en el campo de búsqueda de la columna izquierda, escriba al menos tres caracteres del nombre del usuario y, a continuación, haga clic **Intro**.



© Acronis International GmbH, 2003-2025

9. En la pantalla principal, haga clic en **Buscar**, especifique su consulta de búsqueda y, a continuación, haga clic en **Buscar**.



   Puede utilizar una o varias palabras. Para buscar una frase específica, coloque la frase entre comillas. Los comodines no son compatibles.

   La búsqueda se realiza en los siguientes campos:

   - Desde
   - Para
   - CC
   - CCO
   - Asunto
   - Cuerpo del correo electrónico

10. [Opcional] Para buscar solo en un campo específico, como **De**, **Para/CC/Cco**, **El asunto contiene**, o para especificar otros criterios de búsqueda, haga clic en **Filtro**.
    a. Configure sus criterios de búsqueda.

       Por ejemplo, puede buscar solo correos electrónicos que tengan archivos adjuntos o correos electrónicos que se hayan enviado o recibido en una fecha específica.
    b. En **Estado de eliminación**, seleccione el ámbito de búsqueda.

       Al seleccionar **Elementos no eliminados**, la búsqueda se limita únicamente a los correos electrónicos que no están en almacenamiento inmutable.

       Al seleccionar **Elementos eliminados**, la búsqueda se limita únicamente a los correos electrónicos que están en almacenamiento inmutable.
    c. Haga clic en **Aplicar**.

Como resultado, solo se enumeran los correos electrónicos que coinciden con la consulta de búsqueda.

Puede guardar la consulta de búsqueda para usarla más adelante. Para obtener más información, consulte "Creación de una consulta de búsqueda guardada" (p. 774).

© Acronis International GmbH, 2003-2025

Creación de una consulta de búsqueda guardada

Puede crear una consulta de búsqueda guardada desde el archivo de correos electrónicos o desde la pestaña **Gestión** > **Planes de archivos comprimidos**.

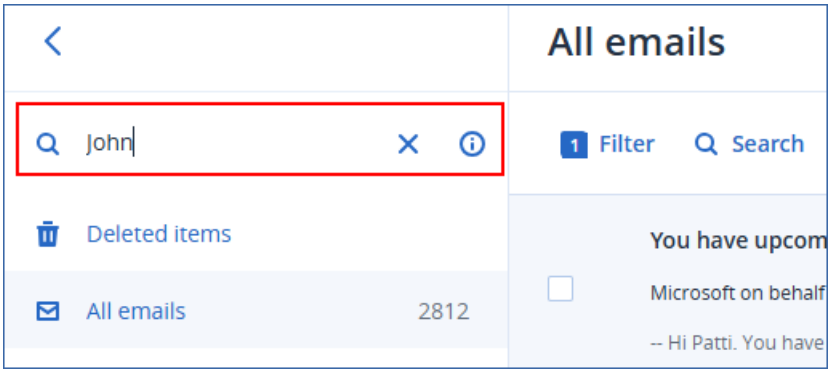
Puede utilizar una consulta de búsqueda guardada en las reglas de retención o las reglas de retención legal, o ejecutarla en el archivo de correos para encontrar los correos electrónicos que desee previsualizar o recuperar.

Pasos para crear una consulta de búsqueda guardada

Desde el archivo de correos electrónicos

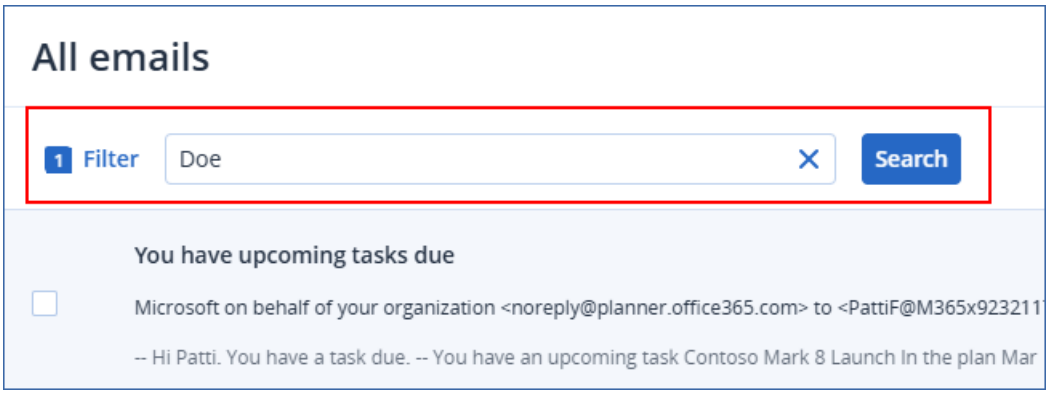
1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** > **Copias de seguridad de aplicaciones en la nube**.
3. [Si desea buscar en un archivo de correos en almacenamiento inmutable] Haga clic en **Mostrar elementos eliminados**.
4. Seleccione un archivo de correos y, a continuación, haga clic en **Examinar el archivo**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
7. Seleccione el nivel en el que desea llevar a cabo la búsqueda.

   Puede seleccionar **Todos los correos electrónicos**, un buzón de correo de usuario o la carpeta **Entrantes** o **Salientes** en un buzón de correo de usuario.
8. [Opcional] Para buscar el buzón de correo de un usuario específico, en el campo de búsqueda de la columna izquierda, escriba al menos tres caracteres del nombre del usuario y, a continuación, haga clic **Intro**.



9. En la pantalla principal, haga clic en **Buscar**, especifique su consulta de búsqueda y, a continuación, haga clic en **Buscar**.

© Acronis International GmbH, 2003-2025



Puede utilizar una o varias palabras. Para buscar una frase específica, coloque la frase entre comillas. Los comodines no son compatibles.

La búsqueda se realiza en los siguientes campos:

- Desde
- Para
- CC
- CCO
- Asunto
- Cuerpo del correo electrónico

10. [Opcional] Para buscar solo en un campo específico, como **De**, **Para/CC/Cco**, **El asunto contiene**, o para especificar otros criterios de búsqueda, haga clic en **Filtro**.
    a. Configure sus criterios de búsqueda.

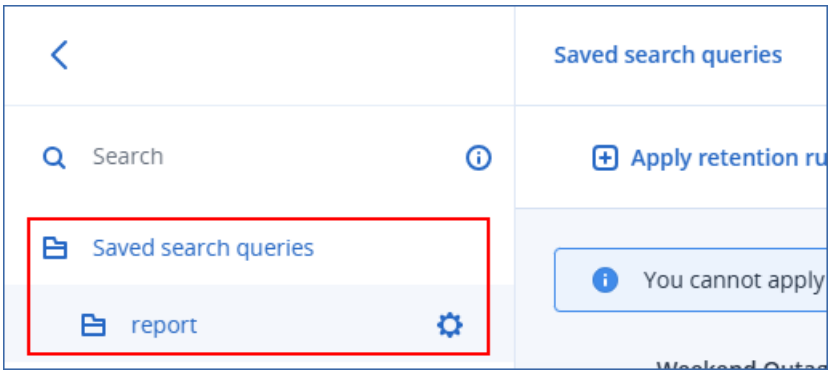
       Por ejemplo, puede buscar solo correos electrónicos que tengan archivos adjuntos o correos electrónicos que se hayan enviado o recibido en una fecha específica.
    b. En **Estado de eliminación**, seleccione el ámbito de búsqueda.

       Al seleccionar **Elementos no eliminados**, la búsqueda se limita únicamente a los correos electrónicos que no están en almacenamiento inmutable.

       Al seleccionar **Elementos eliminados**, la búsqueda se limita únicamente a los correos electrónicos que están en almacenamiento inmutable.
    c. Haga clic en **Aplicar**.
11. Haga clic en **Guardar como**.
12. En **Nombre de la consulta de búsqueda**, especifique un nombre.
13. Haga clic en **Guardar**.

Como resultado, se crea una consulta de búsqueda guardada que se muestra en la sección **Consultas de búsqueda guardadas**. Los resultados de la búsqueda son dinámicos e incluyen todos los nuevos correos electrónicos que coincidan con la consulta.

© Acronis International GmbH, 2003-2025



La consulta de búsqueda está vinculada a este archivo de correos y solo se puede ejecutar en él. No utilice esta consulta de búsqueda en una regla de retención o regla de retención legal que desee aplicar a otro archivo de correos electrónicos.

Desde Gestión > Planes de archivos comprimidos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Consultas de búsqueda** y, a continuación, haga clic en **Añadir consulta de búsqueda**.
3. En **Nombre de la consulta de búsqueda**, especifique un nombre.
4. [Opcional] Seleccione un archivo de correos electrónicos al que desee vincular la consulta de búsqueda.

   Si selecciona un archivo de correos, solo podrá ejecutar la consulta en ese archivo.

   Si no selecciona un archivo de correos, podrá aplicar la consulta en cualquier archivo de correos.
5. En **Consulta de búsqueda**, especifique su consulta de búsqueda.

   Puede utilizar una o varias palabras. Para buscar una frase específica, coloque la frase entre comillas. Los comodines no son compatibles.

   La búsqueda se realiza en los siguientes campos:

   - Desde
   - Para
   - CC
   - CCO
   - Asunto

   También puede buscar en estos campos por separado, utilizando los campos **De**, **Para/CC/CCo** y **El asunto contiene**.
6. En **Estado de eliminación**, seleccione el ámbito de búsqueda.

   Al seleccionar **Elementos no eliminados**, la búsqueda se limita únicamente a los correos electrónicos que no están en almacenamiento inmutable.

   Al seleccionar **Elementos eliminados**, la búsqueda se limita únicamente a los correos electrónicos que están en almacenamiento inmutable.
7. [Opcional] Especifique otros criterios de búsqueda.

© Acronis International GmbH, 2003-2025

Por ejemplo, puede buscar solo los correos electrónicos que tienen archivos adjuntos, los correos electrónicos que se enviaron o recibieron en una fecha específica o los correos electrónicos con un tamaño determinado.

8. Haga clic en **Crear**.

Como resultado, se crea una nueva consulta de búsqueda guardada. Los resultados de la búsqueda son dinámicos e incluyen todos los nuevos correos electrónicos que coincidan con la consulta.

Ejecutar una consulta de búsqueda guardada

Puede ejecutar una consulta de búsqueda guardada desde un archivo de correos electrónicos o desde la pestaña **Gestión** > **Planes de archivos comprimidos**.

Para ejecutar una consulta de búsqueda guardada

Desde el archivo de correos electrónicos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** > **Copias de seguridad de aplicaciones en la nube**.
3. [Si desea buscar un archivo en almacenamiento inmutable] Haga clic en **Mostrar elementos eliminados**.
4. Seleccione un archivo de correos y, a continuación, haga clic en **Examinar el archivo**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
7. En **Consultas de búsqueda guardadas**, seleccione la consulta que desee ejecutar.

Como resultado, se enumeran los correos electrónicos que coinciden con la consulta de búsqueda.

Desde Gestión > Planes de archivos comprimidos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidoso** > **Consultas de búsqueda**.
3. Haga clic en una consulta de búsqueda y después en **Buscar**.
4. [Si la consulta de búsqueda no está vinculada a un archivo de correos] Seleccione un archivo de correos y, a continuación, haga clic en **Buscar**.
5. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.

Como resultado, se enumeran los correos electrónicos que coinciden con la consulta de búsqueda.

Edición de una consulta de búsqueda guardada

Puede editar una consulta de búsqueda guardada desde el archivo de correos electrónicos o desde la pestaña **Gestión** > **Planes de archivos comprimidos**.

Pasos para editar una consulta de búsqueda

© Acronis International GmbH, 2003-2025

Desde el archivo de correos electrónicos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** > **Copias de seguridad de aplicaciones en la nube**.
3. [Si desea buscar un archivo en almacenamiento inmutable] Haga clic en **Mostrar elementos eliminados**.
4. Seleccione un archivo de correos y, a continuación, haga clic en **Examinar el archivo**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
7. En **Consultas de búsqueda guardadas**, haga clic en el icono de engranaje junto a la consulta y haga clic en **Editar**.
8. Edite la consulta de búsqueda y haga clic en **Guardar**.

Advertencia.
La edición de una consulta de búsqueda afecta a las reglas de retención y a las reglas de retención legal en las que se utiliza esa consulta de búsqueda.

Desde Gestión > Planes de archivos comprimidos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidoso** > **Consultas de búsqueda**.
3. Haga clic en una consulta de búsqueda y, a continuación, en **Editar**.
4. Edite la consulta de búsqueda y haga clic en **Guardar**.

Advertencia.
La edición de una consulta de búsqueda afecta a las reglas de retención y a las reglas de retención legal en las que se utiliza esa consulta de búsqueda.

Eliminación de una consulta de búsqueda guardada

Puede eliminar una consulta de búsqueda guardada desde el archivo de correos electrónicos o desde la pestaña **Gestión** > **Planes de archivos comprimidos**.

Pasos para eliminar una consulta de búsqueda

Desde el archivo de correos electrónicos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** > **Copias de seguridad de aplicaciones en la nube**.
3. [Si desea buscar un archivo en almacenamiento inmutable] Haga clic en **Mostrar elementos eliminados**.

© Acronis International GmbH, 2003-2025

4. Seleccione un archivo de correos y, a continuación, haga clic en **Examinar el archivo**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
7. En **Consultas de búsqueda guardadas**, haga clic en el icono de engranaje junto a la consulta y luego en **Eliminar**.
8. Para confirmar su elección, haga clic en **Eliminar**.

Advertencia.
Eliminar una consulta de búsqueda afecta a las reglas de retención y a las reglas de retención legal en las que se utiliza esa consulta de búsqueda.

Desde Gestión > Planes de archivos comprimidos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidoso** > **Consultas de búsqueda**.
3. Haga clic en una consulta de búsqueda y luego en **Eliminar**.
4. Para confirmar su elección, haga clic en **Eliminar**.

Advertencia.
Eliminar una consulta de búsqueda afecta a las reglas de retención y a las reglas de retención legal en las que se utiliza esa consulta de búsqueda.

Normas de retención

Con las reglas de retención, puede configurar cuánto tiempo se conservarán los correos electrónicos en el archivo de correos.

Las reglas de retención se basan en las consultas de búsqueda. Los correos electrónicos que coincidan con las consultas de búsqueda se conservan en el archivo de correos durante el período de retención establecido. Una vez finalizado el período de retención, los correos electrónicos se eliminan automáticamente. No puede eliminar manualmente los correos electrónicos del archivo de correos electrónicos.

Puede utilizar una o más consultas de búsqueda en una regla de retención. Los correos electrónicos que coincidan con cualquiera de las consultas de búsqueda seguirán esa regla de retención.

Puede aplicar varias reglas de retención a un mismo archivo.

Nota
Si un correo electrónico coincide con más de una regla de retención, se aplica la regla con el período de retención más largo.

© Acronis International GmbH, 2003-2025

Puede aplicar una regla de retención a uno o más archivos de correos. Al crear una regla de retención que desea aplicar a varios archivos de correos, use consultas de búsqueda guardadas que no estén vinculadas a un archivo de correos específico.

Las reglas de retención se ejecutan en sus archivos de correo electrónico una vez cada 24 horas. Esta operación no se puede configurar por el usuario.

Creación de una regla de retención

Puede crear una regla de retención desde el archivo de correos electrónicos o desde la pestaña **Gestión** > **Planes de archivos comprimidos**.

Las reglas de retención que se crean a partir del archivo de correos electrónicos solo pueden utilizar una consulta de búsqueda y un archivo de correos.

Las reglas de retención que se crean desde la pestaña **Gestión** > **Planes de archivos comprimidos** pueden usar múltiples consultas de búsqueda y múltiples archivos de correos.

Para crear una regla de retención

Desde el archivo de correos electrónicos

1. Ejecute una consulta de búsqueda en el archivo de correos, como se describe en "Ejecutar una consulta de búsqueda guardada" (p. 777).
2. Encima de la lista de correos electrónicos coincidentes, haga clic en **Aplicar regla de retención**.
3. [Si hay reglas de retención existentes] En la ventana **Aplicar regla de retención a la consulta de búsqueda**, haga clic en **Añadir regla de retención**.
4. [Opcional] Para cambiar el nombre del plan de archivado, haga clic en el icono del lápiz, especifique un nuevo nombre y después haga clic en **Aceptar**.
5. En **Período de retención**, seleccione una opción.
   a. [Si selecciona **Por antigüedad del correo electrónico**] Especifique el período de tiempo y seleccione la unidad de tiempo.
   b. Haga clic en **Guardar**.

   Por ejemplo, puede especificar 1 año, 2 meses, o 300 días. Los correos electrónicos que sean más antiguos que el período seleccionado se eliminarán del archivo. La antigüedad del correo electrónico se calcula en función de cuándo se envió o recibió cada correo electrónico.
6. En **Contraseña de cifrado de archivos**, especifique la contraseña de cifrado para el archivado de correos electrónicos y, a continuación, haga clic en **Continuar**.
7. Haga clic en **Crear**.

   Como resultado, se crea una regla de retención.

   Los correos electrónicos que coincidan con cualquiera de las consultas de búsqueda de esta regla de retención se eliminarán cuando finalice el período de retención.

Nota
Si un correo electrónico coincide con más de una regla de retención, se aplica la regla con el período de retención más largo.

© Acronis International GmbH, 2003-2025

Desde Gestión > Planes de archivos comprimidos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención** y haga clic en **Añadir regla de retención**.
3. [Opcional] Para cambiar el nombre del plan de archivado, haga clic en el icono del lápiz, especifique un nuevo nombre y después haga clic en **Aceptar**.
4. En **Archivos comprimidos de correo electrónico**, seleccione los archivos de correos electrónicos a los que se aplicarán las reglas de retención.
   a. Haga clic en **Seleccionar**.
   b. Seleccione uno o más archivos de correos.
   c. Haga clic en **Seleccionar**.
5. En **Período de retención**, seleccione una opción.
   a. [Si selecciona **Por antigüedad del correo electrónico**] Especifique el período de tiempo y seleccione la unidad de tiempo.
   b. Haga clic en **Guardar**.

   Por ejemplo, puede especificar 1 año, 2 meses, o 300 días. Los correos electrónicos que sean más antiguos que el período seleccionado se eliminarán del archivo. La antigüedad del correo electrónico se calcula en función de cuándo se envió o recibió cada correo electrónico.
6. En **Consultas de búsqueda guardadas**, seleccione las consultas de búsqueda en las que se basará esta regla de retención.
   a. Haga clic en **Seleccionar**.
   b. [Para crear una nueva consulta de búsqueda] Haga clic en **Añadir consulta de búsqueda** y, a continuación, cree la consulta como se describe en "Creación de una consulta de búsqueda guardada" (p. 774).
   c. Seleccione una o más consultas de búsqueda.

      Nota
      Al crear una regla de retención que desee aplicar a varios archivos de correos electrónicos, utilice consultas de búsqueda guardadas que no estén ya vinculadas a un archivo de correos específico.

   d. Haga clic en **Seleccionar**.
7. En **Contraseña de cifrado de archivos**, especifique la contraseña de cifrado para los archivos de correos electrónicos seleccionados y, a continuación, haga clic en **Continuar**.
8. Haga clic en **Crear**.

Como resultado, se crea una regla de retención.

Los correos electrónicos que coincidan con cualquiera de las consultas de búsqueda de esta regla de retención se eliminarán cuando finalice el período de retención.

© Acronis International GmbH, 2003-2025

Nota
Si un correo electrónico coincide con más de una regla de retención, se aplica la regla con el período de retención más largo.

Edición de una regla de retención

Puede editar una regla de retención.

Para editar una regla de retención

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención**.
3. Seleccione una regla de retención y haga clic en **Editar**.
4. Edite la regla de retención y haga clic en **Guardar**.

Como resultado, se edita la regla de retención. La configuración actualizada se aplicará al archivado de correo electrónico la próxima vez que se ejecute la regla de retención.

Las reglas de retención se ejecutan en sus archivos de correo electrónico una vez cada 24 horas. Esta operación no se puede configurar por el usuario.

Activar una regla de retención

Una regla de retención se activa automáticamente cuando la crea.

Puede activar manualmente una regla de retención que haya desactivado anteriormente.

Para activar una regla de retención

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención**.
3. Marque la casilla de verificación junto al nombre de una regla de retención deshabilitada y, a continuación, haga clic en **Habilitar**.
4. Para confirmar su elección, haga clic en **Habilitar**.

Como resultado, la regla de retención se activa y se aplicará al archivo de correos electrónicos la próxima vez que se ejecute.

Las reglas de retención se ejecutan en sus archivos de correo electrónico una vez cada 24 horas. Esta operación no se puede configurar por el usuario.

Deshabilitar una regla de retención

Una regla de retención deshabilitada no se aplica al archivado de correo electrónico. La regla de retención deshabilitada no se elimina y puede habilitarla más tarde.

Para deshabilitar una regla de retención

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención**.
3. Marque la casilla de verificación junto al nombre de una regla de retención y, a continuación, haga clic en **Deshabilitar**.
4. Para confirmar su elección, haga clic en **Deshabilitar**.

Como resultado, la regla de retención ya no se aplicará al archivado de correo electrónico.

Eliminación de una regla de retención

Puede eliminar una regla de retención.

Para eliminar una regla de retención

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención**.
3. Seleccione una regla de retención y luego haga clic en **Eliminar**.
4. Para confirmar su elección, marque la casilla de verificación y luego haga clic en **Eliminar**.

Como resultado, la regla de retención se elimina y ya no se aplicará al archivado de correo electrónico.

Reglas de retención legales

Con las reglas de retención legal, puede invalidar las reglas de retención y evitar que se eliminen los correos electrónicos.

Las reglas de retención legal se basan en las consultas de búsqueda. Los correos electrónicos que coincidan con las consultas de búsqueda están protegidos contra la eliminación durante el período de retención legal. Una vez finalizado el período de retención legal, estos correos electrónicos pueden eliminarse mediante una regla de retención.

Puede utilizar una o más consultas de búsqueda en una regla de retención legal. Los correos electrónicos que coincidan con cualquiera de las consultas de búsqueda seguirán esa regla de retención legal.

Puede aplicar varias reglas de retención legal al mismo archivo.

Nota
Si un correo electrónico coincide con más de una regla de retención legal, se aplica la regla con el período de retención legal más largo.

Puede aplicar una regla de retención legal a uno o más archivos de correos electrónicos. Al crear una regla de retención legal que desee aplicar a varios archivos de correos, utilice consultas de búsqueda guardadas que no estén vinculadas a un archivo de correos específico.

© Acronis International GmbH, 2003-2025

Las reglas de retención legal se ejecutan una vez cada 24 horas. Esta operación no se puede configurar por el usuario.

Creación de una regla de retención legal

Puede crear una regla de retención legal desde el archivo de correos electrónicos o desde la pestaña **Gestión** > **Planes de archivos comprimidos**.

Las reglas de retención legal que se crean a partir del archivo de correos electrónicos solo pueden usar una consulta de búsqueda y un archivo de correos electrónicos.

Las reglas de retención legal que se crean desde la pestaña **Gestión** > **Planes de archivos comprimidos** pueden utilizar múltiples consultas de búsqueda y múltiples archivos de correos electrónicos.

Para crear una regla de retención legal

Desde el archivo de correos electrónicos

1. Ejecute una consulta de búsqueda en el archivo de correos, como se describe en "Ejecutar una consulta de búsqueda guardada" (p. 777).
2. Encima de la lista de correos electrónicos coincidentes, haga clic en **Aplicar regla de retención legal**.
3. [Si hay reglas de retención legal existentes] En la ventana **Aplicar regla de retención legal a la consulta de búsqueda**, haga clic en **Añadir regla de retención legal**.
4. [Opcional] Para cambiar el nombre de la regla de retención legal, haga clic en el icono del lápiz, especifique un nuevo nombre y después haga clic en **Aceptar**.
5. En **Período de retención legal**, seleccione una opción.
   a. [Si selecciona **Fecha de retención**] Seleccione una fecha.
   b. Haga clic en **Guardar**.

   Los correos electrónicos que coincidan con esta regla de retención legal estarán protegidos contra la eliminación hasta esta fecha, inclusive.
6. En **Contraseña de cifrado de archivos**, especifique la contraseña de cifrado para el archivado de correos electrónicos y, a continuación, haga clic en **Continuar**.
7. Haga clic en **Crear**.

   Como resultado, se crea una regla de retención legal.

   Los correos electrónicos que coincidan con cualquiera de las consultas de búsqueda en esta regla de retención legal estarán protegidos contra la eliminación hasta que finalice el período de retención legal.

   Nota
   Si un correo electrónico coincide con más de una regla de retención legal, se aplica la regla con el período de retención legal más largo.

Desde Gestión > Planes de archivos comprimidos

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención legal** y haga clic en **Añadir regla de retención legal**.
3. [Opcional] Para cambiar el nombre de la regla de retención legal, haga clic en el icono del lápiz, especifique un nuevo nombre y después haga clic en **Aceptar**.
4. En **Archivos comprimidos de correo electrónico**, seleccione los archivos de correos electrónicos a los que se aplicarán las reglas de retención.
   a. Haga clic en **Seleccionar**.
   b. Seleccione uno o más archivos de correos.
   c. Haga clic en **Seleccionar**.
5. En **Período de retención legal**, seleccione una opción.
   a. [Si selecciona **Fecha de retención**] Seleccione una fecha.
   b. Haga clic en **Guardar**.

   Los correos electrónicos que coincidan con esta regla de retención legal estarán protegidos contra la eliminación hasta esta fecha, inclusive.
6. En **Consultas de búsqueda guardadas**, seleccione las consultas de búsqueda en las que se basará esta regla de retención.
   a. Haga clic en **Seleccionar**.
   b. [Para crear una nueva consulta de búsqueda] Haga clic en **Añadir consulta de búsqueda** y, a continuación, cree la consulta como se describe en "Creación de una consulta de búsqueda guardada" (p. 774).
   c. Seleccione una o más consultas de búsqueda.

      Nota
      Al crear una regla de retención legal que desee aplicar a varios archivos de correos electrónicos, utilice consultas de búsqueda que no estén ya vinculadas a un archivo de correos específico.

   d. Haga clic en **Seleccionar**.
7. En **Contraseña de cifrado de archivos**, especifique la contraseña de cifrado para los archivos de correos electrónicos seleccionados y, a continuación, haga clic en **Continuar**.
8. Haga clic en **Crear**.

Como resultado, se crea una regla de retención legal.

Los correos electrónicos que coincidan con cualquiera de las consultas de búsqueda en esta regla de retención legal estarán protegidos contra la eliminación hasta que finalice el período de retención legal.

© Acronis International GmbH, 2003-2025

Nota
Si un correo electrónico coincide con más de una regla de retención legal, se aplica la regla con el período de retención legal más largo.

Edición de una regla de retención legal

Puede editar una regla de retención legal.

Para editar una regla de retención legal

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención legal**.
3. Seleccione una regla de retención legal y, a continuación, haga clic en **Editar**.
4. Edite la regla de retención legal y luego haga clic en **Guardar**.

Como resultado, se edita la regla de retención legal. La configuración actualizada se aplicará al archivado de correo electrónico la próxima vez que se ejecute la regla de retención legal.

Las reglas de retención legal se ejecutan una vez cada 24 horas. Esta operación no se puede configurar por el usuario.

Activar una regla de retención legal

Una regla de retención legal se activa automáticamente cuando la crea.

Puede activar manualmente una regla de retención legal que haya desactivado anteriormente.

Para activar una regla de retención legal

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención legal**.
3. Marque la casilla de verificación junto al nombre de una regla de retención legal deshabilitada y, a continuación, haga clic en **Habilitar**.
4. Para confirmar su elección, haga clic en **Habilitar**.

Como resultado, la regla de retención legal se habilita y se aplicará al archivo de correos electrónicos la próxima vez que se ejecute.

Las reglas de retención legal se ejecutan una vez cada 24 horas. Esta operación no se puede configurar por el usuario.

Deshabilitar una regla de retención legal

No se aplica una regla de retención legal deshabilitada al archivado de correo electrónico. La regla de retención legal deshabilitada no se elimina y puede habilitarla más adelante.

Para deshabilitar una regla de retención legal

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención legal**.
3. Marque la casilla de verificación junto al nombre de una regla de retención legal y, a continuación, haga clic en **Deshabilitar**.
4. Para confirmar su elección, haga clic en **Deshabilitar**.

Como resultado, la regla de retención legal ya no se aplicará al archivado de correo electrónico.

Eliminación de una regla de retención legal

Puede eliminar una regla de retención legal.

Para eliminar una regla de retención legal

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Gestión** > **Planes de archivos comprimidos** > **Reglas de retención legal**.
3. Seleccione una regla de retención legal y, a continuación, haga clic en **Eliminar**.
4. Para confirmar su elección, marque la casilla de verificación y luego haga clic en **Eliminar**.

Como resultado, la regla de retención legal se elimina y ya no se aplicará al archivado de correo electrónico.

Recuperación de datos de un archivo comprimido de correos electrónicos

Vista previa de correos electrónicos

Puede obtener una vista previa de los correos electrónicos archivados sin recuperarlos primero.

Pasos para obtener una vista previa de los correos electrónicos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones en la nube** y seleccione el archivo comprimido de correo electrónico que desea buscar.
3. Haga clic en **Examinar archivo comprimido**.
4. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
5. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
6. Busque los correos electrónicos que desee previsualizar.
   Puede utilizar consultas de búsqueda ad hoc y consultas de búsqueda guardadas. Para obtener más información, consulte "Búsqueda de correos electrónicos" (p. 772).
7. Seleccione el correo electrónico que desee previsualizar.

Como resultado, se muestra el correo electrónico y puede comprobar su contenido y metadatos.

© Acronis International GmbH, 2003-2025

Recuperación de correos electrónicos, carpetas y buzones de correo

Puede recuperar correos electrónicos, carpetas y buzones de correo al buzón de correo original o a un buzón de correo no original.

Correos electrónicos

Pasos para recuperar correos electrónicos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones de la nube** y seleccione el archivo comprimido de correos electrónicos del que desea recuperar los datos.
3. Haga clic en **Examinar archivo comprimido**.
4. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
5. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
6. [Opcional] Busque los correos electrónicos que desea recuperar.
   Puede utilizar consultas de búsqueda ad hoc y consultas de búsqueda guardadas. Para obtener más información, consulte "Búsqueda de correos electrónicos" (p. 772).
7. Seleccione los elementos que desea recuperar y, a continuación, haga clic en **Recuperar correos electrónicos**.
8. [Si se han añadido varios servidores de correo a la consola de Cyber Protect] Seleccione la organización en la que desea recuperar los datos.
   a. En **Organización**, haga clic en **Seleccionar**.
   b. Seleccione la organización y haga clic en **Seleccionar**.
9. En **Ubicación de recuperación**, seleccione la ubicación en la que desea recuperar los correos electrónicos.
10. [Si seleccionó **Nueva ubicación**] Seleccione el buzón de correo de destino.
    a. En **Recuperar a**, haga clic en **Seleccionar**.
    b. Seleccione el buzón de correo de destino y haga clic en **Seleccionar**.
11. Haga clic en **Iniciar recuperación**.

Como resultado, los correos electrónicos entrantes del buzón de correo seleccionado se recuperan en la carpeta **Bandeja de entrada** del buzón de correo de destino, y los correos electrónicos salientes del buzón de correo seleccionado se recuperan en la carpeta **Enviados** del buzón de correo de destino.

Carpetas

Pasos para recuperar una carpeta

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones de la nube** y seleccione el archivo comprimido de correos electrónicos del que desea recuperar los datos.
3. Haga clic en **Examinar archivo comprimido**.
4. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
5. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
6. Seleccione la carpeta **Entrantes** o **Salientes** que desea recuperar y haga clic en **Recuperar carpeta**.
7. [Si se han añadido varios servidores de correo a la consola de Cyber Protect] Seleccione la organización en la que desea recuperar los datos.
   a. En **Organización**, haga clic en **Seleccionar**.
   b. Seleccione la organización y haga clic en **Seleccionar**.
8. En **Ubicación de recuperación**, seleccione la ubicación en la que desea recuperar los datos.
9. [Si seleccionó **Nueva ubicación**] Seleccione el buzón de correo de destino.
   a. En **Recuperar a**, haga clic en **Seleccionar**.
   b. Seleccione el buzón de correo de destino y haga clic en **Seleccionar**.
10. Haga clic en **Iniciar recuperación**.

Como resultado, los correos electrónicos entrantes del buzón de correo seleccionado se recuperan en la carpeta **Bandeja de entrada** del buzón de correo de destino, y los correos electrónicos salientes del buzón de correo seleccionado se recuperan en la carpeta **Enviados** del buzón de correo de destino.

Buzones de correo

Para recuperar un buzón de correo

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones de la nube** y seleccione el archivo comprimido de correos electrónicos del que desea recuperar los datos.
3. Haga clic en **Examinar archivo comprimido**.
4. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
5. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
6. Seleccione los elementos que desea recuperar y, a continuación, haga clic en **Recuperar correos electrónicos de usuario**.
7. [Si se han añadido varios servidores de correo a la consola de Cyber Protect] Seleccione la organización en la que desea recuperar los datos.

© Acronis International GmbH, 2003-2025

a. En **Organización**, haga clic en **Seleccionar**.

b. Seleccione la organización y haga clic en **Seleccionar**.

8. En **Ubicación de recuperación**, seleccione la ubicación en la que desea recuperar los datos.
9. [Si seleccionó **Nueva ubicación**] Seleccione el buzón de correo de destino.
   a. En **Recuperar a**, haga clic en **Seleccionar**.
   b. Seleccione el buzón de correo de destino y haga clic en **Seleccionar**.
10. Haga clic en **Iniciar recuperación**.

Como resultado, los correos electrónicos entrantes del buzón de correo seleccionado se recuperan en la carpeta **Bandeja de entrada** del buzón de correo de destino, y los correos electrónicos salientes del buzón de correo seleccionado se recuperan en la carpeta **Enviados** del buzón de correo de destino.

Reenvío de correos electrónicos archivados

Puede seleccionar hasta 10 correos electrónicos de un archivo comprimido de correos electrónicos y enviarlos a los destinatarios que elija.

Para reenviar correos electrónicos archivados

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Haga una búsqueda en el archivo comprimido de correos electrónicos o use una consulta de búsqueda guardada.
   Para obtener más información, consulte "Búsqueda de correos electrónicos" (p. 772) y "Creación de una consulta de búsqueda guardada" (p. 774).
3. Seleccione hasta 10 correos electrónicos y haga click en **Enviar como correo electrónico**.
4. [Si se han registrado varias organizaciones] Seleccione una organización.
5. Haga clic en el campo **Remitente** y seleccione el usuario en cuyo nombre se enviarán los correos electrónicos.
   El nombre de este usuario aparece en el campo **De** de los correos electrónicos.
6. En **Destinatarios**, escriba una o varias direcciones de correo electrónico a las que desee enviar los correos electrónicos seleccionados.
   Si introduce varias direcciones de correo electrónico, sepárelas con una coma o punto y coma.
7. [Opcional] Agregue una descripción que se añadirá en la parte superior de todos los correos electrónicos enviados.
8. Haga clic en **Enviar**.

Como resultado, los correos electrónicos seleccionados se enviarán como correos electrónicos individuales a las direcciones que haya especificado.

Descarga de archivos adjuntos

Puede descargar los archivos adjuntos de uno o más correos electrónicos en el archivo comprimido.

© Acronis International GmbH, 2003-2025

Pasos para descargar archivos adjuntos

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones en la nube** y seleccione el archivo comprimido de correos electrónicos.
3. Haga clic en **Examinar archivo comprimido**.
4. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
5. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
6. [Opcional] Busque los correos electrónicos con los archivos adjuntos que desea descargar.
   Puede utilizar consultas de búsqueda ad hoc y consultas de búsqueda guardadas. Para obtener más información, consulte "Búsqueda de correos electrónicos" (p. 772).
7. Seleccione los correos electrónicos con los archivos adjuntos que desea descargar y, a continuación, haga clic en **Descargar archivos adjuntos**.

Como resultado, los archivos adjuntos de los correos electrónicos seleccionados se descargan en su equipo.

Cuando descargue más de un elemento, los archivos adjuntos se descargarán como un archivo ZIP.

Almacenamiento inmutable para el archivado de correos electrónicos

Con el almacenamiento inmutable, puede acceder a los siguientes elementos eliminados durante el período de retención del almacenamiento inmutable:

- Los mensajes de correo electrónico que fueron eliminados automáticamente por las reglas de retención.
- Archivos de correos electrónicos que fueron eliminados por un administrador y los mensajes de correo en estos archivos.

Puede explorar y buscar los mensajes de correo electrónico eliminados, recuperarlos y deshacer su eliminación.

No puede aplicar reglas de retención ni reglas de retención legal a correos electrónicos eliminados.

Después de que finalice el período de retención, los elementos en almacenamiento inmutable se eliminan de forma permanente. Para obtener más información, consulte "Almacenamiento inmutable" (p. 1570).

Deshacer la eliminación de correos electrónicos en almacenamiento inmutable

Puede deshacer la eliminación de correos electrónicos que están en almacenamiento inmutable y restaurarlos en el archivo de correos.

© Acronis International GmbH, 2003-2025

Nota
Puede deshacer la eliminación de correos electrónicos individuales. No se puede deshacer la eliminación de archivos de correo electrónico.

Para deshacer la eliminación

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones en la nube**.
3. [Si se eliminó todo el archivo de correos] Haga clic en **Mostrar elementos eliminados**.
4. Seleccione un archivo de correos y, a continuación, haga clic en **Examinar el archivo**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. En el diálogo **Contraseña de cifrado**, especifique la contraseña y haga clic en **Continuar**.
7. [Opcional] Busque correos electrónicos específicos utilizando el campo de búsqueda. Para obtener más información, consulte "Búsqueda de correos electrónicos" (p. 772).
   Alternativamente, puede utilizar una consulta de búsqueda que incluya elementos eliminados. Para obtener más información, consulte "Creación de una consulta de búsqueda guardada" (p. 774).
8. Seleccione hasta 10 correos electrónicos eliminados y, a continuación, haga clic en **Restauración**.

Como resultado, los correos electrónicos seleccionados ya no se marcarán como eliminados y se restaurarán al archivo de correos.

Protección de aplicaciones de Microsoft

Protección de Microsoft SQL Server y Microsoft Exchange Server

Nota
La copia de seguridad de Microsoft SQL solo es compatible con las bases de datos que se ejecutan en sistemas de archivos NTFS, REFS y FAT32. ExFat no es compatible.

Existen dos métodos para proteger las aplicaciones de Microsoft:

- **Copia de seguridad de la base de datos**
  Se trata de una copia de seguridad a nivel de archivo de las bases de datos y los metadatos asociados. Las bases de datos se pueden recuperar en una aplicación activa o como archivos.
- **Copia de seguridad compatible con la aplicación**
  Se trata de una copia de seguridad a nivel de disco que también recopila los metadatos de las aplicaciones. Estos metadatos permiten la exploración y la recuperación de los datos de las aplicaciones sin que sea necesario recuperar todo el disco o volumen. También se puede

© Acronis International GmbH, 2003-2025

recuperar el disco o volumen entero. Esto significa que se puede utilizar una única solución y un solo plan de protección para la recuperación ante desastres y para la protección de datos.

Para Microsoft Exchange Server, puede optar por **Copia de seguridad de buzón de correo**. Esta es una copia de seguridad de buzones de correo individuales que se realiza a través del protocolo de Servicios Exchange Web. Los buzones de correo o elementos de los buzones de correo pueden recuperarse a un servidor activo de Exchange Server o a Microsoft 365. La copia de seguridad del buzón de correo es compatible con Microsoft Exchange Server 2010 Service Pack 1 (SP1) o versión posterior.

Protección de Microsoft SharePoint

Una granja de Microsoft SharePoint está compuesta por servidores front-end que ejecutan servicios de SharePoint, servidores de bases de datos que ejecutan Microsoft SQL Server y (opcionalmente) servidores de aplicaciones que excluyen algunos servicios de SharePoint de los servidores front-end. Algunos servidores front-end y de aplicaciones pueden ser idénticos entre sí.

Para proteger toda una granja de SharePoint:

- Haga una copia de seguridad de todos los servidores de bases de datos con una copia de seguridad compatible con la aplicación.
- Haga una copia de seguridad de todos los servidores front-end únicos y los servidores de aplicaciones con una copia de seguridad normal a nivel de disco.

Las copias de seguridad de todos los servidores se deben realizar en la misma fecha.

Para proteger solo el contenido, puede hacer una copia de seguridad de las bases de datos de contenido por separado.

Protección de un controlador de dominio

Un equipo que ejecuta Servicios de dominio de Active Directory se puede proteger con una copia de seguridad compatible con la aplicación. Si un dominio contiene más de un controlador de dominios y desea recuperar alguno de ellos, se realizará una restauración no autorizada y no habrá reversión USN alguna después de la recuperación.

Recuperación de aplicaciones

La siguiente tabla recoge los métodos de recuperación de aplicaciones disponibles.

	A partir de una copia de seguridad de base de datos	**A partir de una copia de seguridad compatible con la aplicación**	**A partir de una copia de seguridad del disco**
Microsoft SQL Server	Bases de datos a una instancia activa de SQL Server Bases de datos como archivos	Todo el equipo Bases de datos a una instancia activa de SQL Server	Todo el equipo

© Acronis International GmbH, 2003-2025

		Bases de datos como archivos	
Microsoft Exchange Server	Bases de datos a un servidor activo de Exchange Bases de datos como archivos Recuperación granular a un servidor activo de Exchange Server o a Microsoft 365*	Todo el equipo Bases de datos a un servidor activo de Exchange Bases de datos como archivos Recuperación granular a un servidor activo de Exchange Server o a Microsoft 365*	Todo el equipo
Servidores de bases de datos de Microsoft SharePoint	Bases de datos a una instancia activa de SQL Server Bases de datos como archivos Recuperación granular mediante SharePoint Explorer	Todo el equipo Bases de datos a una instancia activa de SQL Server Bases de datos como archivos Recuperación granular mediante SharePoint Explorer	Todo el equipo
Servidor web front-end de Microsoft SharePoint	-	-	Todo el equipo
Servicios de dominio de Active Directory	-	Todo el equipo	-

* La recuperación granular también está disponible a partir de la copia de seguridad de un buzón de correo. La recuperación de elementos de datos de Exchange a Microsoft 365 y viceversa es compatible siempre que se haya instalado localmente el Agente para Microsoft 365.

Requisitos para copias de seguridad con información de aplicaciones

Antes de configurar la copia de seguridad de la aplicación, asegúrese de que se cumplen los siguientes requisitos.

Para consultar el estado de los escritores de VSS, use el comando `vssadmin list writers`.

Requisitos habituales

En Microsoft SQL Server, asegúrese de que:

- Se haya iniciado al menos una instancia de Microsoft SQL Server.
- El escritor de SQL para VSS esté activado.

En Microsoft Exchange Server, asegúrese de que:

© Acronis International GmbH, 2003-2025

- Se haya iniciado el servicio del almacén de información de Microsoft Exchange.
- Windows PowerShell esté instalado. En Exchange 2010 o posterior, la versión de Windows PowerShell debe ser, como mínimo, 2.0.
- Microsoft .NET Framework esté instalado.

  En Exchange 2007, la versión de Microsoft .NET Framework debe ser, como mínimo, 2.0.

  En Exchange 2010 o posterior, la versión de Microsoft .NET Framework debe ser, como mínimo, 3.5.
- El escritor de Exchange para VSS está activado.

Nota
Agente para Exchange necesita un almacenamiento temporal para funcionar. De manera predeterminada, los archivos temporales se encuentran en `%ProgramData%\Acronis\Temp`. Asegúrese de que el espacio libre del volumen en el que se encuentra la carpeta `%ProgramData%` es, como mínimo, igual al 15 % del tamaño de una base de datos de Exchange. Como alternativa, puede cambiar la ubicación de los archivos temporales antes de crear las copias de seguridad de Exchange, según se describe en Cambiar la ubicación de los archivos temporales y la carpeta (40040).

En un controlador de dominio, asegúrese de que:

- El escritor de Active Directory para VSS esté activado.

Al crear un plan de protección, asegúrese de que:

- En los equipos físicos y aquellos en los que esté instalado el agente, la opción de copia de seguridad Servicio de instantáneas de volumen (VSS) esté habilitada.
- En los equipos virtuales, la opción de copia de seguridad Servicio de instantáneas de volumen (VSS) para equipos virtuales esté habilitada.

Otros requisitos para copias de seguridad compatibles con la aplicación

Al crear un plan de protección, compruebe que **Todo el equipo** esté seleccionado para la copia de seguridad. Debe deshabilitarse la opción **Sector por sector** en el plan de protección. De lo contrario, será imposible realizar la recuperación de datos de aplicaciones desde tales copias de seguridad. Si el plan se ejecuta en el modo **Sector por sector** debido a un cambio automático a dicho modo, también será imposible recuperar los datos de aplicaciones.

Requisitos para equipos virtuales ESXi

Si la aplicación se ejecuta en un equipo virtual del que Agent para VMware hace una copia de seguridad, asegúrese de que:

- La máquina virtual que se está respaldando cumple con los requisitos para la copia de seguridad y restauración coherentes con la aplicación que se enumeran en el artículo "Implementaciones de copia de seguridad de Windows" en la documentación de VMware: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere-sdks-tools/8-0/virtual-disk-

© Acronis International GmbH, 2003-2025

development-kit-programming-guide/backing-up-virtual-disks-in-vsphere/windows-backup-implementations/working-with-microsoft-shadow-copy.html.

- Las herramientas de VMware están instaladas y actualizadas en el equipo.
- El control de cuentas de usuario (UAC) está deshabilitado en el equipo. Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominio incorporado (DOMINIO\Administrador) al habilitar la copia de seguridad de las aplicaciones.
  Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominio incorporado (DOMINIO\Administrador) al habilitar la copia de seguridad de las aplicaciones.

  Nota
  Use la cuenta de administrador de dominio incorporado que se configuró como parte de la creación del dominio. No se admiten las cuentas creadas posteriormente.

Requisitos de equipos virtuales Hyper-V

Si la aplicación se ejecuta en un equipo virtual del que Agent para Hyper-V hace una copia de seguridad, asegúrese de que:

- El sistema operativo invitado es Windows Server 2008 o posterior.
- Para Hyper-V 2008 R2: el sistema operativo invitado es Windows Server 2008/2008 R2/2012.
- El equipo virtual no tiene disco dinámico.
- Existe conexión de red entre el host de Hyper-V y el sistema operativo invitado. Esto es necesario para ejecutar consultas de WMI remotas dentro del equipo virtual.
- El control de cuentas de usuario (UAC) está deshabilitado en el equipo. Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominio incorporado (DOMINIO\Administrador) al habilitar la copia de seguridad de las aplicaciones.
  Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominio incorporado (DOMINIO\Administrador) al habilitar la copia de seguridad de las aplicaciones.

  Nota
  Use la cuenta de administrador de dominio incorporado que se configuró como parte de la creación del dominio. No se admiten las cuentas creadas posteriormente.

- La configuración del equipo virtual cumple los siguientes criterios:
  - Hyper-V Integration Services está instalado y actualizado. La actualización crítica es https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - En la configuración del equipo virtual, la opción **Gestión** > **Integration Services** > **Copia de seguridad (punto de comprobación de volumen)** está habilitada.
  - Para Hyper-V 2012 y posterior: el equipo virtual no tiene puntos de comprobación.

© Acronis International GmbH, 2003-2025

- Para Hyper-V 2012 R2 y posterior: el equipo virtual tiene un controlador SCSI (compruebe **Configuración** > **Hardware**).

Copia de seguridad de la base de datos

Antes de hacer una copia de seguridad de las bases de datos, asegúrese de cumplir con los requisitos recogidos en "Requisitos previos".

Seleccione las bases de datos tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Seleccionar bases de datos de SQL

La copia de seguridad de una base de datos de SQL contiene archivos de base de datos (.mdf, .ndf), archivos de registro (.ldf) y otros archivos asociados. Los archivos son copiados con la ayuda del servicio Writer de SQL. El servicio se debe estar ejecutando a la vez que el Servicio de instantáneas de volumen (VSS) solicita una copia de seguridad o recuperación.

Los registros de transacción de SQL se truncan después de crear una copia de seguridad correctamente. El truncamiento de registros de SQL se puede deshabilitar en las opciones del plan de protección.

Para seleccionar bases de datos de SQL

1. Haga clic en **Dispositivos** > **Microsoft SQL**.
   El software muestra el árbol de los grupos de disponibilidad Always On (AAG) de SQL Server, equipos que ejecutan Microsoft SQL Server, instancias de SQL Server y bases de datos.
2. Busque los datos de los que desea realizar la copia de seguridad.
   Expanda los nodos del árbol o haga doble clic en los elementos de la lista de la parte derecha del árbol.
3. Seleccione los datos de los que desea realizar la copia de seguridad. Puede seleccionar los AAG, equipos que ejecuten SQL Server, instancias de SQL Server o bases de datos individuales.
   - Si selecciona un AAG, se realizará una copia de seguridad de todas las bases de datos que se incluyan en el AAG seleccionado. Para obtener más información acerca de la copia de seguridad de los AAG o las bases de datos AAG individuales, consulte "Protección de los grupos de disponibilidad Always On (AAG)".
   - Si selecciona un equipo que ejecute un SQL Server, se realizará una copia de seguridad de todas las bases de datos conectadas a todas las instancias de SQL Server que se ejecuten en el equipo seleccionado.
   - Si selecciona un instancia de SQL Server, se realizará una copia de seguridad de todas las bases de datos conectadas a la instancia seleccionada.
   - Si selecciona base de datos concretas, únicamente se realizarán copias de seguridad de las bases de datos seleccionadas.
4. Haga clic en **Proteger**. Si se le pide, proporcione las credenciales para acceder a los datos de SQL Server.

© Acronis International GmbH, 2003-2025

Si usa la autenticación de Windows, la cuenta debe ser miembro del grupo **Operadores de copia de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

Si usa la autenticación del SQL Server, la cuenta debe ser miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

Seleccionar datos de Exchange Server

La siguiente tabla resume los datos de Microsoft Exchange Server que puede seleccionar para realizar la copia de seguridad y los permisos de usuario mínimos requeridos para realizar la copia de seguridad de los datos.

Versión de Exchange	Elementos de los datos	Permisos de usuario
2007	Grupos de almacenamiento	Asociación en el grupo de funciones **Administradores de la organización de Exchange**.
2010/2013/2016/2019	Bases de datos, grupos de disponibilidad de base de datos (DAG)	Pertenencia al grupo de funciones **Administración de servidores**.

Una copia de seguridad completa contiene todos los datos seleccionados de Exchange Server.

Una copia de seguridad incremental contiene los bloques cambiados de los archivos de la base de datos, los archivos de control y una pequeña cantidad de archivos de acceso que son más recientes que el punto de control de la base de datos correspondiente. Ya que los cambios en los archivos de la base de datos están incluidos en la copia de seguridad, no hay necesidad de realizar copias de seguridad de todos los registros de acceso de transacción desde la copia de seguridad anterior. Después de una recuperación, únicamente se necesita reproducir el acceso que sea más reciente que el punto de control. Esto garantiza una recuperación más rápida y que la copia de seguridad de la base de datos se realice con éxito, aun con el registro circular habilitado.

Los archivos de registro de transacción quedan truncados después de cada copia de seguridad realizada con éxito.

Para seleccionar datos de Exchange Server

1. Haga clic en **Dispositivos** > **Microsoft Exchange**.

   El software muestra el árbol de los grupos de disponibilidad de base de datos (DAG) de Exchange Server, equipos que ejecutan Microsoft Exchange Server y bases de datos de Exchange Server. Si ha configurado Agente para Exchange tal y como se describe en "Copia de seguridad de casillas de correo" (p. 807), los buzones de correo también se muestran en este árbol.
2. Busque los datos de los que desea realizar la copia de seguridad.

   Expanda los nodos del árbol o haga doble clic en los elementos de la lista de la parte derecha del árbol.
3. Seleccione los datos de los que desea realizar la copia de seguridad.

© Acronis International GmbH, 2003-2025

- Si selecciona un DAG, se realizará una copia de seguridad de todas las bases de datos en clúster. Para obtener más información acerca de la copia de seguridad de los DAG, consulte "Protección de los grupos de disponibilidad de bases de datos (DAG)" (p. 801).
- Si selecciona un equipo que ejecute Microsoft Exchange Server, se realizará una copia de seguridad de todas las bases de datos montadas en Exchange Server que se ejecute en el equipo seleccionado.
- Si selecciona base de datos concretas, únicamente se realizarán copias de seguridad de las bases de datos seleccionadas.
- Si ha configurado Agente para Exchange tal y como se describe en "Copia de seguridad de casillas de correo" (p. 807), puede seleccionar los buzones de correo para la copia de seguridad.

Si la selección incluye varias bases de datos, se procesarán de dos en dos. Cuando finalice la copia de seguridad del primer grupo, comenzará la del segundo.

4. Si se le pide, proporcione las credenciales para acceder a los datos.
5. Haga clic en **Proteger**.

Protección de los grupos de disponibilidad Always On (AAG)

Nota
Esta función está disponible con el paquete Advanced Backup.

Descripción de soluciones de alta disponibilidad de SQL Server

La funcionalidad Clúster de conmutación por error de Windows (WSFC) permite configurar SQL Server con alta disponibilidad a través de la redundancia a nivel de la instancia (instancia de clúster de conmutación por error, FCI) o a nivel de la base de datos (grupo de disponibilidad AlwaysOn, AAG). También se pueden combinar ambos métodos.

En una instancia de clúster de conmutación por error, las bases de datos de SQL se ubican en un espacio de almacenamiento compartido. A este almacenamiento solo se puede tener acceso desde un nodo de clúster activo. Si se produce un error en el nodo activo, se genera una conmutación por error y se activa otro nodo.

En el caso de un grupo de disponibilidad, la réplica de cada base de datos reside en un nodo diferente. Si la réplica principal no está disponible, se asigna la función principal a una réplica secundaria que resida en un nodo diferente.

Por lo tanto, los clústeres ya sirven como soluciones de recuperación de desastres por sí mismos. Sin embargo, puede haber casos cuando los clústeres no pueden proporcionar protección de datos: por ejemplo, en caso de un daño en la lógica de la base de datos o cuando todo el clúster está caído. Además, las soluciones de clúster no protegen de los cambios de contenido dañinos, ya que normalmente se replican inmediatamente en todos los nodos de clúster.

© Acronis International GmbH, 2003-2025

Configuraciones de clúster compatibles

Este software de copia de seguridad es compatible *solo* con el grupo de disponibilidad Always On (AAG) para SQL Server 2012 o posterior. Otras configuraciones de clúster, tales como instancia del clúster de conmutación por error, creación de reflejo de la base de datos y trasvase de registros *no* son compatibles.

¿Cuántos agentes se necesitan para la copia de seguridad y recuperación de los datos del clúster?

Para una copia de seguridad y recuperación de datos correcta de un clúster, Agent for SQL debe estar instalado en cada nodo del clúster de WSFC.

Copias de seguridad de bases de datos incluidas en AAG

1. Instale Agent por SQL en cada nodo del clúster WSFC.
2. Seleccione el AAG para realizar una copia de seguridad según se describe en "Seleccionar bases de datos de SQL".

   Debe seleccionar el propio AAG para realizar una copia de seguridad de todas las bases de datos del AAG. Para realizar una copia de seguridad de todas las bases de datos, defina este conjunto de bases de datos en todos los nodos del AAG.

   Advertencia.
   El conjunto de bases de datos debe ser exactamente igual en todos los nodos. Si uno de los conjuntos es diferente o no se ha definido en todos los nodos, la copia de seguridad del clúster no funcionará correctamente.
3. Configure la opción de copia de seguridad «Modo de copia de seguridad de clústeres»

Recuperación de bases de datos incluidas en un AAG

1. Seleccione las bases datos que desea recuperar y, a continuación, seleccione el punto de recuperación desde el cual desea recuperar las bases de datos.

   Al seleccionar una base de datos en clúster bajo **Dispositivos** > **Microsoft SQL** > **Bases de datos** y, a continuación, haga clic en **Recuperar**, el software muestra solo los puntos de recuperación que corresponden a las veces cuando se ha realizado una copia de seguridad de la copia seleccionada de la base de datos.

   La manera más fácil para ver todos los puntos de recuperación de una base de datos en clúster es seleccionar la copia de seguridad del AAG entero en la pestaña Almacenamiento de copias de seguridad. Los nombres de copias de seguridad del AAG están basados en la plantilla siguiente `<AAG name> - <protection plan name>` y tienen un icono especial.
2. Para configurar la recuperación, siga los pasos descritos en «Recuperación de base de datos SQL», a partir del paso 5.

© Acronis International GmbH, 2003-2025

El software define automáticamente un nodo de clúster en donde se recuperarán los datos. El nombre del nodo se visualizará en el campo **Recuperar a**. Puede cambiar manualmente el nodo de destino.

Importante
Microsoft SQL Server no permite que se sobrescriba una base de datos incluida en un grupo de disponibilidad Always On durante una recuperación. Debe excluir la base de datos de destino del AAG antes de la recuperación. O bien, puede recuperar la base de datos como una nueva que no pertenezca al AAG. Una vez que se haya completado la recuperación, puede restablecer la configuración original del AAG.

Protección de los grupos de disponibilidad de bases de datos (DAG)

Nota
Esta función está disponible con el paquete Advanced Backup.

Generalidades de clústeres de Exchange Server

La idea principal de los clústeres de Exchange es proporcionar una alta disponibilidad de la base de datos con recuperación de fallos rápida y sin pérdida de datos. Generalmente, se logra al tener una o más copias de las bases de datos o los grupos de almacenamiento en los miembros del clúster (nodos de clúster). Si el nodo de clúster que alberga la copia activa de la base de datos o la copia activa de la base de datos misma falla, el otro nodo que alberga la copia pasiva toma control automáticamente de las operaciones del nodo que falló y proporciona acceso a los servicios de Exchange con un tiempo de inactividad mínimo. Por lo tanto, los clústeres ya sirven como soluciones de recuperación de desastres por sí mismos.

Sin embargo, es posible que existan casos en donde las soluciones de clúster de recuperación de fallos no proporcionen una protección de los datos: por ejemplo, en caso de un daño en la lógica de la base de datos o cuando una base de datos en particular en un clúster no tiene copia (réplica), o cuando todo el clúster está caído. Además, las soluciones de clúster no protegen de los cambios de contenido dañinos, ya que normalmente se replican inmediatamente en todos los nodos de clúster.

Copia de seguridad compatible con el clúster

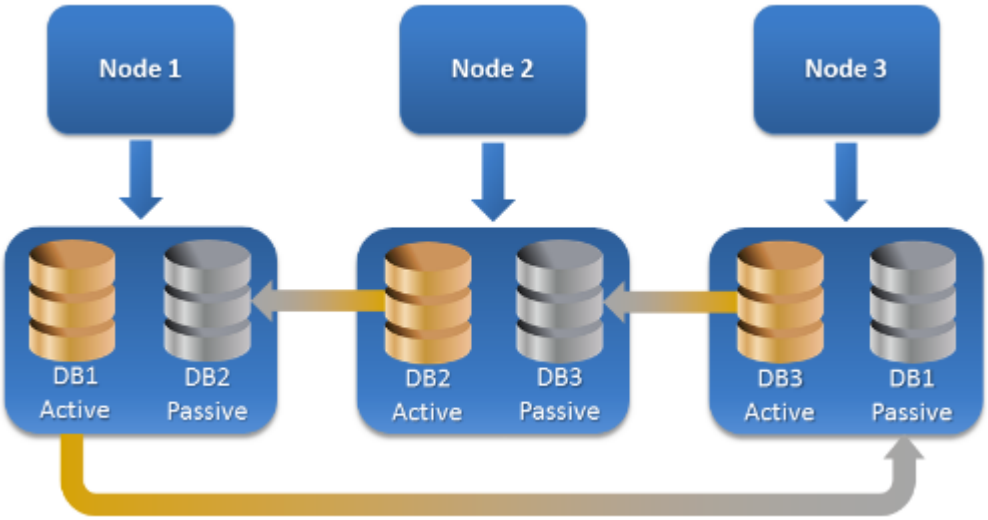
En la copia de seguridad compatible con el clúster, solo se realiza una copia de seguridad de los datos en clúster. Si cambia la ubicación de los datos dentro del clúster (debido a un cambio o conmutación por error), el software realizará el seguimiento de todas las reubicaciones de estos datos y creará una copia de seguridad de forma segura.

Configuraciones de clúster compatibles

La copia de seguridad compatible con el clúster *solo* se admite con Grupo de disponibilidad de base de datos (DAG) en Exchange Server 2010 o versiones posteriores. Otras configuraciones de clústeres, como el clúster de copia única (SCC) y la replicación continua en clústeres (CCR) para Exchange 2007, *no* son compatibles.

© Acronis International GmbH, 2003-2025

DAG es un grupo de hasta 16 servidores de buzones de correo de Exchange. Cualquier nodo puede albergar una copia de la base de datos del buzón de correo de cualquier otro nodo. Cada nodo puede albergar copias de base de datos activas y pasivas. Es posible crear hasta 16 copias de cada base de datos.



¿Cuántos agentes se necesitan para la copia de seguridad y recuperación compatible con el clúster?

Para una copia de seguridad y recuperación correcta de bases de datos en clúster, Agente para Exchange debe estar instalado en cada nodo del clúster de Exchange.

Nota
Después de instalar el agente en uno de los nodos, la consola de Cyber Protect muestra el DAG y sus nodos en **Dispositivos** > **Microsoft Exchange** > **Bases de datos**. Para instalar Agents for Exchange en el resto de los nodos, seleccione el DAG, haga clic **Detalles** y, a continuación, haga clic en **Instalar el agente** junto a cada uno de los nodos.

Copia de seguridad de los datos del clúster de Exchange

1. Al crear un plan de protección, seleccione el DAG según se describe en "Seleccionar datos de Exchange Server" (p. 798).
2. Configure la opción de copia de seguridad de "Modo de copia de seguridad de clústeres" (p. 603).
3. Especifique las demás opciones de configuración del plan de protección según corresponda.

Importante
Para la copia de seguridad compatible con el clúster, asegúrese de seleccionar el propio DAG. Si selecciona nodos individuales o bases de datos dentro del DAG, solo se realizará la copia de seguridad de los elementos seleccionados y se omitirá la opción **Modo de copia de seguridad de clústeres**.

© Acronis International GmbH, 2003-2025

Recuperación de los datos del clúster de Exchange

1. Seleccione el punto de recuperación de la base datos que desea recuperar. No se puede seleccionar todo un clúster para la recuperación.

   Al seleccionar una copia de una base de datos en clúster en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** > `<cluster name>` > `<node name>` y hacer clic en **Recuperar**, el software muestra solo los puntos de recuperación que se correspondan con las horas a las que se realizó la copia de seguridad de la copia.

   La manera más fácil para ver todos los puntos de recuperación de una base de datos en clúster es seleccionar su copia de seguridad en la pestaña Almacenamiento de copias de seguridad.
2. Siga los pasos descritos en "Recuperación de bases de datos de Exchange" (p. 817), a partir del paso 5.

   El software define automáticamente un nodo de clúster en donde se recuperarán los datos. El nombre del nodo se visualizará en el campo **Recuperar a**. Puede cambiar manualmente el nodo de destino.

Copia de seguridad compatible con la aplicación

La copia de seguridad de nivel de disco con información de aplicaciones está disponible para equipos físicos individuales, máquinas virtuales ESXi y máquinas virtuales Hyper-V. No está disponible para grupos de dispositivos.

Al realizar una copia de seguridad de un equipo que ejecute Microsoft SQL Server, Microsoft Exchange Server o Servicios de dominio de Active Directory, habilite **Copia de seguridad de aplicación** para dotar de mayor seguridad a los datos de estas aplicaciones.



Motivos para usar la copia de seguridad compatible con la aplicación

Al usar la copia de seguridad compatible con la aplicación, se asegura de lo siguiente:

- Se realiza una copia de seguridad de las aplicaciones en un estado coherente y, por consiguiente, estarán disponibles inmediatamente después de la recuperación del equipo.
- Puede recuperar las bases de datos de SQL y Exchange, los buzones de correo y los elementos de buzón de correo sin tener que recuperar todo el equipo.
- Los registros de transacción de SQL se truncan después de crear una copia de seguridad correctamente. El truncamiento de registros de SQL se puede deshabilitar en las opciones del plan de protección. Los registros de transacción de Exchange solo se truncan en los equipos virtuales. Puede habilitar la opción de copia de seguridad completa de VSS si quiere truncar los registros de transacción de Exchange en un equipo físico.

© Acronis International GmbH, 2003-2025

- Si un dominio contiene más de un controlador de dominios y desea recuperar alguno de ellos, se realizará una restauración no autorizada y no habrá reversión USN alguna después de la recuperación.

¿Qué necesito para usar la copia de seguridad compatible con la aplicación?

En un equipo físico, hay que tener instalado Agente para SQL o Agente para Exchange además de Agente para Windows.

En una maquina virtual no es necesario instalar ningún agente; se presupone que el Agente para VMware o el Agente para Hyper-V hacen una copia de seguridad de la máquina.

Nota
La copia de seguridad con información de aplicaciones sin agente no es compatible con las máquinas virtuales de Hyper-V y VMware ESXi que ejecutan Windows Server 2022 o Windows Server 2025. Para proteger las aplicaciones de Microsoft en estos equipos, instale el agente de protección dentro del sistema operativo invitado. Para obtener más información, consulte "Configuración de la copia de seguridad con información de aplicaciones de máquinas virtuales que ejecutan Windows Server 2022 y versiones posteriores" (p. 805).

Agente para VMware (dispositivo virtual) puede crear copias de seguridad compatibles con la aplicación, pero no puede recuperar datos de aplicaciones de estas. Para recuperar datos de aplicaciones de copias de seguridad creadas por este agente, necesita Agente para VMware (Windows), Agente para SQL o Agente para Exchange en un equipo con acceso a la ubicación en la que se almacenan las copias de seguridad. Al configurar la recuperación de los datos de aplicaciones, seleccione el punto de recuperación en la pestaña **Almacenamiento de la copia de seguridad** y, a continuación, seleccione este equipo en **Equipo desde el cual examinar**.

En "Requisitos para copias de seguridad con información de aplicaciones" (p. 794) y "Derechos de usuario necesarios para copias de seguridad con información de aplicaciones" (p. 805) se enumeran requisitos adicionales.

Nota
Es posible que fallen las copias de seguridad con información de aplicaciones de las máquinas virtuales de Hyper-V con el error "'ExecQuery' de WMI no ha podido ejecutar la consulta." o "No se ha podido crear un nuevo proceso a través de WMI" si se realizan las copias de seguridad en un host con una carga elevada, debido a la falta o el retraso de una respuesta del Instrumental de administración de Windows. Vuelva a intentar estas copias de seguridad en otro espacio de tiempo cuando la carga del host sea menor.

© Acronis International GmbH, 2003-2025

Configuración de la copia de seguridad con información de aplicaciones de máquinas virtuales que ejecutan Windows Server 2022 y versiones posteriores

Para realizar una copia de seguridad con información de aplicaciones en máquinas virtuales de Hyper-V y VMware ESXi que ejecutan Windows Server 2022 o Windows Server 2025, debe utilizar la copia de seguridad basada en agentes. Para obtener más información sobre los modos de copia de seguridad, consulte "Copia de seguridad basada en agente y sin agente" (p. 41).

	Copia de seguridad basada en agente	**Copia de seguridad sin agente**
Copia de seguridad compatible con la aplicación	Compatible	No compatible
Icono de máquina virtual en la consola de Cyber Protect		

Para configurar la copia de seguridad con información de aplicaciones en el modo basado en agentes

1. Instale el agente de protección (como agente para Windows, agente para SQL o agente para Exchange) dentro del sistema operativo invitado de la máquina virtual.
2. En la consola de Cyber Protect, seleccione el equipo en el que quiera instalar el agente de protección.
3. Configure la copia de seguridad con información de aplicaciones en un nuevo plan de protección.
4. Aplique el plan de protección a la máquina virtual.
5. Ejecute el plan de protección.

Como resultado, se creará un archivo de copia de seguridad que incluya la copia de seguridad con información de aplicaciones.

Derechos de usuario necesarios para copias de seguridad con información de aplicaciones

Una copia de seguridad compatible con la aplicación contiene metadatos de aplicaciones compatibles con VSS que están presentes en el disco. Para acceder a estos metadatos, el agente necesita una cuenta con los derechos apropiados, que se indican a continuación. Se le pedirá que especifique esta cuenta al habilitar la copia de seguridad de la aplicación.

- Para SQL Server:

© Acronis International GmbH, 2003-2025

La cuenta debe ser un miembro del grupo **Operadores de copias de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

Nota
Solo se admite la autenticación de Windows.

- Para Exchange Server:

  Exchange 2007: La cuenta debe pertenecer al grupo **Administradores** del equipo y al grupo de funciones **Administradores de la organización de Exchange**.

  Exchange 2010 y posterior: La cuenta debe pertenecer al grupo **Administradores** del equipo y al grupo de funciones **Gestión de la organización**.
- Para Active Directory:

  La cuenta debe ser un administrador de dominios.

Otros requisitos para equipos virtuales

Si la aplicación se ejecuta en un equipo virtual del que Agent para VMware o Agent para Hyper-V hace una copia de seguridad, asegúrese de que el control de cuentas de usuario (UAC) está deshabilitado en el equipo.

Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominio incorporado (DOMINIO\Administrador) al habilitar la copia de seguridad de las aplicaciones.

Nota
Use la cuenta de administrador de dominio incorporado que se configuró como parte de la creación del dominio. No se admiten las cuentas creadas posteriormente.

Requisitos adicionales para equipos con Windows

En todas las versiones de Windows es necesario deshabilitar las directivas de Control de la cuenta de usuario (UAC) para permitir las copias de seguridad con información de aplicaciones.

Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominio incorporado (DOMINIO\Administrador) al habilitar la copia de seguridad de las aplicaciones.

Nota
Use la cuenta de administrador de dominio incorporado que se configuró como parte de la creación del dominio. No se admiten las cuentas creadas posteriormente.

Para deshabilitar las directivas UAC en Windows

1. En el Editor del Registro, localice la siguiente clave de registro:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`

© Acronis International GmbH, 2003-2025

2. Cambie el valor de **EnableLUA** a **0**.
3. Reinicie el equipo.

Copia de seguridad de casillas de correo

La copia de seguridad del buzón de correo es compatible con Microsoft Exchange Server 2010 Service Pack 1 (SP1) o versión posterior.

La copia de seguridad de los buzones de correo está disponible si se ha registrado por lo menos un Agente for Exchange en el servidor de gestión. El agente tiene que estar instalado en un equipo que pertenezca al mismo bosque de Active Directory que Microsoft Exchange Server.

Antes de realizar la copia de seguridad de los buzones de correo electrónico, debe conectar Agente para Exchange al equipo que ejecuta el rol del servidor **Acceso de cliente** (CAS) de Microsoft Exchange Server. En Exchange 2016 y versiones posteriores, el rol CAS no está disponible como opción de instalación independiente. Se instala automáticamente como parte del rol de servidor Buzón de correo. Por lo tanto, puede conectar el agente a cualquier servidor que ejecute el **Rol de buzón de correo**.

Nota
También puede recuperar los buzones de correo y los elementos de los buzones desde copias de seguridad de bases de datos y desde copias de seguridad con información de aplicaciones. Para obtener más información, consulte "Recuperación de elementos de buzón de correo y de buzones de correo de Exchange" (p. 821). No puede crear planes de protección para buzones de correo individuales con copias de seguridad de bases de datos y copias de seguridad con información de aplicaciones.

Para conectar Agente para Exchange a CAS

1. Haga clic en **Dispositivos** > **Agregar**.
2. Haga clic en **Microsoft Exchange Server**.
3. Haga clic en **Buzones de correo de Exchange**.
   Si no hay ningún Agente para Exchange registrado en el servidor de gestión, el software le sugerirá que instale el agente. Después de la instalación, repita este procedimiento desde el paso 1.
4. [Opcional] Si hay registrados varios Agents for Exchange en el servidor de gestión, haga clic en **Agente** y cambie el agente que llevará a cabo la copia de seguridad.
5. En **Servidor de acceso de cliente**, indique el nombre de dominio completo (FQDN) del equipo donde está habilitado el rol **Acceso de cliente** de Microsoft Exchange Server.
   En Exchange 2016 y versiones posteriores, los servicios de acceso de cliente se instalan automáticamente como parte del rol de servidor Buzón de correo. Por lo tanto, puede especificar cualquier servidor que ejecute el **Rol de buzón de correo**. En adelante, en este apartado llamaremos CAS a este servidor.

© Acronis International GmbH, 2003-2025

6. En **Tipo de autenticación**, seleccione el tipo de autenticación utilizada por CAS. Puede seleccionar **Kerberos** (opción predeterminada) o **Básica**.
7. [Solo para una autenticación básica] Seleccione qué protocolo se debe utilizar. Puede seleccionar **HTTPS** (opción predeterminada) o **HTTP**.
8. [Solo para una autenticación básica con el protocolo HTTPS] Si CAS utiliza un certificado SSL obtenido de una entidad de certificación y desea que el software compruebe el certificado al conectarse a CAS, active la casilla de verificación **Comprobar certificado SSL**. De lo contrario, omita este paso.
9. Proporcione las credenciales de la cuenta que se utilizará para acceder a CAS. Los requisitos de esta cuenta aparecen en la sección Derechos de usuario necesarios.
10. Haga clic en **Agregar**.

Como resultado, los buzones de correo aparecen bajo **Dispositivos** > **Microsoft Exchange** > **Buzones de correo**.

Selección de los buzones de correo de Exchange Server

Seleccione los buzones de correo tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Para seleccionar buzones de correo de Exchange

1. Haga clic en **Dispositivos** > **Microsoft Exchange**.
   El software muestra el árbol de bases de datos y buzones de correo de Exchange.
2. Haga clic en **Buzones de correo** y después seleccione los buzones de correo de los que desee realizar una copia de seguridad.
3. Haga clic en **Proteger**.

Derechos de usuario necesarios

Para acceder a estos buzones de correo, Agente para Exchange necesita una cuenta con los derechos apropiados. Se le pedirá que especifique esta cuenta al configurar varias operaciones con buzones de correo.

Si la cuenta pertenece al grupo de funciones **Gestión de la organización**, podrá acceder a cualquier buzón de correo, incluidos aquellos que se creen en el futuro.

Los derechos de usuario mínimos necesarios son los siguientes:

- La cuenta debe pertenecer a los grupos de roles **Gestión de servidores** y **Gestión de destinatarios**.
- La cuenta debe tener activada la función de gestión **ApplicationImpersonation** para todos los usuarios o grupos de usuarios a cuyos buzones de correo accederá el agente.
  Para obtener más información sobre cómo configurar la función de gestión **ApplicationImpersonation**, consulte el siguiente artículo de la Microsoft Knowledge Base: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

© Acronis International GmbH, 2003-2025

Recuperación de bases de datos SQL

Puede recuperar bases de datos de SQL desde copias de seguridad de bases de datos y desde bases de datos con información de aplicaciones. Para obtener más información sobre la diferencia entre los dos tipos de copias de seguridad, consulte "Protección de Microsoft SQL Server y Microsoft Exchange Server" (p. 792).

Puede recuperar bases de datos de SQL en la instancia original, en una instancia diferente en el equipo original o en una instancia en un equipo distinto al original. Cuando lleva a cabo la recuperación en un equipo no original, el Agente para SQL debe estar instalado en el equipo de destino.

Asimismo, puede recuperar bases de datos como archivos.

Si usa la autenticación de Windows para la instancia de SQL, deberá proporcionar las credenciales de una cuenta que sea miembro del grupo **Operadores de copia de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en la instancia de destino. Si usa la autenticación de SQL Server, deberá proporcionar las credenciales de una cuenta que sea miembro de la función **administrador del sistema** en la instancia de destino.

Las bases de datos del sistema se recuperan como bases de datos de usuario, con algunas distinciones. Para obtener más información acerca de estas distinciones, consulte "Recuperación de bases de datos del sistema" (p. 816).

Durante una recuperación, puede comprobar el progreso de la operación en la consola de Cyber Protect, en la pestaña **Supervisión** > **Actividades**.

Recuperación de las bases de datos de SQL en un equipo original

Puede recuperar bases de datos de SQL en una instancia original, en una instancia diferente en el equipo original o en una instancia en un equipo de destino distinto al original.

Pasos para recuperar las bases de datos de SQL en un equipo original

A partir de una copia de seguridad de base de datos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Microsoft SQL**.
2. Seleccione la instancia de SQL Server o haga clic en el nombre de la instancia para seleccionar bases de datos específicas que desea recuperar y, a continuación, haga clic en **Recuperación**.
   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Para recuperar los datos a un equipo no original, consulte "Recuperación de las bases de datos de SQL en un equipo que no sea original" (p. 811).
3. Seleccione un punto de recuperación.
   Los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Bases de datos en una instancia**.
   De manera predeterminada, la instancia y las bases de datos se recuperan en las originales. También puede recuperar una base de datos original como una nueva base de datos.

© Acronis International GmbH, 2003-2025

5. [Al recuperar una instancia no original en el mismo equipo] Haga clic en **Instancia de SQL Server de destino**, seleccione la instancia de destino y haga clic en **Listo**.
6. [Al recuperar una base de datos como una nueva] Haga clic en el nombre de la base de datos y, a continuación, en **Recuperar a**, seleccione **Nueva base de datos**.
   - Especifique el nuevo nombre de la base de datos.
   - Especifique la ruta de la nueva base de datos.
   - Especifique la ruta del registro.
7. [Opcional] [No disponible en la recuperación de una base de datos como nueva base de datos] Para cambiar el estado de la base de datos después de la recuperación, haga clic en el nombre de la base de datos, elija uno de los siguientes estados y haga clic en **Listo**.
   - **Listo para su uso (RESTAURAR CON RECUPERACIÓN)** (opción predeterminada)

     Una vez que se complete la recuperación, la base de datos estará lista para su uso. Los usuarios tendrán el acceso total. El software revertirá todas las transacciones no confirmadas de la base de datos recuperada que se guardaron en los registros de las transacciones. No se podrán recuperar los registros de transacciones adicionales desde las copias de seguridad nativas de Microsoft SQL.
   - **No funcional (RESTAURACIÓN SIN RECUPERACIÓN)**

     Una vez que se haya completado la recuperación, la base de datos dejará de ser operativa. Los usuarios no podrán tener acceso a ella. El software conservará todas las transacciones no confirmadas de la base de datos recuperada. No se podrán recuperar los registros de transacciones adicionales desde las copias de seguridad nativas de Microsoft SQL y así alcanzar el punto de recuperación necesario.
   - **Solo lectura (RESTAURACIÓN EN ESPERA)**

     Una vez que se completa la recuperación, los usuarios tendrán un acceso de solo lectura a la base de datos. El software deshará todas las transacciones no confirmadas. Sin embargo, guardará las acciones deshechas en un archivo temporal en espera, de manera que se puedan revertir los efectos de la recuperación.

     Este valor se utiliza principalmente para detectar el momento específico en que se produjo un error en SQL Server.
8. Haga clic en **Iniciar recuperación**.

A partir de una copia de seguridad compatible con la aplicación

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo que contenía originalmente los datos que desea recuperar y haga clic en **Recuperación**.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Para recuperar los datos a un equipo no original, consulte "Recuperación de las bases de datos de SQL en un equipo que no sea original" (p. 811).
3. Seleccione un punto de recuperación.

   Los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Bases de datos SQL**.

© Acronis International GmbH, 2003-2025

5. Seleccione la instancia de SQL Server o haga clic en el nombre de la instancia para seleccionar bases de datos específicas que desea recuperar y, a continuación, haga clic en **Recuperar**.
   De manera predeterminada, la instancia y las bases de datos se recuperan en las originales. También puede recuperar una base de datos original como una nueva base de datos.
6. [Al recuperar una instancia no original en el mismo equipo] Haga clic en **Instancia de SQL Server de destino**, seleccione la instancia de destino y haga clic en **Listo**.
7. [Al recuperar una base de datos como una nueva] Haga clic en el nombre de la base de datos y, a continuación, en **Recuperar a**, seleccione **Nueva base de datos**.
   - Especifique el nuevo nombre de la base de datos.
   - Especifique la ruta de la nueva base de datos.
   - Especifique la ruta del registro.
8. [Opcional] [No disponible en la recuperación de una base de datos como nueva base de datos] Para cambiar el estado de la base de datos después de la recuperación, haga clic en el nombre de la base de datos, elija uno de los siguientes estados y haga clic en **Listo**.
   - **Listo para su uso (RESTAURAR CON RECUPERACIÓN)** (opción predeterminada)
     Una vez que se complete la recuperación, la base de datos estará lista para su uso. Los usuarios tendrán el acceso total. El software revertirá todas las transacciones no confirmadas de la base de datos recuperada que se guardaron en los registros de las transacciones. No se podrán recuperar los registros de transacciones adicionales desde las copias de seguridad nativas de Microsoft SQL.
   - **No funcional (RESTAURACIÓN SIN RECUPERACIÓN)**
     Una vez que se haya completado la recuperación, la base de datos dejará de ser operativa. Los usuarios no podrán tener acceso a ella. El software conservará todas las transacciones no confirmadas de la base de datos recuperada. No se podrán recuperar los registros de transacciones adicionales desde las copias de seguridad nativas de Microsoft SQL y así alcanzar el punto de recuperación necesario.
   - **Solo lectura (RESTAURACIÓN EN ESPERA)**
     Una vez que se completa la recuperación, los usuarios tendrán un acceso de solo lectura a la base de datos. El software deshará todas las transacciones no confirmadas. Sin embargo, guardará las acciones deshechas en un archivo temporal en espera, de manera que se puedan revertir los efectos de la recuperación.
     Este valor se utiliza principalmente para detectar el momento específico en que se produjo un error en SQL Server.
9. Haga clic en **Iniciar recuperación**.

Recuperación de las bases de datos de SQL en un equipo que no sea original

Puede recuperar copia de seguridad con información de aplicaciones y copias de seguridad de bases de datos en instancia de SQL Server de equipos de destino que no sean los originales en los cuales esté instalado Agente para SQL. Las copias de seguridad deben localizarse en el almacenamiento en la nube o en un almacenamiento compartido al que el equipo de destino pueda acceder.

© Acronis International GmbH, 2003-2025

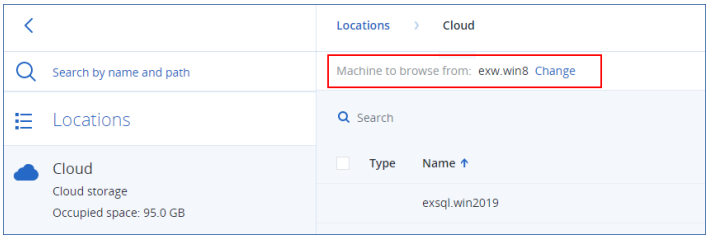
La versión de SQL Server en el equipo de destino debe ser la misma que la versión del equipo de origen o una más nueva.

Pasos para recuperar las bases de datos de SQL en un equipo que no sea original

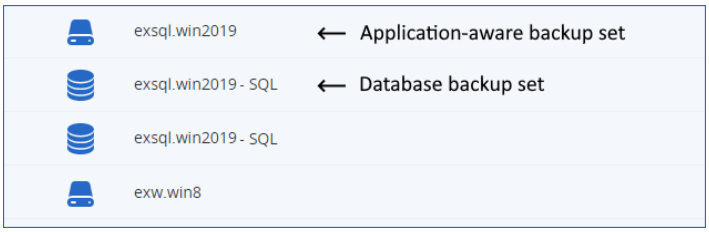
Desde el almacenamiento de copias de seguridad

Este procedimiento se aplica a copias de seguridad con información de aplicaciones y copias de seguridad de bases de datos.

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación del conjunto de copias de seguridad desde donde desea recuperar los datos.
3. En **Equipo desde el cual examinar**, seleccione el equipo de destino.
   Este es el equipo en el que se recuperarán los datos. El equipo de destino deben estar conectado.



4. Seleccione el conjunto de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad** en el panel **Acciones**.
   Los conjuntos de copias de seguridad con información de aplicaciones y los de copias de seguridad de la base de datos tienen iconos diferentes.



5. Seleccione el punto de recuperación desde donde desea recuperar los datos.
6. [Para las copias de seguridad de la base de datos] Haga clic en **Recuperar bases de datos SQL**.
7. [Para las copias de seguridad con información de aplicaciones] Haga clic en **Recuperar** > **Bases de datos SQL**.
8. Seleccione la instancia de SQL Server o haga clic en el nombre de la instancia para seleccionar bases de datos específicas que desea recuperar y, a continuación, haga clic en **Recuperar**.
9. [Si hay más de una instancia de SQL en el equipo de destino] Haga clic en **Instancia de SQL Server de destino**, seleccione la instancia de destino y haga clic en **Listo**.
10. Haga clic en el nombre de la base de datos, especifique la ruta de la nueva base de datos y la ruta de registro y, a continuación, haga clic en **Listo**.
    Puede especificar la misma ruta en ambos campos, por ejemplo:

© Acronis International GmbH, 2003-2025

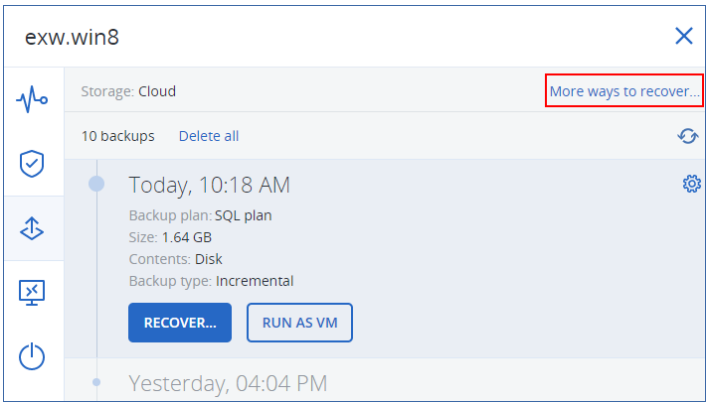
```
C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
```

11. Haga clic en **Iniciar recuperación**.

Desde Dispositivos

Este procedimiento se aplica solo a copias de seguridad con información de aplicaciones.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo que contenía originalmente los datos que desea recuperar y haga clic en **Recuperación**.
3. [Si el equipo de origen está en línea] Haga clic en **Otras formas de recuperar**.



4. Haga clic en **Seleccionar equipo** para seleccionar el equipo de destino y, a continuación, haga clic en **OK**.

   Este es el equipo en el que se recuperarán los datos. El equipo de destino deben estar conectado.
5. Seleccione un punto de recuperación.

   Los puntos de recuperación se filtran por ubicación.
6. Haga clic en **Recuperar** > **Bases de datos SQL**.
7. Seleccione la instancia de SQL Server o haga clic en el nombre de la instancia para seleccionar bases de datos específicas que desea recuperar y, a continuación, haga clic en **Recuperar**.
8. [Si hay más de una instancia de SQL en el equipo de destino] Haga clic en **Instancia de SQL Server de destino**, seleccione la instancia de destino y haga clic en **Listo**.
9. Haga clic en el nombre de la base de datos, especifique la ruta de la nueva base de datos y la ruta de registro y, a continuación, haga clic en **Listo**.

   Puede especificar la misma ruta en ambos campos, por ejemplo:

```
C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
```

10. Haga clic en **Iniciar recuperación**.

© Acronis International GmbH, 2003-2025

Recuperación de bases de datos de SQL como archivos

Puede recuperar bases de datos como archivos. Esta opción puede serle útil si necesita extraer datos para minería de datos, controles u otros procesamientos con herramientas de terceros. Para saber cómo conectar los archivos de la base de datos SQL a una instancia de SQL Server, consulte "Adjuntar bases de datos de SQL Server" (p. 817).

Puede recuperar bases de datos como archivos en el equipo original o en equipos de destino que no sean los originales en los cuales esté instalado Agente para SQL. Cuando recupere datos en equipos que no sean los originales, las copias de seguridad deben localizarse en el almacenamiento en la nube o en un almacenamiento compartido al que el equipo de destino pueda acceder.

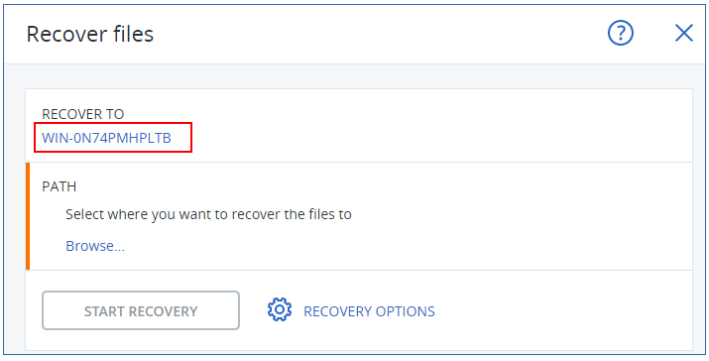
Nota
Si utiliza Agente para VMware (Windows), el único método de recuperación disponible será la recuperación de bases de datos como archivos. No se puede usar Agente para VMware (dispositivo virtual) para recuperar bases de datos.

Para recuperar bases de datos SQL como archivos

A partir de una copia de seguridad de base de datos

Este procedimiento se aplica a los equipos de origen en línea.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Microsoft SQL**.
2. Seleccione las bases datos que desea recuperar y, a continuación, haga clic en **Recuperación**.
3. Seleccione un punto de recuperación.
   Los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Bases de datos como archivos**.
5. [Al recuperar en un equipo no original] En **Recuperar a**, seleccione el equipo de destino.
   Este es el equipo en el que se recuperarán los datos. El equipo de destino deben estar conectado.
   Para cambiar la selección, haga clic en el nombre del equipo, seleccione otro equipo y, a continuación, haga clic en **Aceptar**.



6. En **Ruta**, haga clic en **Examinar**, seleccione una carpeta local o de red en que guardar los

© Acronis International GmbH, 2003-2025

archivos y, a continuación, haga clic en **Listo**.

7. Haga clic en **Iniciar recuperación**.

A partir de una copia de seguridad compatible con la aplicación

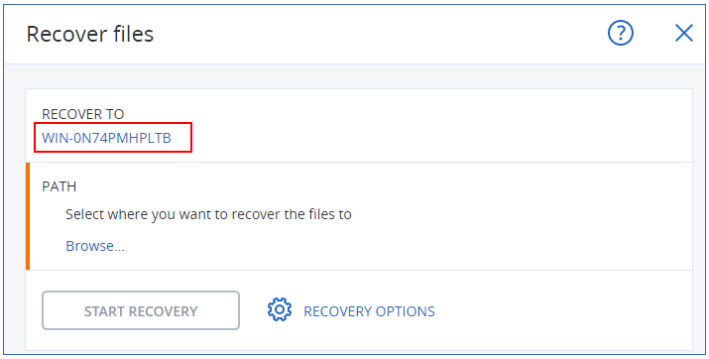
Este procedimiento se aplica a los equipos de origen en línea.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo que contenía originalmente los datos que desea recuperar y haga clic en **Recuperación**.
3. Seleccione un punto de recuperación.

   Los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Bases de datos SQL**, seleccione las bases de datos que desea recuperar y, a continuación, haga clic en **Recuperar como archivos**.
5. [Al recuperar en un equipo no original] En **Recuperar a**, seleccione el equipo de destino.

   Este es el equipo en el que se recuperarán los datos. El equipo de destino deben estar conectado.

   Para cambiar la selección, haga clic en el nombre del equipo, seleccione otro equipo y, a continuación, haga clic en **Aceptar**.



6. En **Ruta**, haga clic en **Examinar**, seleccione una carpeta local o de red en que guardar los archivos y, a continuación, haga clic en **Listo**.
7. Haga clic en **Iniciar recuperación**.

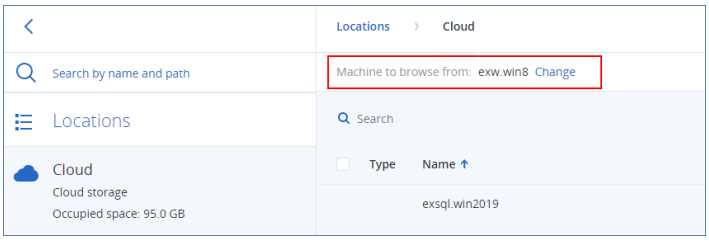
Desde una copia de seguridad en un equipo offline

Este procedimiento se aplica a copias de seguridad con información de aplicaciones y copias de seguridad de bases de datos en equipos de origen que están offline.

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación del conjunto de copias de seguridad desde donde desea recuperar los datos.
3. En **Equipo desde el cual examinar**, seleccione el equipo de destino.

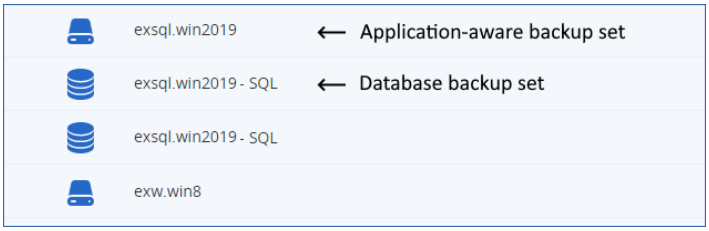
   Este es el equipo en el que se recuperarán los datos. El equipo de destino deben estar conectado.

© Acronis International GmbH, 2003-2025



4. Seleccione el conjunto de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad** en el panel **Acciones**.

   Los conjuntos de copias de seguridad con información de aplicaciones y los de copias de seguridad de la base de datos tienen iconos diferentes.



5. Seleccione el punto de recuperación desde donde desea recuperar los datos.
6. [Para las copias de seguridad de la base de datos] Haga clic en **Recuperar bases de datos SQL**.
7. [Para las copias de seguridad con información de aplicaciones] Haga clic en **Recuperar** > **Bases de datos SQL**.
8. Seleccione la instancia de SQL Server o haga clic en el nombre de la instancia para seleccionar bases de datos específicas que desea recuperar y, a continuación, haga clic en **Recuperar como archivos**.
9. En **Ruta**, haga clic en **Examinar**, seleccione una carpeta local o de red en que guardar los archivos y, a continuación, haga clic en **Listo**.
10. Haga clic en **Iniciar recuperación**.

Recuperación de bases de datos del sistema

Todas las bases de datos del sistema de una instancia se recuperan a la vez. Cuando se recuperan bases de datos del sistema, el software reinicia automáticamente la instancia de destino en el modo de usuario único. Una vez que se completa la recuperación, el software reinicia la instancia y recupera las demás bases de datos (si las hubiera).

Otros aspectos que debe tener en cuenta cuando se recuperan bases de datos del sistema:

- Las bases de datos del sistema únicamente se pueden recuperar en una instancia de la misma versión que la instancia original.
- Las bases de datos del sistema siempre se recuperan en el estado «listo para su uso».

Recuperación de la base de datos maestra

Las bases de datos del sistema incluyen la base de datos **maestra**. La base de datos **maestra** registra información sobre todas las bases de datos de la instancia. Por lo tanto, la base de datos

© Acronis International GmbH, 2003-2025

maestra de una copia de seguridad contiene información sobre las bases de datos, la cual ya existía en la instancia al momento de realizar la copia de seguridad. Es posible que después de recuperar la base de datos **maestra** deba realizar lo siguiente:

- Las bases de datos que aparecieron en la instancia después de realizar la copia de seguridad no se pueden visualizar en la instancia. Para recuperar esas bases de datos, adjúntelas a la instancia manualmente usando SQL Server Management Studio.
- Las bases de datos que se eliminaron en la instancia después de realizar la copia de seguridad se muestran sin conexión en la instancia. Elimine estas bases de datos mediante SQL Server Management Studio.

Adjuntar bases de datos de SQL Server

Esta sección describe cómo adjuntar una base de datos en SQL Server utilizando SQL Server Management Studio. Solo se puede adjuntar una base de datos por vez.

Adjuntar una base de datos requiere uno de los siguientes permisos: **CREAR BASE DE DATOS**, **CREAR CUALQUIER BASE DE DATOS** o **MODIFICAR CUALQUIER BASE DE DATOS**. Generalmente, estos permisos se conceden al rol de la instancia **sysadmin**.

Para adjuntar una base de datos

1. Ejecute Microsoft SQL Server Management Studio.
2. Conéctese a la instancia de SQL Server necesaria y después expanda la instancia.
3. Haga clic con el botón derecho en **Bases de datos** y luego en **Adjuntar**.
4. Haga clic en **Agregar**.
5. En el cuadro de diálogo **Localizar archivos de la base de datos**, busque y seleccione el archivo .mdf de la base de datos.
6. En la sección **Detalles de la base de datos**, asegúrese de que se encuentre el resto de los archivos de la base de datos (archivos .ndf y .ldf).

   Detalles. Quizás los archivos de la base de datos de SQL Server no se puedan encontrar automáticamente si:
   - No están en la ubicación predeterminada o no están en la misma carpeta que el archivo de la base de datos principal (.mdf). Solución: Especifique manualmente la ruta hasta los archivos necesarios en la columna **Ruta actual del archivo**.
   - Recuperó un conjunto incompleto de archivos que forman la base de datos. Solución: Recupere los archivos de la base de datos de SQL Server faltantes desde la copia de seguridad.
7. Cuando se hayan encontrado todos los archivos, haga clic en **Aceptar**.

Recuperación de bases de datos de Exchange

En esta sección se describe la recuperación desde copias de seguridad de bases de datos y desde copias de seguridad compatibles con la aplicación.

© Acronis International GmbH, 2003-2025

Puede recuperar datos de Exchange Server en un servidor de Exchange activo. Puede ser el servidor de Exchange original o un servidor de Exchange de la misma versión que se ejecute en el equipo que tenga el mismo nombre de dominio completo (FQDN). Agente para Exchange debe estar instalado en el equipo de destino.

La siguiente tabla resume los datos de Exchange Server que puede seleccionar para recuperar y los permisos de usuario mínimos que se requieren para recuperar los datos.

Versión de Exchange	Elementos de los datos	Permisos de usuario
2007	Grupos de almacenamiento	Asociación en el grupo de funciones **Administradores de organización de Exchange**.
2010/2013/2016/2019	Bases de datos	Pertenencia al grupo de funciones **Administración de servidores**.

También tiene la opción de recuperar las bases de datos (grupos de almacenamiento) como archivos. Los archivos de bases de datos, junto con los archivos de registro de transacción, se extraerán de la copia de seguridad a la carpeta que especifique. Esta opción puede serle útil si necesita extraer información para un control o procesos futuros con herramientas adicionales, o cuando la recuperación falle por alguna razón y necesite una solución para montar las bases de datos manualmente.

Si solo usa Agente para VMware (Windows), el único método de recuperación disponible será la recuperación de bases de datos como archivos. No se puede usar Agente para VMware (dispositivo virtual) para recuperar bases de datos.

Nos referiremos tanto a las bases de datos como a los grupos de almacenamiento como "bases de datos" en estos procedimientos.

Para recuperar bases de datos de Exchange a un servidor activo de Exchange Server

1. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione las bases de datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo

© Acronis International GmbH, 2003-2025

conectado que tenga instalado Agente para Exchange y seleccione un punto de recuperación.

- Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación de datos de Exchange.

4. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Bases de datos de Exchange**, seleccione las bases de datos que desea recuperar y, a continuación, haga clic en **Recuperar**.
   - Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar** > **Bases de datos a un servidor de Exchange**.
5. De manera predeterminada, las bases de datos se recuperan en las originales. Si no existe la base de datos original, se volverá a crear.

   Para recuperar una base de datos como una diferente:

   a. Haga clic en el nombre de la base de datos.

   b. Seleccione **Nueva base de datos** en **Recuperar a**.

   c. Especifique el nuevo nombre de la base de datos.

   d. Especifique la nueva ruta de la base de datos y la ruta de acceso. La carpeta que especifique no debe contener la base de datos original ni los archivos de registro.
6. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña Actividades.

Para recuperar los bases de datos como archivos de Exchange

1. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione las bases de datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para Exchange o Agent for VMware, y seleccione un punto de recuperación.

© Acronis International GmbH, 2003-2025

- Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación de datos de Exchange.

4. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Bases de datos de Exchange**, seleccione las bases de datos que desea recuperar y, a continuación, haga clic en **Recuperar como archivos**.
   - Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar** > **Bases de datos como archivos**.
5. Haga clic en **Examinar** y, a continuación, seleccione una carpeta local o de red en que guardar los archivos.
6. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña Actividades.

Montaje de bases de datos de Exchange Server

Después de recuperar los archivos de bases de datos, puede conectar las bases de datos al montarlas. El montaje se realiza por medio de la consola de gestión de Exchange, Exchange System Manager o Exchange Management Shell.

Las bases de datos recuperadas se encontrarán en el estado de Cierre con errores. Una base de datos que se encuentra en el estado de Cierre con errores puede montarse por medio del sistema si se recupera en su ubicación original (es decir, la información sobre la base de datos original está presente en Active Directory). Cuando se recupera una base de datos en una ubicación alternativa, (como una base de datos nueva o como la base de datos de recuperación), la base de datos no se puede montar hasta que se encuentre en el estado de Cierre correcto; para ello se utiliza el comando `Eseutil /r <Enn>`. `<Enn>` especifica el prefijo del archivo de registro para la base de datos (o el grupo de almacenamiento que contiene la base de datos) a la cual debe aplicar los archivos de registro de transacciones.

La cuenta que usa para adjuntar una base de datos debe tener asignado un rol de Administrador de Exchange Server y un grupo de administradores locales para el servidor de destino.

Para obtener información sobre cómo montar las bases de datos, consulte los siguientes artículos:

- Exchange 2010 o versiones posteriores: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/es-es/library/aa998871(v=EXCHG.80).aspx

© Acronis International GmbH, 2003-2025

Recuperación de elementos de buzón de correo y de buzones de correo de Exchange

Puede recuperar elementos de buzón de correo y de buzones de correo de Exchange desde las siguientes copias de seguridad:

- Copias de seguridad de bases de datos (incluidas las copias de seguridad de DAG)
- Copias de seguridad con información de aplicaciones
- Copias de seguridad de buzones de correo

Puede recuperar los siguientes elementos:

- Buzones de correo (salvo los buzones de correo de archivo)
- Carpetas públicas

Nota
Disponible solo desde copias de seguridad de bases de datos. Consulte "Seleccionar datos de Exchange Server" (p. 798).

- Elementos de la carpeta pública
- Carpetas de correo electrónico
- Mensajes de correo electrónico
- Eventos del calendario
- Tareas
- Contactos
- Entradas del diario
- Notas

Puede usar la búsqueda para localizar los elementos.

Los buzones de correo o elementos de los buzones de correo pueden recuperarse a un servidor activo de Exchange Server o a Microsoft 365.

Recuperación a Exchange Server

La recuperación granular se puede realizar en Microsoft Exchange Server 2010 Service Pack 1 (SP1) y versiones posteriores. La copia de seguridad de origen puede contener bases de datos o buzones de correo de cualquier versión compatible de Exchange.

La recuperación granular la pueden realizar Agente para Exchange o Agente para VMware (Windows). La aplicación Exchange Server de destino y el equipo donde se ejecute el agente deben pertenecer al mismo bosque de Active Directory.

© Acronis International GmbH, 2003-2025

Cuando se recupera un buzón de correo sobre un buzón de correo existente, los elementos anteriores que tengan los mismos ID se sobrescriben.

Al recuperar elementos de buzón de correo no se sobrescribe nada. En su lugar, en la carpeta de destino se reproduce la ruta completa al elemento del buzón de correo.

Requisitos para las cuentas de usuario

Un buzón de correo que se recupera desde una copia de seguridad debe tener una cuenta de usuario asociada en Active Directory.

Los buzones de correo del usuario y su contenido solo pueden recuperarse si las cuentas de usuario asociadas están *habilitadas*. Los buzones de correo compartidos, de sala y equipo pueden recuperarse solo si sus cuentas de usuario asociadas están *deshabilitadas*.

Un buzón de correo que no cumpla con las condiciones anteriores se omitirá durante la recuperación.

Si se omiten algunos buzones de correo, la recuperación finalizará correctamente con advertencias. Si se omiten todos los buzones de correo, la recuperación fallará.

Recuperar a Microsoft 365

La recuperación de elementos de datos de Exchange a Microsoft 365 y viceversa es compatible siempre que se haya instalado localmente el Agente para Microsoft 365.

La recuperación puede realizarse desde copias de seguridad de Microsoft Exchange Server 2010 y versiones posteriores.

Cuando se recupera un buzón de correo a un buzón de Microsoft 365 existente, los elementos anteriores se mantienen intactos y los elementos recuperados se colocan junto a ellos.

Si recupera un único buzón de correo, deberá seleccionar el buzón de Microsoft 365 de destino. Si recupera varios buzones de correo en una única operación de recuperación, el software intentará recuperar cada buzón de correo al buzón del usuario que tenga el mismo nombre. Si no se encuentra un usuario con estas características, se omite el buzón de correo. Si se omiten algunos buzones de correo, la recuperación finalizará correctamente con advertencias. Si se omiten todos los buzones de correo, la recuperación fallará.

Para obtener más información sobre la recuperación Microsoft 365, consulte "Protección de los datos de Microsoft 365" (p. 833).

Recuperación de buzones de correo

Para recuperar buzones de correo a partir de una copia de seguridad compatible con la aplicación o una copia de seguridad de base de datos

1. [Solo al recuperar desde una copia de seguridad de base de datos a Microsoft 365] Si el Agente para Microsoft 365 no está instalado en la máquina que ejecuta Exchange Server y de la que se ha realizado la copia de seguridad, haga una de las acciones siguientes:

© Acronis International GmbH, 2003-2025

- Si no tiene el Agente para Microsoft 365 en su organización, instale el Agente para Microsoft 365 en la máquina de la que se ha realizado la copia de seguridad (u otra máquina con la misma versión de Microsoft Exchange Server).
- Si ya tiene el Agente para Microsoft 365 en su organización, copie las bibliotecas desde la máquina de la que se ha realizado la copia de seguridad (o desde otra máquina con la misma versión de Microsoft Exchange Server) a la máquina con el Agente para Microsoft 365, como se describe en "Copia de bibliotecas de Microsoft Exchange Server" (p. 827).

2. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione la base de datos que contenía originalmente los datos que desea recuperar.
3. Haga clic en **Recuperación**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Use otros métodos de recuperación:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para Exchange o Agent for VMware, y seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

   El equipo elegido para examinar en cualquiera de las acciones anteriores realizará la recuperación en lugar del equipo original que está desconectado.
5. Haga clic en **Recuperar** > **Buzones de correo de Exchange**.
6. Seleccione los buzones de correo que desea recuperar.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.
7. Haga clic en **Recuperar**.
8. [Solo al recuperar a Microsoft 365]:
   a. En **Recuperar a**, seleccione **Microsoft 365**.
   b. [Si solo ha seleccionado un buzón de correo en el paso 6] En **Buzón de correo de destino**, especifique el buzón de correo de destino.
   c. Haga clic en **Iniciar recuperación**.

   No se requieren más pasos para este procedimiento.
9. Haga clic en **Equipo de destino con Microsoft Exchange Server** para seleccionar o cambiar el equipo de destino. Este paso permite recuperar en un equipo que no esté ejecutando Agente para Exchange.

© Acronis International GmbH, 2003-2025

Especifique el nombre de dominio completo (FQDN) de un equipo en el que esté habilitado el rol **Acceso de cliente** (en Microsoft Exchange Server 2010/2013) o el **rol Buzón de correo** (en Microsoft Exchange Server 2016 o versiones posteriores). El equipo debe pertenecer al mismo bosque de Active Directory que el equipo que realiza la recuperación.

Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo. Los requisitos de esta cuenta aparecen en "Derechos de usuario necesarios" (p. 808).

10. [Opcional] Haga clic en **Base de datos para volver a crear buzones de correo faltantes** para cambiar la base de datos seleccionada automáticamente.
11. Haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Para recuperar un buzón de correo desde una copia de seguridad de buzón de correo

1. Haga clic en **Dispositivos** > **Microsoft Exchange** >**Buzones de correo**.
2. Seleccione el buzón de correo que desea recuperar y, a continuación, haga clic en **Recuperación**.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.

   Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Buzón de correo**.
5. Siga los pasos 8 a 11 del procedimiento anterior.

Recuperación de elementos de buzón de correo

Para recuperar elementos de buzones de correo a partir de una copia de seguridad compatible con la aplicación o una copia de seguridad de base de datos

1. [Solo al recuperar desde una copia de seguridad de base de datos a Microsoft 365] Si el Agente para Microsoft 365 no está instalado en la máquina que ejecuta Exchange Server y de la que se ha realizado la copia de seguridad, haga una de las acciones siguientes:
   - Si no tiene el Agente para Microsoft 365 en su organización, instale el Agente para Microsoft 365 en la máquina de la que se ha realizado la copia de seguridad (u otra máquina con la misma versión de Microsoft Exchange Server).
   - Si ya tiene el Agente para Microsoft 365 en su organización, copie las bibliotecas desde la máquina de la que se ha realizado la copia de seguridad (o desde otra máquina con la misma versión de Microsoft Exchange Server) a la máquina con el Agente para Microsoft 365, como se describe en "Copia de bibliotecas de Microsoft Exchange".
2. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.

© Acronis International GmbH, 2003-2025

- Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione la base de datos que contenía originalmente los datos que desea recuperar.

3. Haga clic en **Recuperación**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Use otros métodos de recuperación:

   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para Exchange o Agent for VMware, y seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

   El equipo elegido para examinar en cualquiera de las acciones anteriores realizará la recuperación en lugar del equipo original que está desconectado.
5. Haga clic en **Recuperar** > **Buzones de correo de Exchange**.
6. Haga clic en el buzón de correo que contenía originalmente los elementos que desea recuperar.
7. Seleccione los elementos que desea recuperar.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

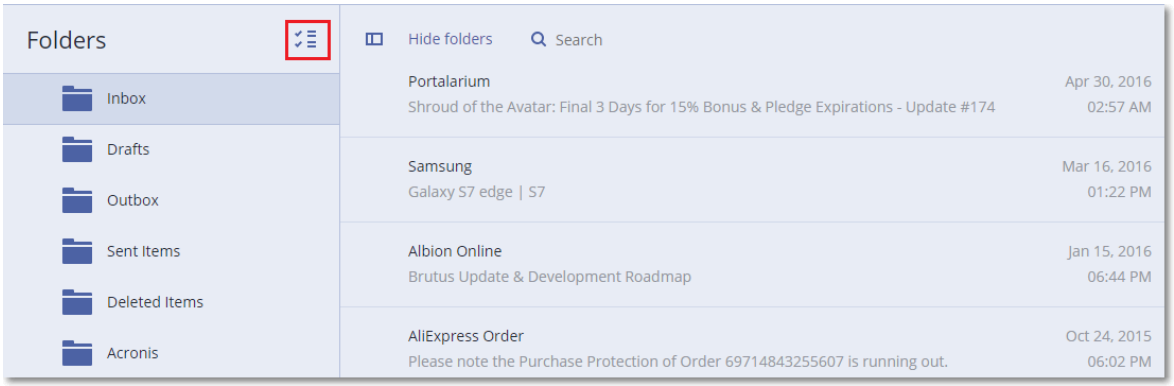
   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Mostrar contenido** para ver el contenido, incluidos los documentos adjuntos.

   Nota
   Haga clic en el nombre de un archivo adjunto para descargarlo.

   Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas.

© Acronis International GmbH, 2003-2025



8. Haga clic en **Recuperar**.
9. Para recuperar a Microsoft 365, seleccione **Microsoft 365** en **Recuperar a**.

   Para recuperar a un Exchange Server, mantenga el valor predeterminado de **Microsoft Exchange** en **Recuperar a**.
10. [Solo al recuperar a Exchange Server] Haga clic en **Equipo de destino con Microsoft Exchange Server** para seleccionar o cambiar el equipo de destino. Este paso permite recuperar en un equipo que no esté ejecutando Agente para Exchange.

    Especifique el nombre de dominio completo (FQDN) de un equipo en el que esté habilitado el rol **Acceso de cliente** (en Microsoft Exchange Server 2010/2013) o el **rol Buzón de correo** (en Microsoft Exchange Server 2016 o versiones posteriores). El equipo debe pertenecer al mismo bosque de Active Directory que el equipo que realiza la recuperación.

    Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo. Los requisitos de esta cuenta aparecen en "Derechos de usuario necesarios" (p. 808).
11. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.

    De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona un equipo de destino que no es el original, debe indicar el buzón de correo de destino.
12. [Solo al recuperar mensajes de correo electrónico] En **Carpeta de destino** puede consultar o cambiar la carpeta de destino en el buzón de correo de destino. De manera predeterminada, se selecciona la carpeta **Elementos recuperados**. Debido a las limitaciones de Microsoft Exchange, los eventos, las tareas, las notas y los contactos se restauran en su ubicación de origen independientemente de que se haya indicado cualquier otra **carpeta de destino**.
13. Haga clic en **Iniciar recuperación**.

Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Para recuperar un elemento del buzón de correo de una copia de seguridad de buzón de correo

1. Haga clic en **Dispositivos** > **Microsoft Exchange** >**Buzones de correo**.
2. Seleccione el buzón de correo que contenía originalmente los elementos que desea recuperar y, a continuación, haga clic en **Recuperación**.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.

© Acronis International GmbH, 2003-2025

Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
5. Seleccione los elementos que desea recuperar.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Mostrar contenido** para ver el contenido, incluidos los documentos adjuntos.

   Nota
   Haga clic en el nombre de un archivo adjunto para descargarlo.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Enviar como correo electrónico** para enviar el mensaje a una dirección de correo electrónico. El mensaje se envía desde el correo electrónico de su cuenta de administrador.

   Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 
6. Haga clic en **Recuperar**.
7. Siga los pasos 9 a 13 del procedimiento anterior.

Copia de bibliotecas de Microsoft Exchange Server

Al recuperar los buzones de correo de Exchange o los elementos de buzón de correo en Microsoft 365, puede que necesite copiar las bibliotecas siguientes desde la máquina de la que se ha realizado la copia de seguridad (o desde otra máquina con la misma versión de Microsoft Exchange Server) a la máquina con el Agente para Microsoft 365.

Copie los archivos siguientes, en función de la versión de Microsoft Exchange Server de la que se ha realizado la copia de seguridad.

Versión de Microsoft Exchange Server	Bibliotecas	Ubicación predeterminada
Microsoft Exchange Server 2010	`ese.dll` `esebcli2.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

© Acronis International GmbH, 2003-2025

	`store.exe`	
Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016 y 2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

Las bibliotecas deben ubicarse en la carpeta `%ProgramData%\Acronis\ese`. Si esta carpeta no existe, créela manualmente.

Cambio de las credenciales de acceso de SQL Server o Exchange Server

Puede cambiar las credenciales de acceso de SQL Server o Exchange Server sin tener que volver a instalar el agente.

Para cambiar las credenciales de acceso de SQL Server o Exchange Server

1. Haga clic en **Dispositivos** y, a continuación, en **Microsoft SQL** o **Microsoft Exchange**.
2. Seleccione el Grupo de disponibilidad de Always On, el Grupo de disponibilidad de base de datos, la instancia de SQL Server o el servidor de Exchange Server cuyas credenciales de acceso desee cambiar.
3. Haga clic en **Especificar credenciales**.
4. Especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Aceptar**.

Para cambiar las credenciales de acceso de Exchange Server para la copia de seguridad de buzón de correo

1. Haga clic en **Dispositivos** > **Microsoft Exchange** y expanda los **Buzones de correo**.
2. Seleccione el Exchange Server cuyas credenciales de acceso desee cambiar.
3. Haga clic en **Configuración**.
4. En **Cuenta de administrador de Exchange**, especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Guardar**.

Protección de dispositivos móviles

La aplicación Acronis Cyber Protect le permite hacer una copia de seguridad de sus datos móviles en el almacenamiento en la nube para recuperarlos en caso de pérdida o daños. Tenga en cuenta que la copia de seguridad en el almacenamiento en la nube requiere una cuenta y la suscripción a la nube.

© Acronis International GmbH, 2003-2025

Dispositivos móviles compatibles

Puede instalar la aplicación Acronis Cyber Protect en un dispositivo móvil que funcione con uno de los siguientes sistemas operativos:

- iOS 16 a iOS 18 (iPhone, iPod, iPad)
- Android 11 a Android 15

Importante
Para iniciar el proceso de copia de seguridad, debe iniciar la aplicación de forma manual.

De qué puede realizar una copia de seguridad

- Contactos (nombre, número de teléfono y correo electrónico)
- Fotografías (se conservará el tamaño y formato original de las fotografías)

  Nota
  En iOS, las fotografías en movimiento se restauran como imágenes fijas.

- Vídeos
- Calendarios
- Recordatorios (solo en dispositivos iOS)

Qué necesita saber

- Puede realizar una copia de seguridad de los datos solo en el almacenamiento en la cloud.
- Cuando abra la aplicación, verá el resumen de los cambios en los datos y podrá iniciar manualmente una copia de seguridad.
- La funcionalidad de **Copia de seguridad continua** está habilitada por defecto. Si esta configuración está activada, la aplicación Acronis Cyber Protect detecta automáticamente nuevos datos al instante y los sube a la nube.
- La opción **Usar solo Wi-Fi** está habilitada por defecto en la configuración de la aplicación. Si esta configuración está activada, la aplicación Acronis Cyber Protect respaldará sus datos solo cuando haya una conexión Wi-Fi disponible. Si se pierde la conexión Wi-Fi, no se iniciará el proceso de copia de seguridad. Para que la aplicación también use la conexión celular, desactive esta opción.
- La optimización de la batería de su dispositivo podría impedir el funcionamiento adecuado de la aplicación Acronis Cyber Protect. Para ejecutar las copias de seguridad a tiempo, debería detener la optimización de la batería para la aplicación.
- Existen dos métodos para ahorrar batería:
  - La funcionalidad de **Hacer copia de seguridad mientras se carga** está desactivada por defecto. Si esta configuración está activada, la aplicación Acronis Cyber Protect realizará una copia de seguridad de sus datos solo cuando su dispositivo esté conectado a una fuente de

© Acronis International GmbH, 2003-2025

alimentación. Cuando el dispositivo se desconecta de una fuente de alimentación durante un proceso de copia de seguridad continuo, la copia de seguridad se pausa.
    - El **Modo de ahorro de energía** está habilitado por defecto. Si esta configuración está activada, la aplicación Acronis Cyber Protect respaldará sus datos solo cuando la batería de su dispositivo no esté baja. Cuando la batería del dispositivo se agota, la copia de seguridad continua se pausa.
- Puede acceder a los datos de la copia de seguridad desde cualquier dispositivo móvil registrado en su cuenta. Esto le ayudará a transferir los datos desde un dispositivo móvil antiguo a uno nuevo. Los contactos y fotografías de un dispositivo Android pueden recuperarse en un dispositivo iOS y viceversa. También puede descargar una foto, un vídeo o un contacto en cualquier dispositivo mediante la consola de Cyber Protect.
- Los datos de los que realizó una copia de seguridad desde un dispositivo móvil registrado en su cuenta solo están disponibles en dicha cuenta. Nadie más puede ver o recuperar sus datos.
- En la aplicación Acronis Cyber Protect solo puede recuperar las versiones más recientes de los datos. Si necesita recuperar datos de una versión de copia de seguridad específica, use la consola de Cyber Protect en una tablet o un ordenador.
- No se aplican las reglas de retención a las copias de seguridad de dispositivos móviles.
- Solo para dispositivos Android: si hay una tarjeta SD presente durante la copia de seguridad, también se realizará una copia de seguridad de los datos almacenados en dicha tarjeta. Los datos se recuperarán en la carpeta **Recuperado por la copia de seguridad** de una tarjeta SD si está presente durante la recuperación. En caso contrario, la aplicación le solicitará que indique otra ubicación en la que recuperar los datos.

Dónde obtener la aplicación Acronis Cyber Protect

Según el tipo de dispositivo móvil que tenga, deberá instalar la aplicación desde el App Store o Google Play.

Cómo empezar a realizar copias de seguridad de los datos

1. Abra la aplicación.
2. Inicie sesión con los datos de su cuenta.
3. Toque **Configurar** para crear su copia de seguridad. Tenga en cuenta que este botón solo se muestra cuando no tiene ninguna copia de seguridad de su dispositivo móvil.
4. Seleccione las categorías de datos de las que desea realizar la copia de seguridad. De manera predeterminada, se seleccionan todas las categorías.
5. Paso opcional: habilite **Cifrar copia de seguridad** para proteger su copia de seguridad con cifrado. En ese caso, también deberá hacer lo siguiente:

© Acronis International GmbH, 2003-2025

a. Escriba una contraseña de cifrado en dos campos distintos.

Nota
Es importante que recuerde la contraseña, puesto que, si se le olvida, no podrá restaurarla ni cambiarla.

b. Pulse **Cifrar**.

6. Pulse **Crear copia de seguridad**.
7. Permita a la aplicación acceder a sus datos personales. Si deniega el acceso a algunas categorías de datos, estas no se incluirán en la copia de seguridad.

La copia de seguridad comienza.

Cómo recuperar los datos en un dispositivo móvil

Advertencia.
Para recuperar los datos en un dispositivo móvil, debe usar la cuenta de usuario final.

1. Abra la aplicación Acronis Cyber Protect.
2. Pulse **Examinar**.
3. Pulse el nombre del dispositivo.
4. Realice uno de los siguientes procedimientos:
   - Para recuperar todos los datos incluidos en la copia de seguridad, pulse **Recuperar todos**. No es necesario realizar más acciones.
   - Para recuperar una o más categorías de datos, pulse **Seleccionar** y después seleccione las casillas de verificación de las categorías elegidas. Pulse **Recuperar**. No es necesario realizar más acciones.
   - Para recuperar uno o más elementos que pertenecen a la misma categoría de datos, pulse la categoría de datos concreta. Continúe a los pasos siguientes.
5. Realice uno de los siguientes procedimientos:
   - Para recuperar un único elemento, púlselo.
   - Para recuperar varios elementos, pulse **Seleccionar** y después seleccione las casillas de verificación de los elementos elegidos.
6. Pulse **Recuperar**.

Cómo revisar los datos a través de la consola de Cyber Protect

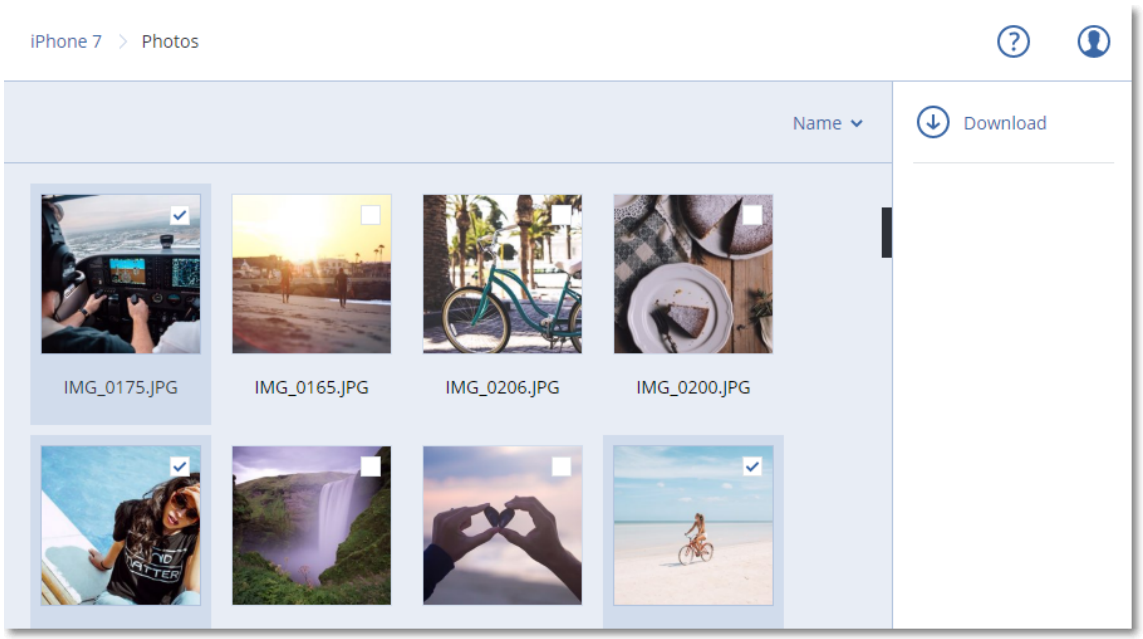
1. En un equipo, abra un explorador y escriba el URL de la consola de Cyber Protect.
2. Inicie sesión con los datos de su cuenta.
3. En **Todos los dispositivos**, haga clic en la opción **Recuperar** bajo el nombre de su dispositivo móvil.

© Acronis International GmbH, 2003-2025

4. Realice una de las siguientes operaciones:
   - Para descargar las fotografías, los vídeos, los contactos, los calendarios o los recordatorios del dispositivo, seleccione las categorías de datos correspondientes. Haga clic en **Descargar**.



   - Para descargar fotografías, vídeos, contactos, calendarios o recordatorios específicos, seleccione el nombre de la categoría de datos correspondiente y, después, marque las casillas de verificación de los elementos en cuestión. Haga clic en **Descargar**.



   - Para ver una vista preliminar de una fotografía o un contacto, seleccione el nombre de la categoría de datos correspondiente y, después, haga clic en el elemento elegido.

© Acronis International GmbH, 2003-2025

Protección de los datos de Microsoft 365

Las copias de seguridad periódicas de los datos de Microsoft 365 le proporcionan una capa de protección adicional frente a errores de los usuarios y acciones malintencionadas. Puede recuperar los elementos eliminados desde una copia de seguridad incluso después de que caduque el periodo de retención de Microsoft 365. Asimismo, puede conservar una copia local de los buzones de correo de Exchange Online si es necesario para cumplir la normativa.

Puede realizar copias de seguridad de los datos de Microsoft 365 mediante las siguientes soluciones que proporciona Cyber Protect Cloud:

- **Microsoft 365 Business (copia de seguridad)**
- **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**
- **Agente para Office 365** (agente instalado de forma local)

Para obtener más información sobre estas soluciones, consulte "Comparación de soluciones de copia de seguridad para datos de Microsoft 365" (p. 833).

Importante
Las acciones con recursos de la nube a la nube como ver el contenido de los correos electrónicos con copia de seguridad, descargar adjuntos o archivos, recuperar correos electrónicos de buzones de correo no originales o enviarlos como correos electrónicos podrían infringir la privacidad del usuario. Estas acciones se registran en **Supervisión** > **Registro de auditoría** en el portal de administración.

Comparación de soluciones de copia de seguridad para datos de Microsoft 365

Dependiendo de los servicios que estén habilitados para el inquilino de cliente, están disponibles las siguientes soluciones de copia de seguridad:

- **Microsoft 365 Business (copia de seguridad)**
- **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**
- **Agente para Office 365** (agente instalado de forma local)

Nota
Para los inquilinos en el modo de cumplimiento, solo está disponible el agente instalado de forma local. Estos inquilinos solo pueden realizar copias de seguridad de los buzones de correo de Microsoft 365. No pueden utilizar la funcionalidad ampliada que proporciona el agente en la nube.

Azure Information Protection (AIP) es compatible con todas las soluciones.

La siguiente tabla resume la funcionalidad de las soluciones de copia de seguridad.

© Acronis International GmbH, 2003-2025

Solución	Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365	Agente para Office 365
Tipo de agente	Agente en la nube • El agente de la nube proporciona funcionalidades de copia de seguridad extendidas, que son accesibles directamente en la consola de Cyber Protect • No se necesita instalación	Agente en la nube • El agente de la nube proporciona funcionalidades de copia de seguridad extendidas, que son accesibles directamente en la consola de Cyber Protect • No se necesita instalación	Agente local • El agente instalado de forma local solo proporciona copias de seguridad de los buzones de correo en línea de Exchange • El agente debe instalarse en un equipo Windows que esté conectado a Internet
Elementos de datos que se pueden incluir en copias de seguridad	• **Exchange Online**: ◦ buzones de correo de usuario y compartidos (incluidos los buzones de correo de usuarios en un plan de Kiosk y los buzones de correo en espera por asuntos legales) ◦ buzones de correo de grupo ◦ carpetas públicas • **OneDrive**: archivos y carpetas del usuario • **SharePoint Online**: ◦ sitios de comunicación clásicos ◦ sitios de grupo modernos ◦ sitios de datos individuales	• **Exchange Online**: ◦ buzones de correo de usuario • **OneDrive**: archivos y carpetas del usuario • **SharePoint Online**: ◦ sitios de comunicación clásicos ◦ sitios de grupo modernos	**Exchange Online:** buzones de correo de usuario y compartidos (incluidos los buzones de correo de usuarios en un plan de Kiosk y los buzones de correo en espera por asuntos legales)

© Acronis International GmbH, 2003-2025

Solución	Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365	Agente para Office 365
	• **Microsoft 365 Teams**: ◦ todos los equipos ◦ canales del equipo ◦ archivos del canal ◦ buzones de correo del equipo ◦ archivos y mensajes de correo electrónico en los buzones del equipo ◦ reuniones ◦ sitios del equipo • **Blocs de notas de OneNote**: como parte de las copias de seguridad de OneDrive, SharePoint Online y Microsoft 365 Teams		
Copia de seguridad de los buzones de correo electrónico comprimido (**archivo comprimido local**)	Sí	Sí	No
Programación de copia de seguridad	Hasta seis veces al día*	Cada 10 minutos	Definida por el usuario
Retención de copias de seguridad	Flexible: por fecha, número de copias de seguridad o ilimitado	Fijo • Para buzones de correo: un año de copias de seguridad frecuentes • Para cuentas de	Flexible: por fecha, número de copias de seguridad o ilimitado

© Acronis International GmbH, 2003-2025

Solución	Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365	Agente para Office 365
		OneDrive y sitios de SharePoint: un año, con dos semanas de copias de seguridad frecuentes y copias de seguridad semanales para el resto del período	
Ubicaciones de las copias de seguridad	Almacenamiento en la nube (incluido el almacenamiento alojado en partners)	Almacenamiento de copia de seguridad de Microsoft 365	Almacenamiento en la nube, o bien la carpeta local o de red
Resiliencia de la copia de seguridad	Se proporciona de forma estándar: los centros de datos de almacenamiento en la nube no se encuentran en la misma ubicación que los centros de datos de Microsoft	Replicación automática a otros contenedores de almacenamiento dentro de la red de Microsoft	No
Protección automática de sitios, grupos, usuarios y equipos de Microsoft 365	Sí, mediante la aplicación de un plan de protección a los grupos **Todos los usuarios**, **Todos los grupos**, **Todos los sitios** o **Todos los equipos**	Sí, mediante la aplicación de un plan de protección a **Todos los usuarios** y **Todos los grupos**, y **Todos los sitios**	No
Protección de más de una organización de Microsoft 365	Sí	Sí	No
Recuperación granular	Sí	No	Sí
Recuperación a otro usuario en la misma organización de	Sí	No	Sí

© Acronis International GmbH, 2003-2025

Solución	Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365	Agente para Office 365
Microsoft 365 dentro de la misma solución de copia de seguridad			
Recuperación a otra organización de Microsoft 365 en el mismo inquilino, dentro de la misma solución de copia de seguridad	Sí	No	No
Recuperación en un servidor de Microsoft Exchange local	No	No	No
Número máximo de elementos que se pueden incluir en copias de seguridad sin que se produzca ninguna degradación del rendimiento	Hasta 50 000 recursos informáticos protegidos por empresa**	N/D	Al realizar copias de seguridad en el almacenamiento en la nube: 5000 buzones de correo por empresa Al realizar copias de seguridad en otros destinos: 2000 buzones de correo por plan de protección (sin límite de número de buzones de correo por empresa)
Cantidad máxima de copias de seguridad ejecutadas manualmente	10 ejecuciones manuales durante una hora	N/D	Unlimited
Cantidad máxima de operación de recuperación simultáneas	10 operaciones, incluidas operaciones de recuperación de Google Workspace	N/D	Unlimited
Rendimiento	Velocidades típicas de	Copia de seguridad y	Velocidades típicas

© Acronis International GmbH, 2003-2025

Solución	Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365	Agente para Office 365
	la copia de seguridad y recuperación de la nube a la nube	recuperación más rápidas, sin limitación de datos	para copia de seguridad y recuperación

* Con las funciones estándar incluidas, la opción predeterminada es **Una vez por día**. Con el paquete de Advanced Backup, la opción predeterminada es **Dos veces por día**. Puede planificar hasta seis copias de seguridad por día. Las copias de seguridad se inician a intervalos aproximados en función de la carga actual del agente de la nube, que gestiona varios clientes en un centro de datos. De este modo, se garantiza una carga equilibrada durante el día y la misma calidad de servicio para todos los clientes.

Nota
La planificación de la protección puede verse afectada por el funcionamiento de servicios de terceros, por ejemplo, la accesibilidad a los servidores de Microsoft 365, la regulación de los ajustes de los servidores de Microsoft y otros. Consulte también la Guía de limitación de Microsoft Graph.

** El número máximo de recursos informáticos depende del tipo de recurso informático, tal y como sigue: 50 000 buzones de correo de Exchange o 10 000 equipos o 10 000 sitios de SharePoint o 5000 cuentas de OneDrive.

Para calcular las combinaciones admitidas, utilice la siguiente fórmula:

```
10 mailboxes = 2 teams = 2 sites = 1 OneDrive account
```

Por ejemplo:

- 50 000 buzones de correo
- 40 000 buzones de correo y 1000 cuentas de OneDrive
- 40 000 buzones de correo y 2000 sitios
- 40 000 buzones de correo y 2000 equipos
- 30 000 buzones de correo, 1000 cuentas de OneDrive, 1000 sitios y 1000 equipos
- 30 000 buzones de correo, 2000 sitios y 2000 equipos

Le recomendamos que realice la copia de seguridad de los recursos informáticos de forma secuencial y en el siguiente orden:

1. Buzones de correo
2. Cuentas de OneDrive

© Acronis International GmbH, 2003-2025

3. Teams
4. Sitios de SharePoint

La primera copia de seguridad completa puede tardar varios días, según la cantidad de elementos protegidos y su tamaño. No inicie la siguiente copia de seguridad hasta que la anterior esté completa.

Limitaciones

- La consola de Cyber Protect muestra todos los usuarios con un buzón de correo o una cuenta de OneDrive, incluidos los que no tienen una licencia de Microsoft 365 y los que tienen bloqueado el inicio de sesión en los servicios de Microsoft 365.
- Una copia de seguridad de un buzón de correo incluye solo las carpetas visibles para los usuarios. La carpeta **Elementos recuperables** y sus subcarpetas (**Eliminaciones**, **Versiones**, **Depuraciones**, **Auditorías**, **Retenciones**, **Registro del calendario**) no se incluyen en la copia de seguridad de un buzón de correo.
- No es posible crear automáticamente usuarios, carpetas públicas, grupos o sitios durante una recuperación. Por ejemplo, si quiere recuperar un sitio de SharePoint Online eliminado, cree primero un sitio manualmente y, a continuación, especifique que es el sitio de destino durante una recuperación.
- No puede recuperar elementos de diferentes puntos de recuperación de forma simultánea, incluso aunque pueda seleccionar esos elementos en los resultados de búsqueda.
- Durante la copia de seguridad, se conservará cualquier etiqueta confidencial que se aplique al contenido. Por ello, puede que el contenido confidencial no se muestre si se recupera a una ubicación que no es la original y su usuario tiene permisos de acceso diferentes.
- [Para **Microsoft 365 Business (copia de seguridad)**] Puede aplicar solo un plan de copias de seguridad individual a un recurso informático.
- [Para **Microsoft 365 Business (copia de seguridad)**] Cuando se aplican un plan de copias de seguridad individual y un plan de copias de seguridad en grupo al mismo recurso informático, la configuración del plan individual tiene prioridad.
- [Para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**] Puede crear y aplicar un plan de copias de seguridad por tipo de datos (buzones de correo de Exchange, sitios de SharePoint o cuentas de OneDrive).

Derechos de usuario necesarios

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)** y **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**.

El uso del agente de la nube requiere los siguientes derechos de usuario en Cyber Protect Cloud y en Microsoft 365.

© Acronis International GmbH, 2003-2025

En Cyber Protect Cloud

- Con **Microsoft 365 Business (copia de seguridad)**, el agente en la nube puede utilizarse tanto a nivel de inquilino de cliente como a nivel de la unidad. Para obtener más información sobre estos niveles y sus respectivos administradores, consulte "Administración de organizaciones de Microsoft 365 añadidas en diferentes niveles" (p. 843).
- Con **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**, el agente de la nube se puede utilizar a nivel de inquilino de cliente.
- El agente local debe registrarse con una cuenta de administrador de la empresa y utilizarse en el nivel de inquilino del cliente. Los administradores de la empresa que actúen a nivel de la unidad, los administradores de la unidad y los usuarios no pueden realizar copias de seguridad ni recuperar datos de Microsoft 365.

En Microsoft 365

- Su cuenta debe tener la función de administrador global en Microsoft 365.
- Para descubrir realizar una copia de seguridad de carpetas públicas de Microsoft 365 y recuperarlas, al menos una sus cuentas de administrador de Microsoft 365 tiene que tener un buzón de correo y derechos de escritura y lectura de las carpetas públicas de las que desea realizar una copia de seguridad.
  - El agente local iniciará sesión en Microsoft 365 mediante esta cuenta. Para que el agente pueda acceder al contenido de todos los buzones de correo, a esta cuenta se le asignará el rol de administración **ApplicationImpersonation**. Si cambia la contraseña de la cuenta, actualícela en la consola de Cyber Protect, como se describe en "Cambio de las credenciales de acceso de Microsoft 365" (p. 904).
  - El agente de la nube no inicia sesión en Microsoft 365. Para otorgar al agente de la nube los permisos que son necesarios para su funcionamiento, debe iniciar sesión en Microsoft 365 como administrador global.

    La tabla siguiente resume los permisos necesarios.

Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365
▪ Iniciar sesión y leer el perfil de usuario ▪ Leer y escribir archivos en todas las recopilaciones de sitios ▪ Leer y escribir los perfiles completos de todos los usuarios ▪ Leer y escribir todos los grupos ▪ Leer datos del directorio ▪ Leer todos los mensajes del canal ▪ Leer y escribir metadatos gestionados	▪ Utilizar Exchange Web Services con acceso completo a todos los buzones de correo ▪ Leer y escribir elementos en todas las colecciones de sitios ▪ Leer y escribir elementos y listas en todas las recopilaciones de sitios ▪ Tener control total de todas las recopilaciones de sitios ▪ Leer todas las directivas de configuración de copias de seguridad

© Acronis International GmbH, 2003-2025

Microsoft 365 Business (copia de seguridad)	Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365
▪ Leer y escribir elementos y listas en todas las recopilaciones de sitios ▪ Tener control total de todas las recopilaciones de sitios ▪ Utilizar Exchange Web Services con acceso completo a todos los buzones de correo	▪ Leer y editar todas las directivas de configuración de copias de seguridad ▪ Leer todas las sesiones de restauración ▪ Leer todas las sesiones de restauración y comenzar a restaurar sesiones desde copias de seguridad ▪ Leer toda la información de supervisión, cuota y facturación del inquilino ▪ Realizar la búsqueda de las propiedades de metadatos en todas las instantáneas de copias de seguridad ▪ Actualizar o leer el estado del servicio de copia de seguridad de M365 ▪ Leer el estado del servicio de copia de seguridad de M365 ▪ Leer los perfiles completos de todos los usuarios ▪ Leer información de la organización ▪ Actualizar o leer el estado del servicio de copia de seguridad de M365 ▪ Iniciar sesión y leer el perfil de usuario ▪ Leer y escribir los perfiles completos de todos los usuarios ▪ Leer archivos en todas las recopilaciones de sitios ▪ Leer todos los grupos ▪ Leer datos del directorio

- El agente en la nube no almacena las credenciales de su cuenta y no las utiliza para realizar copias de seguridad ni recuperaciones. Cambiar las credenciales, desactivar la cuenta o eliminarla no afectará al funcionamiento del agente en la nube.

Cómo añadir una organización de Microsoft 365

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)** y **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**.

Con **Microsoft 365 Business (copia de seguridad)**, puede agregar una organización de Microsoft 365 a un inquilino de cliente o unidad.

© Acronis International GmbH, 2003-2025

Con **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**, puede agregar una organización de Microsoft 365 a un inquilino de cliente.

Para agregar una organización de Microsoft 365, debe tener privilegios de administrador para el inquilino de cliente o unidad.

Puede agregar varias organizaciones de Microsoft 365 en el inquilino, pero no puede agregar la misma organización de Microsoft 365 en **Microsoft 365 Business (copia de seguridad)** y **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**.

Para añadir una organización de Microsoft 365

1. [Para agregar una organización de Microsoft 365 a nivel de inquilino de cliente] Inicie sesión en la consola de Cyber Protect como administrador.
2. [Solo para **Microsoft 365 Business (copia de seguridad)**] [Pasos para agregar una organización de Microsoft 365 a nivel de unidad] Según su rol, realice lo siguiente:
   a. [Para los administradores de unidad] Inicie sesión en la consola de Cyber Protect como administrador de unidad.
   b. [Para los administradores de la empresa que actúan a nivel de unidad] Vaya a la unidad en la que desee agregar la organización.
3. Haga clic en **Dispositivos** > **Agregar**.
4. Seleccione la solución de copia de seguridad.
   Dependiendo de los servicios que estén habilitados para su inquilino, puede elegir entre las siguientes opciones:
   - **Microsoft 365 Business (copia de seguridad)**
   - **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**
   - **Microsoft 365**
     Esta opción se muestra cuando tanto **Microsoft 365 Business (copia de seguridad)** como **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** están habilitados para su inquilino. Para obtener más información acerca de las diferencias entre estas soluciones, consulte "Comparación de soluciones de copia de seguridad para datos de Microsoft 365" (p. 833).
5. [Si ha seleccionado **Microsoft 365**] Haga clic en el botón de opción para seleccionar **Microsoft 365 Business (copia de seguridad)** o **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** y, a continuación, haga clic en **Continuar**.
6. En la página de inicio de sesión de Microsoft 365, acceda con las credenciales de administrador global de Microsoft 365.
   Microsoft 365 muestra una lista con aquellos permisos que son necesarios para realizar copias de seguridad de los datos de su organización, además de recuperarlos.
7. Confirme que concede los permisos requeridos.

© Acronis International GmbH, 2003-2025

Dependiendo de la solución seleccionada, verá la organización de Microsoft 365 en la consola de Cyber Protect, en la pestaña **Dispositivos** > **Microsoft 365** o en la pestaña **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.

Administración de organizaciones de Microsoft 365 añadidas en diferentes niveles

Nota
Con **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**, puede agregar organizaciones solo a nivel de inquilino de cliente.

Los administradores de empresa tienen acceso completo a las organizaciones de Microsoft 365 que se añaden al nivel de inquilino de cliente.

Los administradores de empresa tienen acceso limitado a las organizaciones que se añaden a una unidad. En estas organizaciones, que se muestran con el nombre de la unidad entre paréntesis, los administradores de empresa pueden hacer lo siguiente:

- Recuperar datos desde copias de seguridad.
  Los administradores de empresa pueden recuperar datos de todas las organizaciones en el inquilino, independientemente del nivel al que se añadan estas.
- Buscar copias de seguridad y puntos de recuperación en copias de seguridad.
- Eliminar copias de seguridad y puntos de recuperación en copias de seguridad.
- Ver alertas y actividades.

Los administradores de empresa, cuando actúan a nivel de inquilino de cliente, no pueden hacer lo siguiente:

- Añadir organizaciones de Microsoft 365 a unidades.
- Eliminar organizaciones de Microsoft 365 de unidades.
- Sincronizar organizaciones de Microsoft 365 que se hayan añadido a una unidad.
- Ver, crear, editar, eliminar, aplicar, ejecutar o revocar planes de copia de seguridad para elementos de datos en las organizaciones de Microsoft 365 que se añadan a una unidad.

Los administradores de unidad y de empresa que actúan a nivel de unidad tienen acceso completo a las organizaciones que se añaden a una unidad. Sin embargo, no tienen acceso a ningún recurso del inquilino de cliente principal, incluidos los planes de protección que se crean en este.

Detección de recursos de Microsoft 365

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)** y **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**.

© Acronis International GmbH, 2003-2025

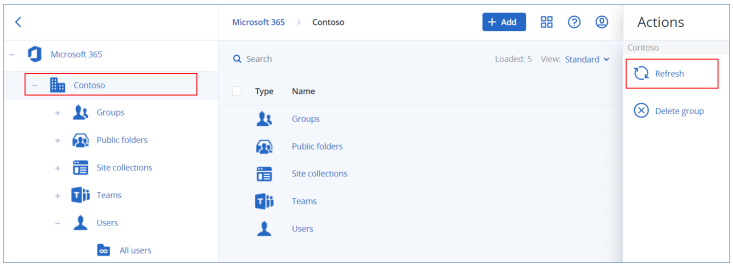
Cuando añade una organización de Microsoft 365 a Cyber Protect Cloud, los recursos de esta organización, como los buzones de correo de Exchange, las cuentas de OneDrive o los sitios de SharePoint, se sincronizan con la consola de Cyber Protect. Esta operación se llama detección y se registra en **Supervisión** > **Actividades**.

Cuando se complete la operación de detección, verá los recursos de la organización de Microsoft 365 en la consola de Cyber Protect y podrá aplicarles planes de copias de seguridad.

Una operación de detección automática se ejecuta una vez al día para mantener actualizada la lista de recursos de la consola de Cyber Protect. Puede sincronizar la lista bajo demanda si ejecuta una operación de detección manualmente.

Pasos para ejecutar una operación de detección manualmente

1. [Para **Microsoft 365 Business (copia de seguridad)**] En la consola de Cyber Protect,vaya a **Dispositivos** > **Microsoft 365**.
2. [Para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**] En la consola de Cyber Protect, vaya a **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.
3. Seleccione la organización de Microsoft 365 y, a continuación, en el panel **Acciones**, haga clic en **Actualizar**.



Nota
Puede ejecutar manualmente una operación de detección hasta 10 veces por hora. Cuando se alcance este número, las ejecuciones permitidas se restablecen durante una hora, y después una ejecución adicional pasa a estar disponible por cada hora, hasta que se alcanza de nuevo un total de 10 ejecuciones por hora.

Consejos útiles

- El agente en la nube se sincroniza con Microsoft 365 cada 24 horas desde el momento en que la organización se añade al servicio de Cyber Protection. Si añade o elimina un usuario, grupo o sitio, no verá este cambio en la consola de Cyber Protect inmediatamente. Para sincronizar el cambio de manera inmediata, ejecute una operación de detección manualmente.
- Si aplica un plan de copias de seguridad a **Todos los grupos**, **Todas las carpetas públicas**, **Todas las recopilaciones de sitios**, **Todos los equipos** o **Todos los usuarios**, los elementos recién agregados se incluirán en la copia de seguridad después de la sincronización.
- Según la política de Microsoft, cuando se elimina un usuario, grupo o sitio de la interfaz gráfica de usuario de Microsoft 365, sigue estando disponible durante varios días a través de la API.

© Acronis International GmbH, 2003-2025

Durante ese periodo, el elemento eliminado está inactivo (en gris) en la consola de Cyber Protect y no se realiza ninguna copia de seguridad de este. Cuando el elemento eliminado deja de estar disponible a través de la API, desaparece de la consola de Cyber Protect. Puede encontrar las copias de seguridad del usuario, grupo o sitio eliminado (si existen) en la consola de Cyber Protect en la pestaña **Almacenamiento de la copia de seguridad**> **Copias de seguridad de aplicaciones en la nube**.

Cómo eliminar una organización de Microsoft 365

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)** y **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**.

Si se elimina una organización de Microsoft 365, no afectará a las copias de seguridad existentes de los datos de dicha organización. Si ya no necesita estas copias de seguridad, elimínelas primero y, a continuación, elimine la organización de Microsoft 365. De lo contrario, las copias de seguridad seguirán ocupando espacio de almacenamiento en la nube que podría cobrársele. Para obtener más información acerca de cómo eliminar copias de seguridad, consulte "Para eliminar copias de seguridad o archivos de copia de seguridad" (p. 727).

Para eliminar una organización de Microsoft 365

1. [Pasos para eliminar una organización de Microsoft 365 a nivel de inquilino de cliente] Inicie sesión en la consola de Cyber Protect como administrador.
2. [Para eliminar una organización de Microsoft 365 a nivel de unidad] Según su rol, haga lo siguiente:
   a. [Para los administradores de unidad] Inicie sesión en la consola de Cyber Protect como administrador de unidad.
   b. [Para los administradores de la empresa que actúan a nivel de la unidad] Vaya a la unidad en la que se ha añadido la organización.
3. Vaya a **Dispositivos** y seleccione la solución de copia de seguridad que utiliza esta organización:
   - **Microsoft 365 Business (copia de seguridad)**
   - **Copia de seguridad directa para Microsoft 365**
4. Seleccione la organización y haga clic en **Eliminar**.

Como resultado, los planes de copias de seguridad aplicados a esta organización se revocarán y los recursos informáticos de la misma quedarán sin protección.

A continuación, revoque los derechos de acceso que se otorgan a la aplicación de servicio de copia de seguridad. Para obtener más información, consulte "Revocación de los derechos de acceso de la aplicación de servicio de copia de seguridad" (p. 846).

© Acronis International GmbH, 2003-2025

Revocación de los derechos de acceso de la aplicación de servicio de copia de seguridad

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)** y **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**.

Cuando agrega una organización de Microsoft 365 a la consola de Cyber Protect, otorga los derechos de acceso de la aplicación de **servicio de copia de seguridad** a la organización de Microsoft 365. Después de eliminar la organización de Microsoft 365 de la consola de Cyber Protect, debe revocar estos derechos de acceso.

Para obtener más información acerca de cómo eliminar una organización, consulte "Cómo eliminar una organización de Microsoft 365" (p. 845).

Pasos para revocar los derechos de acceso

1. Inicie sesión en Microsoft 365 como administrador global.
2. Vaya a **Centro de administración de Microsoft** > **Identidad** > **Aplicaciones** > **Aplicaciones empresariales** > **Todas las aplicaciones**.
3. Seleccione la aplicación **Servicio de copia de seguridad**.
4. Vaya a la pestaña **Propiedades** y, en el menú vertical, haga clic en **Eliminar**.
5. Confirme la eliminación.

Como resultado, se elimina la aplicación de **servicio de copia de seguridad** y se revocan los derechos de acceso a los datos de la organización de Microsoft 365.

Informe de licencia de usuarios de Microsoft 365

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)**. Con **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**, esta funcionalidad no está disponible.

Los administradores de la empresa pueden descargar un informe sobre los usuarios de Microsoft 365 protegidos y su licencia. El informe está en formato CSV e incluye información sobre el estado de la licencia de un usuario y el motivo por el que se utiliza una licencia. El informe también incluye el nombre del usuario protegido, el correo electrónico asociado, el grupo, la organización de Microsoft 365, el nombre y el tipo de recurso informático protegido.

Este informe solo está disponible para inquilinos en los que se haya registrado una organización de Microsoft 365.

Pasos para descargar el informe de licencia de usuarios de Microsoft 365

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect como administrador de la empresa.
2. Haga clic en el icono de la cuenta en la esquina superior derecha.
3. Haga clic en **Informe de licencia de usuarios de Microsoft 365**.

Configuración de la frecuencia de las copias de seguridad de Microsoft 365

Nota
Este tema se aplica a **Microsoft 365 Business (copia de seguridad)**. Con **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft**, esta funcionalidad no está disponible.

Con las funciones estándar incluidas, las copias de seguridad de Microsoft 365 se ejecutan una vez al día de manera predeterminada y no hay opciones de programación adicionales disponibles.

Si el paquete Advanced Backup está habilitado en su inquilino, la opción **Dos veces al día** está habilitada de forma predeterminada y hay más frecuencias disponibles entre las que seleccionar.

Puede seleccionar el número de copias de seguridad por día, pero no puede configurar la hora de inicio de la copia de seguridad. Las copias de seguridad se inician automáticamente a intervalos aproximados en función de la carga actual del agente de la nube, que gestiona varios clientes en un centro de datos. De este modo, se garantiza una carga equilibrada durante el día y la misma calidad de servicio para todos los clientes.

Las siguientes opciones están disponibles.

Opciones de planificación	Intervalo aproximado entre cada copia de seguridad
Una vez al día*	24 horas
Dos veces al día (predeterminado)**	12 horas
Tres veces al día**	8 horas
Seis veces al día**	4 horas

* Aunque la opción **Dos veces al día** es la predeterminada cuando Advanced Backup está habilitado, la opción **Una vez al día** podría habilitarse de forma temporal en algunos centros de datos, según la disponibilidad de almacenamiento.

** Se requiere el paquete Advanced Backup

© Acronis International GmbH, 2003-2025

Nota
Según la carga del agente de la nube y la posible limitación de Microsoft 365, puede que las copias de seguridad se inicien más tarde de lo previsto o tarden más en completarse. Si una copia de seguridad tarda más que el intervalo medio entre dos copias de seguridad, se reprogramará la siguiente y, por tanto, podría haber menos copias de seguridad por día de las que se habían seleccionado. Por ejemplo, es posible que solo se puedan completar dos copias de seguridad, aunque haya seleccionado seis por día.

Las copias de seguridad de los buzones de correo en grupo solo pueden ejecutarse una vez al día.

Microsoft 365 Business (copia de seguridad)

Nota
Esta función está disponible en los inquilinos de clientes para las **licencias de Microsoft 365** (**buzones de correo**, **OneDrive**) y **Microsoft 365 SharePoint Online** seleccionados en **Protección estándar** en el portal de administración.

Si no se seleccionan algunas de las casillas de verificación, la función estará parcialmente disponible.

Los datos de la copia de seguridad se comprimen automáticamente y utilizan menos espacio en la ubicación de la copia de seguridad que en su ubicación original. La tasa de compresión para las copias de seguridad de la nube a la nube es fija y corresponde al nivel **Normal** de las copias de seguridad que no son de la nube a la nube. Para obtener más información sobre estos niveles, consulte "Tasa de compresión" (p. 605).

Planes de copias de seguridad aplicados y programados para cargas de trabajo de Microsoft 365

Puede aplicar solo un plan de copias de seguridad por servicio a una carga de trabajo de Microsoft 365 individual. Para obtener más información sobre los servicios disponibles por carga de trabajo, consulte "Visualización del estado de protección de una carga de trabajo de Microsoft 365 por servicio" (p. 849).

Por ejemplo, puede aplicar solo un plan de copias de seguridad de buzón de correo a un usuario de Microsoft 365. También puede aplicar el mismo tipo de plan (copia de seguridad de buzón de correo) a uno o más grupos dinámicos o estáticos que contengan esta carga de trabajo. En este caso, el buzón de correo del usuario puede ser respaldado por más de un plan de copias de seguridad.

Importante
Solo el plan que se aplique primero se ejecutará automáticamente según la programación. Los demás planes se aplicarán correctamente a la carga de trabajo, pero solo se podrán ejecutar manualmente.

© Acronis International GmbH, 2003-2025

Por ejemplo:

- Aplica el Plan A (copia de seguridad del buzón de correo) al usuario John Doe. No puede aplicar otro plan de copias de seguridad del buzón de correo (Plan B) al mismo usuario porque el Plan A ya está aplicado.
- Aplica el Plan B (copia de seguridad del buzón de correo) a un grupo dinámico o estático que contenga a John Doe. No puede aplicar otro plan de buzón de correo (Plan C) al mismo grupo dinámico porque ya se ha aplicado el Plan B.
- Aplica el Plan C (copia de seguridad de buzón de correo) a **Todos los grupos**, o a un grupo dinámico o estático diferente que contenga a John Doe.

Como resultado, el plan A, el plan B y el plan C pueden realizar la copia de seguridad del buzón de correo de John Doe, pero solo el plan A se ejecutará según lo programado para este usuario porque fue el primero en aplicarse. Puede ejecutar manualmente el plan B y el plan C para John Doe. El plan B y el plan C se ejecutarán según lo programado para los usuarios o grupos en los que cada uno de estos planes sea el primero en aplicarse.

Visualización del estado de protección de una carga de trabajo de Microsoft 365 por servicio

Dependiendo del tipo de carga de trabajo de Microsoft 365, puede proteger los siguientes servicios:

Carga de trabajo	Servicios
Grupos*	Casilla de correo
	Sitio
Carpetas públicas	Casilla de correo
Recopilación de sitios	Sitio
Teams	Canales de Teams
Usuarios	Casilla de correo
	OneDrive

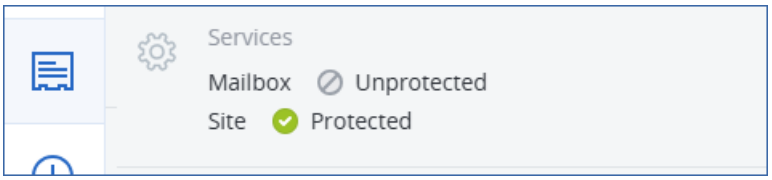
* Los grupos contienen sitios modernos (de equipo) y buzones de correo de grupo. Los grupos que son parte de un equipo pueden tener una copia de seguridad doble si están protegidos como grupo y como parte del equipo. Para obtener más información, consulte "Evitar copias de seguridad duplicadas de grupos de Microsoft 365" (p. 851).

Si hay más de un servicio disponible para una carga de trabajo, pero solo uno está protegido, la carga de trabajo está parcialmente protegida. Por ejemplo, si se realiza una copia de seguridad del buzón de correo de un usuario, pero no de los archivos de OneDrive, este usuario está parcialmente protegido.

Cómo comprobar el estado de protección por servicio

© Acronis International GmbH, 2003-2025

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365.
3. Seleccione una carga de trabajo y haga clic en **Detalles**.
4. Compruebe la sección **Servicios**.
   Por ejemplo:



Revocar un plan de copias de seguridad para Microsoft 365 Business – Copia de seguridad

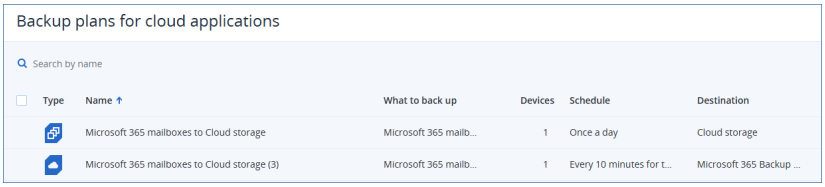
Puede revocar un plan de copias de seguridad en la pestaña **Gestión** > **Copias de seguridad de aplicaciones en la nube** o en la pestaña **Dispositivos**.

Puede revocar un plan de copias de seguridad de una carga de trabajo individual o de un grupo de dispositivos.

Pasos para revocar un plan de copias de seguridad

Gestión > Copias de seguridad de aplicaciones en la nube

1. En la consola de Cyber Protect, vaya a **Gestión** y luego pulse en **Copias de seguridad de aplicaciones en la nube**.
2. Seleccione un plan de copias de seguridad para **Microsoft 365 Business – Copia de seguridad** y, a continuación, haga clic en **Editar**.
   Puede distinguir entre los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** y **Microsoft 365 Business (copia de seguridad)** comparando sus iconos y el destino de la copia de seguridad. Los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** solo pueden utilizar el almacenamiento de copia de seguridad de Microsoft 365.



   a. Haga clic en **Dispositivos**.
   b. Seleccione las cargas de trabajo o grupos de dispositivos en los que quiera revocar el plan y, a continuación, haga clic en **Eliminar**.
   c. Haga clic en **Listo**.
3. Haga clic en **Guardar cambios**.

© Acronis International GmbH, 2003-2025

Como resultado, el plan de copias de seguridad se revoca de todos las cargas de trabajo que se eliminaron.

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** y pulse en **Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. [Para cargas de trabajo individuales] Seleccione una carga de trabajo en la que desee revocar un plan de copias de seguridad y, a continuación, haga clic en **Copia de seguridad**.
   Los planes de copias de seguridad que se aplican a un grupo estático o dinámico están bloqueados. Puede revocarlos a nivel de grupo.
4. [Para grupos de dispositivos] Seleccione un grupo en el que desee revocar un plan de copias de seguridad y, a continuación, haga clic en **Agrupar copia de seguridad**.
5. Pulse en el icono de engranaje situado junto al nombre del plan de copias de seguridad y, a continuación, haga clic en **Revocar**.

Evitar copias de seguridad duplicadas de grupos de Microsoft 365

Las copias de seguridad duplicadas para un grupo de Microsoft 365 que forma parte de un equipo pueden producirse si configura la copia de seguridad en **Grupos** y **Equipos** en la consola de Cyber Protect:

- En **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**, puede configurar una copia de seguridad para el sitio de SharePoint y el buzón de correo del grupo.
- En **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Equipos**, puede configurar una copia de seguridad de un equipo. Esta copia de seguridad también incluye el sitio de SharePoint y el buzón de correo del grupo, junto con otros datos relacionados con el equipo.

Las copias de seguridad duplicadas dan como resultado un uso ineficiente del almacenamiento y pueden dar lugar a un aumento de costes. Recomendamos que realice copias de seguridad de los grupos que forman parte de un equipo aplicando un plan de copias de seguridad al equipo.

Nota
A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

En **Grupos**, puede gestionar los siguientes grupos:

- Grupos de Microsoft 365 protegidos y no protegidos que no son parte de un equipo.
- Grupos protegidos que son parte de un equipo de Microsoft.
  Un grupo protegido es un grupo al que se aplica un plan de copias de seguridad. Un grupo no protegido es un grupo al que no se aplica un plan de copias de seguridad.

© Acronis International GmbH, 2003-2025

Cómo evitar copias de seguridad duplicadas de un grupo de Microsoft 365

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos** > **Todos los grupos**.
3. Compruebe la columna **Equipo**.
   Para los grupos que no son parte de un equipo, esta columna está vacía.
   Para los grupos que son parte de un equipo, se muestra el nombre del equipo. Un icono de triángulo amarillo  indica que este grupo puede tener copias de seguridad duplicadas.
4. Seleccione un grupo que esté marcado con el icono de triángulo amarillo y verifique que este grupo solo se respalda como parte de un equipo.
   a. [Si se aplica un plan de copias de seguridad de SharePoint o buzón de correo] Revoque los planes de copias de seguridad aplicados, como se describe en "Revocar un plan de copias de seguridad para Microsoft 365 Business – Copia de seguridad" (p. 850).
   b. Vaya a **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Equipos** > **Todos los equipos** y luego asegúrese de que se aplique un plan de copias de seguridad al equipo que incluya este grupo.

Protección de los datos de Exchange Online

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de los buzones de correo de usuario, compartidos y de grupo. De manera opcional, también puede llevar a cabo copias de seguridad de buzones de correo de archivos comprimidos en línea (**archivo comprimido local**) de los buzones de correo seleccionados.

A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

Si su organización de Microsoft 365 se añadió antes de Cyber Protect 8.0, debe repetir los pasos descritos en "Cómo añadir una organización de Microsoft 365" (p. 841) para poder realizar copias de seguridad de carpetas públicas. No tiene que eliminar la organización antes de volver a añadirla.

¿Qué elementos de datos pueden recuperarse?

Los siguientes elementos pueden recuperarse de la copia de seguridad de buzones de correo:

- Buzones de correo
- Carpetas de correo electrónico
- Mensajes de correo electrónico

© Acronis International GmbH, 2003-2025

- Eventos del calendario
- Tareas
- Contactos
- Entradas del diario
- Notas

Los siguientes elementos pueden recuperarse de la copia de seguridad de una carpeta pública:

- Subcarpetas
- Publicaciones
- Mensajes de correo electrónico

Puede usar la búsqueda para localizar los elementos.

Al recuperar elementos de buzones de correo, buzones de correo, elementos de carpetas públicas y carpetas públicas, puede seleccionar si quiere sobrescribir los elementos en la ubicación de destino.

Selección de buzones de correo

Seleccione los buzones de correo que desee proteger y, a continuación, aplíqueles un plan de copias de seguridad.

Puede crear un nuevo plan o seleccionar un plan existente.

Pasos para seleccionar buzones de correo de Exchange Online y aplicar un plan de copias de seguridad

Nuevo plan

1. En la consola de Cyber Protect, en **Dispositivos**, haga clic en **Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Seleccione los buzones de correo de los que desea realizar una copia de seguridad.
   - [Para realizar una copia de seguridad de los buzones de correo de todos los usuarios y de todos los compartidos, incluidos los que se crearán en el futuro] Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.
   - [Para realizar una copia de seguridad de los buzones de correo compartidos o de usuarios individuales] Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los buzones de correo desea respaldar y haga clic en **Copia de seguridad**.
   - [Para realizar una copia de seguridad de los buzones de correo de todos los grupos, incluidos los buzones de los grupos que se creen en el futuro] Amplíe el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Copia de seguridad de grupos**.

© Acronis International GmbH, 2003-2025

Nota
A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

Nota
Al menos uno de los propietarios del grupo debe ser un usuario con licencia de Microsoft 365 con buzón de correo. Si el grupo es privado o con una membresía oculta, el propietario también debe ser miembro del grupo.

- [Para realizar una copia de seguridad de los buzones de correo de grupos individuales] Amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija los buzones de correo de los que desea realizar una copia de seguridad y haga clic en **Copia de seguridad**.

Nota
A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

Nota
Al menos uno de los propietarios del grupo debe ser un usuario con licencia de Microsoft 365 con buzón de correo. Si el grupo es privado o con una membresía oculta, el propietario también debe ser miembro del grupo.

4. Para crear un plan de copias de seguridad, haga clic en **Crear nuevo**.
5. En el plan de copias de seguridad, configure lo siguiente:
   - [Si está disponible en] En **Qué incorporar en la copia de seguridad**, seleccione **Buzones de correo de Microsoft 365**.

     Si alguno de los usuarios seleccionados individualmente no tiene el servicio de Exchange incluido en su plan Microsoft 365, no podrá elegir esta opción.

     Si alguno de los usuarios seleccionados para la copia de seguridad en grupo no tiene el servicio de Exchange incluido en su plan Microsoft 365, no podrá elegir esta opción, pero el plan de protección no se aplicará a dichos usuarios.
   - En **Programar**, seleccione la frecuencia de la copia de seguridad.

     Esta opción es configurable si el paquete **Advanced Backup** está habilitado para este cliente. Para obtener más información, consulte "Configuración de la frecuencia de las copias de seguridad de Microsoft 365" (p. 847).
   - En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.

© Acronis International GmbH, 2003-2025

- [Opcional] Para incluir los buzones de correo de archivo en la copia de seguridad, habilite el interruptor **Buzón de correo de archivo**.
- En **Cifrado**, haga clic en **Especificar contraseña**.
  - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
  - Haga clic en **Aceptar**.
- [Opcional] Para habilitar el análisis antimalware, habilite el interruptor **Análisis de copia de seguridad en busca de malware**.

  Nota
  La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

  Para obtener más información, consulte "Análisis antimalware de buzones de correo" (p. 857).

6. Haga clic en **Aplicar**.

Plan existente

1. En la consola de Cyber Protect, en **Dispositivos**, haga clic en **Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Seleccione los buzones de correo de los que desea realizar una copia de seguridad.
   - [Para realizar una copia de seguridad de los buzones de correo de todos los usuarios y de todos los compartidos, incluidos los que se crearán en el futuro] Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.
   - [Para realizar una copia de seguridad de los buzones de correo compartidos o de usuarios individuales] Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los buzones de correo desea respaldar y haga clic en **Copia de seguridad**.
   - [Para realizar una copia de seguridad de los buzones de correo de todos los grupos, incluidos los buzones de los grupos que se creen en el futuro] Amplíe el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Copia de seguridad de grupos**.

     Nota
     A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

     Nota
     Al menos uno de los propietarios del grupo debe ser un usuario con licencia de Microsoft 365 con buzón de correo. Si el grupo es privado o con una membresía oculta, el propietario también debe ser miembro del grupo.

© Acronis International GmbH, 2003-2025

- [Para realizar una copia de seguridad de los buzones de correo de grupos individuales] Amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija los buzones de correo de los que desea realizar una copia de seguridad y haga clic en **Copia de seguridad**.

Nota
A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

Nota
Al menos uno de los propietarios del grupo debe ser un usuario con licencia de Microsoft 365 con buzón de correo. Si el grupo es privado o con una membresía oculta, el propietario también debe ser miembro del grupo.

4. Seleccione un plan de copias de seguridad existente.
5. Haga clic en **Aplicar**.

Selección de carpetas públicas

Seleccione las carpetas públicas tal como se describe a continuación y, luego, especifique otros ajustes del plan de protección según corresponda.

Nota
Las carpetas públicas utilizan licencias de su cuota de copias de seguridad para puestos de Microsoft 365.

Pasos para seleccionar carpetas públicas de Exchange Online

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, amplíe la organización cuyos datos quiera recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Carpetas públicas** y después seleccione **Todas las carpetas públicas**.
4. Realice uno de los siguientes procedimientos:
   - Para realizar una copia de seguridad de todas las carpetas públicas (incluidas las carpetas públicas que se crearan en el futuro), haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de carpetas públicas individuales, seleccione las carpetas públicas para las que quiere realizar una copia de seguridad y, después, haga clic en **Copia de seguridad**.
5. En el plan de copias de seguridad, configure lo siguiente:
   - En **Programar**, seleccione la frecuencia de la copia de seguridad.

© Acronis International GmbH, 2003-2025

Esta opción es configurable si el paquete **Advanced Backup** está habilitado para este cliente. Para obtener más información, consulte "Configuración de la frecuencia de las copias de seguridad de Microsoft 365" (p. 847).

- En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.
- En **Cifrado**, haga clic en **Especificar contraseña**.
  - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
  - Haga clic en **Aceptar**.
- [Opcional] Para habilitar el análisis antimalware, habilite el interruptor **Análisis de copia de seguridad en busca de malware**.

  Nota
  La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

  Para obtener más información, consulte "Análisis antimalware de buzones de correo" (p. 857).

Análisis antimalware de buzones de correo

El análisis antimalware de los buzones de correo de Microsoft 365 comprueba los correos electrónicos que se incluyen en la copia de seguridad en busca de archivos maliciosos y URL sospechosas, y le notifica si se detectan amenazas.

Esta función requiere el paquete **Advanced Security + XDR**, en el que la cuota de **licencias de Microsoft 365** debe estar habilitada. El análisis antimalware de los buzones de correo de Microsoft 365 se proporciona como parte del paquete avanzado, sin coste adicional.

Nota
En la versión 24.11, la cuota de **licencias de Microsoft 365** en el paquete **Advanced Security + XDR** se habilita automáticamente para los clientes existentes que utilizan el paquete **Advanced Security + XDR** con la cuota de **Cargas de trabajo** incluida y que tienen la cuota de **licencias de Microsoft 365** en la **Protección estándar**.

Para estos clientes, el análisis antimalware se habilita automáticamente en los planes de copias de seguridad existentes para los buzones de correo de Microsoft 365.

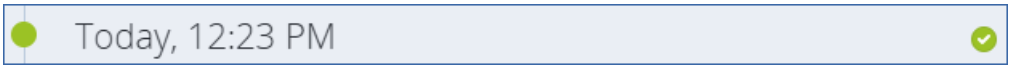
Puede habilitar análisis antimalware al configurar un plan de copias de seguridad para buzones de Microsoft 365. Para obtener más información, consulte "Selección de buzones de correo" (p. 853).

Los análisis se ejecutan automáticamente después de cada nueva copia de seguridad. No puede programar ni ejecutar un análisis manualmente.

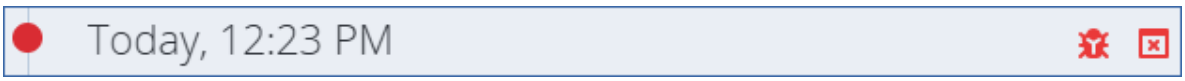
Después de que finalice el análisis, la copia de seguridad (punto de recuperación) dentro del archivo de copia de seguridad se marca de la siguiente manera:

© Acronis International GmbH, 2003-2025

- Si no se encuentra malware, la copia de seguridad se marca con un punto y un icono verdes.



- Si se encuentra malware, la copia de seguridad se marca con un punto rojo y uno o dos iconos rojos, según el tipo de amenaza detectada (archivo malicioso o URL sospechosa).

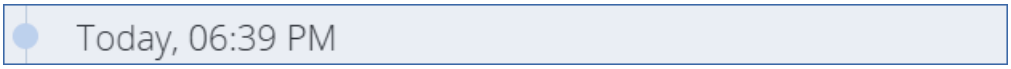


  Para obtener más información sobre cómo comprobar los detalles de estas amenazas, consulte "Cómo comprobar los detalles de una amenaza detectada" (p. 859).

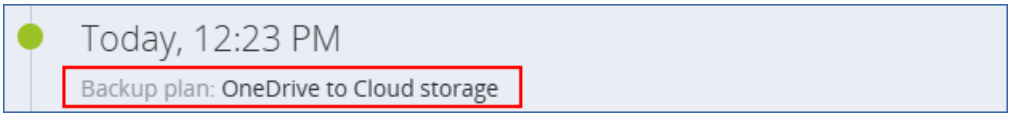
  Importante
  Tenga cuidado al recuperar copias de seguridad: el análisis antimalware de los buzones de correo le notifica sobre la amenaza detectada, pero no le impide recuperar una copia de seguridad infectada.
  Para limpiar una copia de seguridad infectada, vaya al buzón de correo de Microsoft 365 y elimine el archivo adjunto malicioso o el mensaje de correo electrónico al completo. Así, la próxima copia de seguridad estará limpia.

  Puede mejorar su protección habilitando Advanced Email Security. Con este paquete avanzado, los correos electrónicos sospechosos se detectan antes de llegar a la bandeja de entrada. Para obtener más información, consulte Advanced Email Security.

Si una copia de seguridad aún no se ha analizado, se marca con un punto gris y no se muestran iconos adicionales.



Una copia de seguridad para la que no está disponible el análisis antimalware, como una copia de seguridad de OneDrive, se marca con un punto verde y no se muestran iconos adicionales.



Limitaciones

- El análisis antimalware no es compatible con los siguientes tipos de archivos:
  - RAR
  - 7z
  - ISO
- Si una tarea de análisis falla, se volverá a intentar en un día.
- El análisis antimalware no es compatible con los componentes de Loop en los correos electrónicos. No se detectarán posibles amenazas en un componente de Loop.

© Acronis International GmbH, 2003-2025

- El análisis antimalware solo se admite en el almacenamiento en la nube predeterminado. No se admite en los almacenamientos locales, los almacenamientos alojados por partners ni los almacenamientos en la nube pública.
- El análisis antimalware no es compatible con los inquilinos en el modo Cumplimiento.

Cómo comprobar los detalles de una amenaza detectada

Puede obtener más información sobre las amenazas detectadas al comprobar el archivo de copia de seguridad, el correo electrónico infectado o la pestaña **Alertas** en la consola de Cyber Protect.

Pasos para comprobar los detalles de una amenaza detectada

En el archivo de copia de seguridad

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**> **Copias de seguridad** y seleccione el **Almacenamiento de aplicaciones en la nube**.
2. Seleccione el archivo de copia de seguridad que desee comprobar y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione una copia de seguridad que esté marcada con un icono rojo de archivo infectado o URL maliciosa.
4. Para obtener más información sobre la amenaza, haga clic en el enlace **Archivos infectados** o **URL maliciosas**.

En un correo electrónico que se ha incluido en una copia de seguridad

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**> **Copias de seguridad** y seleccione el **Almacenamiento de aplicaciones en la nube**.
2. Seleccione el archivo de copia de seguridad que desee comprobar y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione una copia de seguridad que esté marcada con un icono rojo de archivo infectado o URL maliciosa.
4. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
5. [Si se muestra un aviso de privacidad] En el diálogo **Aviso de privacidad**, haga clic en **Continuar**.
6. Seleccione un mensaje de correo electrónico que esté marcado con un icono rojo de archivo infectado o URL maliciosa y, a continuación, haga clic en **Mostrar contenido**.
7. En **Se han detectado amenazas maliciosas en este correo electrónico**, haga clic en **Detalles**.

En Supervisión > Alertas

1. En la consola de Cyber Protect, vaya a **Supervisión** > **Alertas** y seleccione **Almacenamiento de aplicaciones en la nube**.
2. Clasifique las alertas por gravedad.
3. En **Advertencia**, busque **URL maliciosa detectada** o **Malware detectado**.
4. [Si se detecta una URL maliciosa] Compruebe la línea **URL** en la parte inferior de la alerta.

© Acronis International GmbH, 2003-2025

5. [Si se detecta malware] Compruebe la línea **Nombre de la amenaza** en la parte inferior de la alerta.

Recuperación de buzones de correo y elementos de los buzones

Recuperación de buzones de correo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para recuperar el buzón de correo de un usuario, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario cuyo buzón de correo quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar un buzón de correo compartido, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el buzón de correo compartido que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar el buzón de correo de un grupo, amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija el grupo cuyo buzón de correo quiera recuperar y haga clic en **Recuperación**.
   - Si el usuario, el grupo o el buzón de correo compartido se ha eliminado, seleccione el elemento de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

   Nota
   Para ver únicamente los puntos de recuperación que incluyan buzones de correo, seleccione **Buzones de correo** en **Filtrar por contenido**.

5. Haga clic en **Recuperar** > **Todo el buzón de correo**.
6. Si se añaden varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
7. En **Recuperar al buzón de correo**, puede consultar, cambiar o especificar el buzón de correo de destino.

   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona una organización que no es la original, debe indicar el buzón de correo de destino.

   No puede crear un nuevo buzón de correo de destino durante la recuperación. Para recuperar un buzón de correo en uno nuevo, primero necesita crear el buzón de correo de destino en la organización de Microsoft 365 deseada y, a continuación, dejar que el agente en la nube

© Acronis International GmbH, 2003-2025

sincronice el cambio. El agente en la nube se sincroniza automáticamente con Microsoft 365 cada 24 horas. Para sincronizar el cambio inmediatamente, en la consola den Cyber Protect, seleccione la organización en la página **Microsoft 365** y luego haga clic en **Actualizar**.

8. Haga clic en **Iniciar recuperación**.
9. Seleccione una de las opciones de sobreescritura:
   - **Sobrescribir elementos existentes**
   - **No sobrescribir elementos existentes**
10. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de elementos de buzón de correo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para recuperar elementos del buzón de correo de un usuario, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario en cuyo buzón de correo se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar los elementos de un buzón de correo compartido, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el buzón de correo compartido que contenía los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar elementos del buzón de correo de un grupo, amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija el grupo en cuyo buzón de correo se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Si el usuario, el grupo o el buzón de correo compartido se ha eliminado, seleccione el elemento de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

   Nota
   Para ver únicamente los puntos de recuperación que incluyan buzones de correo, seleccione **Buzones de correo** en **Filtrar por contenido**.

5. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de los elementos necesarios.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

© Acronis International GmbH, 2003-2025

- Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario, nombre del archivo adjunto y fecha. Puede seleccionar una fecha de inicio o de fin, o ambas fechas, para buscar dentro de un intervalo de tiempo.
- Para los eventos: búsqueda por título y fecha.
- Para las tareas: búsqueda por asunto y fecha.
- Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

7. Seleccione los elementos que desea recuperar. Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 

   No puede crear un nuevo buzón de correo de destino durante la recuperación. Para recuperar un nuevo elemento de buzón de correo en un nuevo buzón de correo, primero necesita crear el nuevo elemento de buzón de correo de destino en la organización de Microsoft 365 y, a continuación, dejar que el agente en la nube sincronice el cambio. El agente en la nube se sincroniza automáticamente con Microsoft 365 cada 24 horas. Para sincronizar el cambio inmediatamente, en la consola den Cyber Protect, seleccione la organización en la página **Microsoft 365** y luego haga clic en **Actualizar**.

   También puede optar por una de las siguientes opciones:

   - Cuando se seleccione un elemento, haga clic en **Mostrar contenido** para ver su contenido, incluidos los archivos adjuntos. Haga clic en el nombre de un archivo adjunto para descargarlo.
   - Cuando un mensaje de correo electrónico o el elemento de un calendario esté seleccionado, haga clic en **Enviar como correo electrónico** para enviar el elemento a la dirección de correo electrónico especificada. Puede seleccionar el remitente y escribir un texto para añadirlo al elemento reenviado.
   - Únicamente si la copia de seguridad no está cifrada, ha usado la búsqueda y ha seleccionado un único elemento de la lista de resultados de búsqueda: haga clic en **Mostrar versiones** para seleccionar la versión del elemento que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.

8. Haga clic en **Recuperar**.
9. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
10. En **Recuperar al buzón de correo**, puede consultar, cambiar o especificar el buzón de correo de destino.

    De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona una organización que no es la original, debe indicar el buzón de correo de destino.

© Acronis International GmbH, 2003-2025

11. [Solo al recuperar un buzón de correo de usuario o compartido] En **Ruta**, puede consultar o cambiar la carpeta de destino en el buzón de correo de destino. De manera predeterminada, se selecciona la carpeta **Elementos recuperados**.
    Los elementos de buzón de correo de grupos siempre se recuperan en la carpeta **Bandeja de entrada**.
12. Haga clic en **Iniciar recuperación**.
13. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir elementos existentes**
    - **No sobrescribir elementos existentes**
14. Haga clic en **Continuar** para confirmar su decisión.

Recuperar todos los buzones de correo en archivos de datos PST

Nota
Puede recuperar correos electrónicos o carpetas del archivo en ubicación como elementos de buzón de correo independientes al utilizar la opción **Recuperación > Mensajes de correo electrónico**. Para obtener más información, consulte "Recuperación de elementos de buzón de correo" (p. 861). El archivo en ubicación no se recupera cuando utiliza las opciones **Recuperación > Buzón de correo completo** o **Recuperación > Como archivos PST**.

Pasos para recuperar un buzón de correo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para recuperar el buzón de correo de un usuario en un archivo de datos PST, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el buzón de correo que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar el buzón de correo compartido de un usuario en un archivo de datos PST, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el buzón de correo que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar el buzón de correo de un grupo en un archivo de datos PST, amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija el grupo cuyo buzón de correo quiera recuperar y haga clic en **Recuperación**.

   Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
   Si el usuario, el grupo o el archivo de datos de Outlook compartido se ha eliminado, seleccione el elemento de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
4. Haga clic en **Recuperar** > **Como archivos PST**.

© Acronis International GmbH, 2003-2025

5. Configure la contraseña para cifrar el archivo comprimido con los archivos PST.
   La contraseña debe contener al menos un símbolo.
6. Confirme la contraseña y haga clic en **Listo**.
7. Los elementos del buzón de correo seleccionado se recuperarán como archivos de datos PST y se comprimirán en formato zip. El tamaño máximo de un archivo PST se limita a 2 GB, por lo que si los datos que va a recuperar exceden los 2 GB, se dividirán en varios archivos PST. El archivo zip estará protegido con la contraseña que configure.
8. Recibirá un correo electrónico con un enlace a un archivo zip que contine los archivos PST creados.
9. El administrador recibirá un correo electrónico para informarle de que ha realizado el procedimiento de recuperación.

Nota
La recuperación por buzón de correo a archivos PST puede llevar tiempo, ya que implica no solo la transferencia de datos, sino también su transformación mediante algoritmos complejos.

Pasos para descargar el archivo comprimido con los archivos pst y completar la recuperación

1. Realice uno de los siguientes procedimientos:
   - Para descargar el archivo comprimido del correo electrónico, siga el enlace **Descargar archivos**.
     El archivo esta disponible 96 horas. Para descargar el archivo comprimido después de las 96 horas, repita el procedimiento de recuperación.
   - Para descargar el archivo comprimido de la consola de Cyber Protect:
     a. Vaya a **Almacenamiento de la copia de seguridad** > **Archivos PST**.
     b. Seleccione el archivo destacado más reciente.
     c. En el panel derecho, haga clic en **Descargar**.

   El archivo comprimido se descargará en el directorio de descargas predeterminado de su ordenador.
2. Extraiga los archivos PST del archivo comprimido con la contraseña que configuró para cifrar el archivo comprimido.
3. Abra los archivos PST con Microsoft Outlook.
   Los archivos PST resultantes podrían tener un tamaño mucho menor que el buzón original. Eso es normal.

   Importante
   No importe estos archivos a Microsoft Outlook usando el **Asistente para importación y exportación**.
   Abra los archivos haciendo doble clic en ellos o haciendo clic con el botón derecho y seleccionando **Abrir con...** > **Microsoft Outlook** en el menú contextual.

© Acronis International GmbH, 2003-2025

Recuperación de elementos del buzón de correo en archivos PST

Nota
Puede recuperar correos electrónicos o carpetas del archivo en ubicación como elementos de buzón de correo independientes al utilizar la opción **Recuperación > Mensajes de correo electrónico**. Para obtener más información, consulte "Recuperación de elementos de buzón de correo" (p. 861). El archivo en ubicación no se recupera cuando utiliza las opciones **Recuperación > Buzón de correo completo** o **Recuperación > Como archivos PST**.

Pasos para recuperar elementos del buzón de correo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para recuperar elementos del buzón de correo de un usuario, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario en cuyo buzón de correo se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar los elementos de un buzón de correo compartido, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el buzón de correo compartido que contenía los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar elementos del buzón de correo de un grupo, amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija el grupo en cuyo buzón de correo se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Si el usuario, el grupo o el buzón de correo compartido se ha eliminado, seleccione el elemento de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
4. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
5. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de los elementos necesarios.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.
   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario, nombre del adjunto y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

© Acronis International GmbH, 2003-2025

6. Seleccione los elementos que desea recuperar. Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 

   También puede optar por una de las siguientes opciones:
   - Cuando un elemento está seleccionado, haga clic en **Mostrar contenido** para ver lo que se incluye, incluidos los adjuntos. Haga clic en el nombre de un archivo adjunto para descargarlo.
   - Cuando un mensaje de correo electrónico o el elemento de un calendario esté seleccionado, haga clic en **Enviar como correo electrónico** para enviar el elemento a la dirección de correo electrónico especificada. Puede seleccionar el remitente y escribir un texto para añadirlo al elemento reenviado.
   - Únicamente si la copia de seguridad no está cifrada, ha usado la búsqueda y ha seleccionado un único elemento de la lista de resultados de búsqueda: haga clic en **Mostrar versiones** para seleccionar la versión del elemento que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.
7. Haga clic en **Recuperar como archivos PST**.
8. Configure la contraseña para cifrar el archivo comprimido con los archivos PST.
   La contraseña debe contener al menos un símbolo.
9. Confirme la contraseña y haga clic en **LISTO**.

Los elementos del buzón de correo seleccionado se recuperarán como archivos de datos PST y se comprimirán en formato zip. El tamaño máximo de un archivo PST se limita a 2 GB, por lo que si los datos que vas a recuperar exceden los 2 GB, se dividirán en varios archivos PST. El archivo zip estará protegido con la contraseña que configure.

Recibirá un correo electrónico con un enlace a un archivo zip que contine los archivos PST creados.

El administrador recibirá un correo electrónico para informarle de que ha realizado el procedimiento de recuperación.

Pasos para descargar el archivo comprimido con los archivos pst y completar la recuperación

1. Realice uno de los siguientes procedimientos:
   - Para descargar el archivo comprimido del correo electrónico, siga el enlace **Descargar archivos**.
     El archivo esta disponible 96 horas. Para descargar el archivo comprimido después de las 96 horas, repita el procedimiento de recuperación.
   - Para descargar el archivo comprimido de la consola de Cyber Protect:
     a. Vaya a **Almacenamiento de la copia de seguridad** > **Archivos PST**.
     b. Seleccione el archivo destacado más reciente.
     c. En el panel derecho, haga clic en **Descargar**.

   El archivo comprimido se descargará en el directorio de descargas predeterminado de su ordenador.

© Acronis International GmbH, 2003-2025

2. Extraiga los archivos PST del archivo comprimido con la contraseña que configuró para cifrar el archivo comprimido.
3. Abra los archivos PST con Microsoft Outlook.

   Los archivos PST resultantes podrían tener un tamaño mucho menor que el buzón original. Eso es normal.

Importante

No importe estos archivos a Microsoft Outlook usando el **Asistente para importación y exportación**.

Abra los archivos haciendo doble clic en ellos o haciendo clic con el botón derecho y seleccionando **Abrir con...** > **Microsoft Outlook** en el menú contextual.

Recuperación de carpetas públicas y elementos de carpeta

Para recuperar una carpeta pública y elementos de carpeta pública, al menos un administrador de la organización de Microsoft 365 de destino debe tener derechos de **Propietario** para la carpeta pública de destino. Si se produce un error de acceso denegado en la recuperación, asigne estos derechos en las propiedades de la carpeta de destino, seleccione la organización de destino en la consola de Cyber Protect, haga clic en **Actualizar** y, después, repita la recuperación.

Pasos para recuperar una carpeta pública o elementos de carpeta

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, amplíe la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Amplíe el nodo **Carpetas públicas**, seleccione **Todas las carpetas públicas**, elija la carpeta pública que quiera recuperar o que originalmente contenía los elementos que quiera recuperar y, después, haga clic en **Recuperación**.
   - Si la carpeta pública se ha eliminado, selecciónela en la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar Carpetas públicas por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar datos**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de los elementos necesarios.

   Puede buscar los mensajes de correo electrónico y publicaciones por asunto, remitente, destinatario y fecha. No se pueden usar caracteres comodín.
7. Seleccione los elementos que desea recuperar. Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 

   También puede optar por una de las siguientes opciones:

© Acronis International GmbH, 2003-2025

- Cuando un mensaje de correo electrónico o publicación esté seleccionado, haga clic en **Mostrar contenido** para ver lo que se incluye, incluidos los adjuntos. Haga clic en el nombre de un archivo adjunto para descargarlo.
- Cuando un mensaje de correo electrónico o una publicación esté seleccionado, haga clic en **Enviar como correo electrónico** para enviar el elemento a la dirección de correo electrónico especificada. Puede seleccionar el remitente y escribir un texto para añadirlo al elemento reenviado.
- Únicamente si la copia de seguridad no está cifrada, ha usado la búsqueda y ha seleccionado un único elemento de la lista de resultados de búsqueda: haga clic en **Mostrar versiones** para seleccionar la versión del elemento que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.

8. Haga clic en **Recuperar**.
9. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
10. En **Recuperar a la carpeta pública**, puede consultar, cambiar o especificar la carpeta pública de destino.

    De manera predeterminada se selecciona la carpeta original. Si esta carpeta no existe o se selecciona una organización que no es la original, debe indicar la carpeta de destino.

    No puede crear una nueva carpeta pública durante la recuperación. Para recuperar una carpeta pública en una nueva, primero necesita crear la carpeta pública de destino en la organización de Microsoft 365 deseada y, a continuación, dejar que el agente en la nube sincronice el cambio. El agente en la nube se sincroniza automáticamente con Microsoft 365 cada 24 horas. Para sincronizar el cambio inmediatamente, en la consola den Cyber Protect, seleccione la organización en la página **Microsoft 365** y luego haga clic en **Actualizar**.
11. En **Ruta**, vea o cambie la subcarpeta de destino en la carpeta pública de destino. De manera predeterminada, se recreará la ruta original.
12. Haga clic en **Iniciar recuperación**.
13. Seleccione una de las opciones de sobreescritura:

Opción	Descripción
Sobrescribir elementos existentes	Todos los archivos existentes en la ubicación de destino se sobrescribirán.
No sobrescribir elementos existentes	Si la ubicación de destino contiene un archivo con el mismo nombre, ese archivo no se sobrescribirá y el archivo de origen no se guardará en la ubicación de destino.

© Acronis International GmbH, 2003-2025

14. Haga clic en **Continuar** para confirmar su decisión.

Protección de archivos de OneDrive

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de un OneDrive completo, o bien de archivos o carpetas individuales.

Una opción independiente del plan de copias de seguridad habilita la copia de seguridad de los cuadernos de OneNote.

Los archivos se incluyen en la copia de seguridad junto con sus permisos para compartir. Los niveles de permiso avanzados (**Diseño**, **Completo**, **Contribuir**) no se pueden incluir en las copias de seguridad.

Algunos archivos pueden contener información confidencial y el acceso a ellos puede quedar bloqueado por una regla de prevención de pérdida de datos (DLP) en Microsoft 365. No se realizará copia de seguridad de estos archivos y no se muestran advertencias después de que se complete la operación de copia de seguridad.

Limitaciones

La creación de la copia de seguridad del contenido de OneDrive no es compatible con los buzones de correo compartidos. Para realizar la copia de seguridad de este contenido, convierta el buzón de correo compartido a una cuenta de usuario regular y asegúrese de que OneDrive está habilitado para esa cuenta.

¿Qué elementos de datos pueden recuperarse?

Puede recuperar un OneDrive completo, o bien cualquier archivo o carpeta incluida en una copia de seguridad.

Puede usar la búsqueda para localizar los elementos.

Puede elegir entre recuperar los permisos para compartir o permitir que los archivos hereden los permisos de la carpeta desde donde se recuperan.

Los enlaces para compartir para los archivos y las carpetas no se recuperan.

Selección de archivos de OneDrive

Seleccione los archivos tal como se describe a continuación y, luego, especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar archivos de OneDrive

© Acronis International GmbH, 2003-2025

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos de los usuarios quiera recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para realizar una copia de seguridad de los archivos de todos los usuarios (incluidos los que se crearan en el futuro), amplíe el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de los archivos de usuarios individuales, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los usuarios cuyos archivos quiera recuperar y haga clic en **Copia de seguridad**.
4. En el plan de copias de seguridad, configure lo siguiente:
   - [Si está disponible] En **Qué incorporar en la copia de seguridad**, seleccione **OneDrive**.
     Si alguno de los usuarios seleccionados individualmente no tiene el servicio de OneDrive incluido en su plan Microsoft 365, no podrá elegir esta opción.
     Si alguno de los usuarios seleccionados para la copia de seguridad en grupo no tiene el servicio de OneDrive incluido en su plan Microsoft 365, no podrá elegir esta opción, pero el plan de protección no se aplicará a dichos usuarios.
   - En **Elementos que se incluirán en la copia de seguridad**, realice uno de los siguientes procedimientos:
     - Mantenga los ajustes predeterminados **[Todos]** (todos los archivos).
     - Especifique los archivos y las carpetas que quiere incluir en la copia de seguridad. Para ello, añada sus nombres o rutas.
       Puede usar los caracteres comodín (*, ** y ?). Para obtener más información sobre la especificación de rutas y el uso de los caracteres comodín, consulte "Filtros de archivo (inclusiones y exclusiones)" (p. 607).
     - Examine los archivos y las carpetas para especificar cuáles quiere incluir en la copia de seguridad.
       El enlace **Examinar** está disponible únicamente cuando se crea un plan de protección para un solo usuario.
   - En **Cifrado**, haga clic en **Especificar contraseña**.
     - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
     - Haga clic en **Aceptar**.
   - [Opcional] En **Elementos que se incluirán en la copia de seguridad**, haga clic en **Mostrar exclusiones** para especificar los archivos y las carpetas que quiere excluir durante la realización de la copia de seguridad.
     Las exclusiones de archivos sobrescriben la selección de estos. Si especifica el mismo archivo en ambos campos, este archivo se omitirá durante el proceso de realización de la copia de seguridad.

© Acronis International GmbH, 2003-2025

- [Opcional] Para hacer copias de seguridad de blocs de notas de OneNote, active el conmutador **Incluir OneNote**.

Recuperación de OneDrive y archivos de OneDrive

Recuperación de un OneDrive completo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario cuyo OneDrive quiera recuperar y haga clic en **Recuperación**.

   Si se ha eliminado el usuario, seleccione el usuario de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

   Nota
   Para ver únicamente los puntos de recuperación que incluyan archivos de OneDrive, seleccione **OneDrive** en **Filtrar por contenido**.
5. Haga clic en **Recuperar** > **Todo OneDrive**.
6. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.

   No se puede crear un nuevo destino de OneDrive durante la recuperación. Para la recuperación de OneDrive a uno nuevo, primero necesita crear el destino de OneDrive en la organización de Microsoft 365 y, después, dejar que el agente en la nube sincronice el cambio. El agente en la nube se sincroniza automáticamente con Microsoft 365 cada 24 horas. Para sincronizar el cambio inmediatamente, en la consola den Cyber Protect, seleccione la organización en la página **Microsoft 365** y luego haga clic en **Actualizar**.
7. En **Recuperar a la unidad** puede consultar, cambiar o especificar el usuario de destino.

   De manera predeterminada, se selecciona el usuario original. Si este usuario no existe o se selecciona una organización que no es la original, debe indicar el usuario de destino.
8. Seleccione si quiere recuperar los permisos para compartir de los archivos.
9. Haga clic en **Iniciar recuperación**.
10. Seleccione una de las opciones de sobreescritura:

© Acronis International GmbH, 2003-2025

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir archivos existentes	Todos los archivos existentes en la ubicación de destino se sobrescribirán, independientemente de la última fecha de modificación.
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

Nota
Al recuperar los blocs de notas de OneNote, las opciones **Sobrescribir un archivo existente si es más antiguo** como **Sobrescribir archivos existentes** sobrescribirán los blocs de notas de OneNote existentes.

11. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de archivos de OneDrive

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario cuyos archivos de OneDrive quiera recuperar y haga clic en **Recuperación**.
   Si se ha eliminado el usuario, seleccione el usuario de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
   Puede buscar usuarios por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

   Nota
   Para ver únicamente los puntos de recuperación que incluyan archivos de OneDrive, seleccione **OneDrive** en **Filtrar por contenido**.

5. Haga clic en **Recuperar** > **Archivos/carpetas**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de archivos y carpetas deseados.
7. Seleccione los archivos que desea recuperar.
   Si la copia de seguridad no está cifrada y ha seleccionado un único archivo, puede hacer clic en **Mostrar versiones** para seleccionar la versión del archivo que quiera recuperar. Puede elegir

© Acronis International GmbH, 2003-2025

cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.

8. Si desea descargar un archivo, selecciónelo, haga clic en **Descargar**, seleccione la ubicación en la que se guardará y, a continuación, haga clic en **Guardar**. De lo contrario, omita este paso.
9. Haga clic en **Recuperar**.
10. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

    De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.

    No puede crear un nuevo OneDrive durante la recuperación. Para la recuperación de un archivo en un nuevo OneDrive, primero necesita crear el OneDrive de destino en la organización de Microsoft 365 deseada y, a continuación, dejar que el agente en la nube sincronice el cambio. El agente en la nube se sincroniza automáticamente con Microsoft 365 cada 24 horas. Para sincronizar el cambio inmediatamente, en la consola den Cyber Protect, seleccione la organización en la página **Microsoft 365** y luego haga clic en **Actualizar**.
11. En **Recuperar a la unidad** puede consultar, cambiar o especificar el usuario de destino.

    De manera predeterminada, se selecciona el usuario original. Si este usuario no existe o se selecciona una organización que no es la original, debe indicar el usuario de destino.
12. En **Ruta** puede consultar o cambiar la carpeta de destino en el OneDrive del usuario de destino. De manera predeterminada se selecciona la ubicación original.
13. Seleccione si quiere recuperar los permisos para compartir de los archivos.
14. Haga clic en **Iniciar recuperación**.
15. Seleccione una de las opciones de sobreescritura de archivos:

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir archivos existentes	Todos los archivos existentes en la ubicación de destino se sobrescribirán, independientemente de la última fecha de modificación.
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

Nota

Al recuperar los blocs de notas de OneNote, las opciones **Sobrescribir un archivo existente si es más antiguo** como **Sobrescribir archivos existentes** sobrescribirán los blocs de notas de OneNote existentes.

© Acronis International GmbH, 2003-2025

16. Haga clic en **Continuar** para confirmar su decisión.

Protección de sitios de SharePoint Online

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de los sitios de comunicación clásicos de SharePoint y de los sitios de equipo modernos. Puede seleccionar subsitios, listas y bibliotecas individuales para realizar copias de seguridad.

A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

Una opción independiente del plan de copias de seguridad habilita la copia de seguridad de los cuadernos de OneNote.

Los siguientes elementos *no se incluyen* al realizar una copia de seguridad:

- La configuración del sitio **Aspecto y diseño** (excepto el **título, la descripción y el logotipo**).
- Los comentarios de la página del sitio y su configuración (comentarios **activados**/**desactivados**).
- La configuración del sitio **Características del sitio**.
- Las páginas de partes de webs y las partes de webs integradas en las páginas de wikis (por limitaciones de la API de SharePoint Online).
- Archivos comprobados: archivos que se comprueban manualmente para su edición y todos aquellos archivos que se crean o cargan en bibliotecas, para los que la opción **Requerir comprobación** está habilitada. Para realizar una copia de seguridad de estos archivos primero tiene que comprobarlos.
- Datos externos y los tipos de columna "Metadatos gestionados".
- La recopilación de sitios predeterminada "domain-my.sharepoint.com". Es una recopilación en la que se encuentran los archivos de OneDrive de todos los usuarios de la organización.
- El contenido de la papelera de reciclaje.

Limitaciones

- Los títulos y las descripciones de sitios, subsitios, listas y columnas se truncan durante una copia de seguridad si el título o la descripción tiene un tamaño superior a 10 000 bytes.
- No puede realizar una copia de seguridad de versiones anteriores de archivos creados en SharePoint Online. Solo las versiones más recientes de los archivos están protegidas.
- No puede realizar una copia de seguridad de la biblioteca de suspensión para conservación.
- No se puede realizar una copia de seguridad de sitios creados en Business Productivity Online Suite (BPOS), el predecesor de Microsoft 365.

© Acronis International GmbH, 2003-2025

- No se puede realizar una copia de seguridad de la configuración de sitios que utilizan la ruta gestionada `/portals` (por ejemplo, `https://<tenant>.sharepoint.com/portals/...`).
- La configuración de Information Rights Management (IRM) de una lista o una biblioteca puede recuperarse solo si IRM está activado en la organización Microsoft 365 de destino.

¿Qué elementos de datos pueden recuperarse?

Los siguientes elementos pueden recuperarse de la copia de seguridad de un sitio:

- Sitio completo
- Subsitios
- Listas
- Elementos de lista
- Bibliotecas de documentos
- Documentos
- Adjuntos de elementos de lista
- Páginas de sitios y de wikis

Puede usar la búsqueda para localizar los elementos.

Elementos que se pueden recuperar en el sitio original o en uno nuevo. La ruta de un elemento recuperado es la misma que la del original. Si la ruta no existe, se crea.

Puede elegir entre recuperar los permisos para compartir o permitir que los elementos hereden los permisos del objeto primario después de la recuperación.

¿Qué elementos no se pueden recuperar?

- Subsitios basados en la plantilla **Visio Process Repository**.
- Listas de los tipos siguientes: **Encuesta**, **Tareas**, **Biblioteca de imágenes**, **Enlaces**, **Calendario**, **Foro de discusión**, **Externa** y **Hoja de cálculo de importación**.
- Las listas con varios tipos de contenido que estén habilitadas.

Selección de los datos de SharePoint Online

Seleccione los datos tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar datos de SharePoint Online

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos de los usuarios quiera recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:

© Acronis International GmbH, 2003-2025

- Para realizar una copia de seguridad de todos los sitios de SharePoint clásicos de la organización, incluidos los sitios que se crearán en el futuro, amplíe el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios** y haga clic en **Agrupar copia de seguridad**.
- Para realizar una copia de seguridad de sitios clásicos individuales, amplíe el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios**, elija los sitios que quiere incluir en la copia de seguridad y haga clic en **Copia de seguridad**.
- Para realizar una copia de seguridad de los sitios de todos los grupos (equipo moderno), incluidos los sitios que se crearán en el futuro, amplíe el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Agrupar copia de seguridad**.

  Nota
  A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

- Para realizar una copia de seguridad de los sitios de grupos individuales (equipo moderno), amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija los grupos de cuyos sitios quiera realizar una copia de seguridad y haga clic en **Copia de seguridad**.

  Nota
  A partir de Cyber Protect Cloud 25.06, los grupos no protegidos que son parte de un equipo no se muestran en **Dispositivos** > **Microsoft 365** > Organización de Microsoft 365 > **Grupos**. Puede proteger el sitio de SharePoint y el buzón de correo del grupo de estos grupos aplicando un plan de copias de seguridad a todo el equipo. Para obtener más información, consulte "Protección de Microsoft 365 Teams" (p. 879).

4. En el plan de copias de seguridad, configure lo siguiente:
   - En **Elementos que se incluirán en la copia de seguridad**, realice uno de los siguientes procedimientos:
     - Mantenga los ajustes predeterminados **[Todos]** (todos los elementos de los sitios seleccionados).
     - Especifique los subsitios, las listas y las bibliotecas que quiere incluir en la copia de seguridad. Para ello, añada sus nombres o rutas.

       Para realizar una copia de seguridad de un subsitio, o bien una biblioteca, lista o sitio de máximo nivel, especifique su nombre para mostrar con el siguiente formato: `/display name/**`

       Para realizar una copia de seguridad de un subsitio, una biblioteca o una lista, especifique su nombre para mostrar con el siguiente formato: `/subsite display name/list display name/**`

© Acronis International GmbH, 2003-2025

Los nombres para mostrar de los subsitios, las listas y las bibliotecas aparecen en la página **Contenidos del sitio** del sitio o el subsitio de SharePoint.

- Examine los subsitios para especificar cuáles quiere incluir en la copia de seguridad.

  El enlace **Examinar** está disponible únicamente cuando se crea un plan de protección para un solo sitio.

- [Opcional] En **Elementos que se incluirán en la copia de seguridad**, haga clic en **Mostrar exclusiones** para especificar los subsitios, las listas y las bibliotecas que quiere excluir durante la realización de la copia de seguridad.

  Las exclusiones de elementos sobrescriben la selección de estos, es decir, si especifica el mismo subsitio en los dos campos, este subsitio se omitirá durante el proceso de realización de la copia de seguridad.
- En **Programar**, seleccione la frecuencia de la copia de seguridad.

  Esta opción es configurable si el paquete **Advanced Backup** está habilitado para este cliente. Para obtener más información, consulte "Configuración de la frecuencia de las copias de seguridad de Microsoft 365" (p. 847).
- En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.
- En **Cifrado**, haga clic en **Especificar contraseña**.
  - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
  - Haga clic en **Aceptar**.
- [Opcional] Para hacer copias de seguridad de blocs de notas de OneNote, active el conmutador **Incluir OneNote**.

Recuperación de datos de SharePoint Online

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para recuperar los datos del sitio de un grupo (equipo moderno), amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija el grupo en cuyo sitio se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Para recuperar los datos de un sitio clásico, amplíe el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios**, elija el sitio en el que se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.
   - Si el sitio se ha eliminado, selecciónelo en la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar grupos y sitios por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

© Acronis International GmbH, 2003-2025

Nota
Para ver únicamente los puntos de recuperación que incluyan sitios de SharePoint, seleccione **Sitios de SharePoint** en **Filtrar por contenido**.

5. Haga clic en **Recuperar archivos de SharePoint**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de los elementos de datos necesarios.
7. Seleccione los elementos que desea recuperar.

   Si la copia de seguridad no está cifrada, ha usado la búsqueda y ha seleccionado un único elemento de la lista de resultados de búsqueda, puede hacer clic en **Mostrar versiones** para seleccionar la versión del elemento que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.
8. [Opcional] Para descargar un elemento, selecciónelo, haga clic en **Descargar**, seleccione la ubicación en la que desea guardarlo y, a continuación, haga clic en **Guardar**.
9. Haga clic en **Recuperar**.
10. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

    De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
11. En **Recuperar al sitio** puede consultar, cambiar o especificar el sitio de destino.

    No puede crear un nuevo sitio de SharePoint durante la recuperación. Para recuperar un sitio de SharePoint en uno nuevo, primero necesita crear el sitio de destino en la organización de Microsoft 365 deseada y, a continuación, dejar que el agente en la nube sincronice el cambio. El agente en la nube se sincroniza automáticamente con Microsoft 365 cada 24 horas. Para sincronizar el cambio inmediatamente, en la consola den Cyber Protect, seleccione la organización en la página **Microsoft 365** y luego haga clic en **Actualizar**.
12. Seleccione si quiere recuperar los permisos para compartir de los elementos recuperados.

    Se recuperan los permisos de uso compartido tanto para los usuarios internos como para los externos.
13. Haga clic en **Iniciar recuperación**.
14. Seleccione una de las opciones de sobreescritura:

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir archivos	Todos los archivos existentes en la ubicación de destino se sobrescribirán, independientemente de la última fecha de modificación.

© Acronis International GmbH, 2003-2025

Opción	Descripción
existentes	
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

Nota
Al recuperar los blocs de notas de OneNote, las opciones **Sobrescribir un archivo existente si es más antiguo** como **Sobrescribir archivos existentes** sobrescribirán los blocs de notas de OneNote existentes.

15. Haga clic en **Continuar** para confirmar su decisión.

Protección de Microsoft 365 Teams

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de equipos enteros. Estas copias incluyen el nombre del equipo, la lista de miembros, los canales y su contenido, los buzones y reuniones, y el sitio.

Una opción independiente del plan de copias de seguridad habilita la copia de seguridad de los cuadernos de OneNote.

¿Qué elementos de datos pueden recuperarse?

- Todo el equipo
- Canales del equipo
- Archivos del canal
- Buzón de correo del equipo
- Carpetas de correo electrónico en el buzón del equipo
- Mensajes de correo electrónico en el buzón del equipo
- Reuniones
- Sitio de equipo

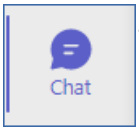
No se pueden recuperar las conversaciones de los canales del equipo, pero sí puede descargarlas como un solo archivo html.

Limitaciones

Los siguientes elementos no se incluyen en las copias de seguridad:

- La configuración del canal general (preferencias de moderación), debido a una limitación de la API beta de Microsoft Teams.

© Acronis International GmbH, 2003-2025

- La configuración de los canales personalizados (preferencias de moderación), debido a una limitación de la API beta de Microsoft Teams.
- Notas de las reuniones.
- Mensajes en la sección de chat 

. Esta sección contiene chats privados unipersonales y chats grupales.
- Pegatinas y elogios.

La copia de seguridad y la recuperación son compatibles con las siguientes pestañas de canal:

- Word
- Excel
- PowerPoint
- PDF
- Biblioteca de documentos

Selección de equipos

Seleccione los equipos tal como se describe a continuación y especifique otros ajustes del plan de protección según corresponda.

Para seleccionar equipos

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos quiera recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para realizar una copia de seguridad de todos los equipos de la organización (incluidos los que se crearán en el futuro), amplíe el nodo **Teams**, seleccione **Todos los equipos** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de equipos individuales, amplíe el nodo **Teams**, seleccione **Todos los equipos**, elija los equipos que quiere incluir en la copia de seguridad y haga clic en **Copia de seguridad**.

   Puede buscar equipos por el nombre. No se pueden usar caracteres comodín.
4. En el plan de copias de seguridad, configure lo siguiente:
   - En **Programar**, seleccione la frecuencia de la copia de seguridad.

     Esta opción es configurable si el paquete **Advanced Backup** está habilitado para este cliente. Para obtener más información, consulte "Configuración de la frecuencia de las copias de seguridad de Microsoft 365" (p. 847).
   - En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.

© Acronis International GmbH, 2003-2025

- En **Cifrado**, haga clic en **Especificar contraseña**.
  - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
  - Haga clic en **Aceptar**.
- [Opcional] Para hacer copias de seguridad de blocs de notas de OneNote, active el conmutador **Incluir OneNote**.

Recuperación de un equipo completo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Teams**, seleccione **Todos los equipos**, elija el usuario cuyo equipo quiera recuperar y haga clic en **Recuperación**.
   Puede buscar equipos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Todo el equipo**.
   Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.
   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
6. En **Recuperar a equipo**, vea el equipo de destino o seleccione otro.
   De manera predeterminada, se selecciona el equipo original. Si este equipo no existe, (por ejemplo, se eliminó) o ha seleccionado una organización que no contiene el equipo original, debe seleccionar un equipo de destino en la lista desplegable.
   Puede recuperar un equipo solo en un equipo existente. No puede crear equipos durante las operaciones de recuperación.
7. Haga clic en **Iniciar recuperación**.
8. Seleccione una de las opciones de sobreescritura:
   - **Sobrescribir contenido existente si es anterior**
   - **Sobrescribir contenido existente**
   - **No sobrescribir contenido existente**

   Nota
   Al recuperar los blocs de notas de OneNote, tanto la opción **Sobrescribir contenido existente si es anterior** como **Sobrescribir contenido existente** sobrescribirán los blocs de notas de OneNote existentes.
9. Haga clic en **Continuar** para confirmar su decisión.

© Acronis International GmbH, 2003-2025

Cuando elimina un canal en la interfaz gráfica de Microsoft Teams, no se elimina inmediatamente del sistema. Por tanto, cuando recupera el equipo entero, el nombre de este canal no se puede utilizar y se le añadirá un postfijo.

Las conversaciones se recuperan como un solo archivo html en la pestaña **Archivos** del canal. Puede encontrar este archivo en una carpeta denominada según el siguiente patrón: `<Team name>_<Channel name>_conversations_backup_<date of recovery>T<time of recovery>Z`.

Nota
Después de recuperar un equipo o los canales de un equipo, vaya a Microsoft Teams, seleccione los canales recuperados y haga clic en su pestaña **Archivos**. De lo contrario, las copias de seguridad posteriores de estos canales no incluirán el contenido de esta pestaña debido a una limitación de la API beta de Microsoft Teams.

Cómo recuperar canales de equipo o archivos de canales de equipo

Para recuperar canales de equipo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Teams**, seleccione **Todos los equipos**, seleccione el equipo cuyos canales quiera recuperar y haga clic en **Recuperación**.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Canales**.
6. Seleccione los canales que desea recuperar y, a continuación, haga clic en **Recuperar**. Para seleccionar un canal en el panel principal, marque la casilla de verificación que hay delante de su nombre.

   Tiene a su disposición las siguientes opciones de búsqueda:
   - Para **Conversaciones**: asunto, remitente, contenido, idioma, nombre de adjunto, fecha o intervalo de fechas.
   - Para **Archivos**: nombre de archivo o nombre de carpeta, tipo de archivo, tamaño, fecha o intervalo de fechas del último cambio.

   Nota
   También puede descargar los archivos de forma local en lugar de recuperarlos.
7. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
8. En **Recuperar al equipo**, puede consultar, cambiar o especificar el equipo de destino.

© Acronis International GmbH, 2003-2025

De manera predeterminada, se selecciona el equipo original. Si este equipo no existe o se selecciona una organización que no es la original, debe indicar el equipo de destino.

9. En **Recuperar al canal**, puede consultar, cambiar o especificar el canal de destino.
10. Haga clic en **Iniciar recuperación**.
11. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir contenido existente si es anterior**
    - **Sobrescribir contenido existente**
    - **No sobrescribir contenido existente**

    Nota
    Al recuperar los blocs de notas de OneNote, tanto la opción **Sobrescribir contenido existente si es anterior** como **Sobrescribir contenido existente** sobrescribirán los blocs de notas de OneNote existentes.
12. Haga clic en **Continuar** para confirmar su decisión.

Las conversaciones se recuperan como un solo archivo html en la pestaña **Archivos** del canal. Puede encontrar este archivo en una carpeta denominada según el siguiente patrón: `<Team name>_<Channel name>_conversations_backup_<date of recovery>T<time of recovery>Z`.

Nota
Después de recuperar un equipo o los canales de un equipo, vaya a Microsoft Teams, seleccione los canales recuperados y haga clic en su pestaña **Archivos**. De lo contrario, las copias de seguridad posteriores de estos canales no incluirán el contenido de esta pestaña debido a una limitación de la API beta de Microsoft Teams.

Para recuperar archivos en un canal de equipo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Teams**, seleccione **Todos los equipos**, seleccione el equipo cuyos canales quiera recuperar y haga clic en **Recuperación**.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Canales**.
6. Seleccione el canal deseado y después abra la carpeta **Archivos**.
   Vaya hasta los elementos requeridos o utilice la función de búsqueda para obtener la lista de los elementos necesarios. Están disponibles las siguientes opciones de búsqueda: nombre de archivo o nombre de carpeta, tipo de archivo, tamaño, fecha o intervalo de fechas del último cambio.

© Acronis International GmbH, 2003-2025

7. [Opcional] Para descargar un elemento, selecciónelo, haga clic en **Descargar**, seleccione la ubicación en la que desea guardarlo y, a continuación, haga clic en **Guardar**.
8. Seleccione los elementos que desea recuperar y, a continuación, haga clic en **Recuperar**
9. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en la organización de Microsoft 365 para verla, modificarla o especificar la organización de destino.
   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
10. En **Recuperar al equipo**, puede consultar, cambiar o especificar el equipo de destino.
    De manera predeterminada, se selecciona el equipo original. Si este equipo no existe o se selecciona una organización que no es la original, debe indicar el equipo de destino.
11. En **Recuperar al canal**, puede consultar, cambiar o especificar el canal de destino.
12. Seleccione si quiere recuperar los permisos para compartir de los elementos recuperados.
13. Haga clic en **Iniciar recuperación**.
14. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir contenido existente si es anterior**
    - **Sobrescribir contenido existente**
    - **No sobrescribir contenido existente**

    Nota
    Al recuperar los blocs de notas de OneNote, tanto la opción **Sobrescribir contenido existente si es anterior** como **Sobrescribir contenido existente** sobrescribirán los blocs de notas de OneNote existentes.
15. Haga clic en **Continuar** para confirmar su decisión.

No se pueden recuperar conversaciones individuales. En el panel principal, solo puede examinar la carpeta **Conversación** o descargar su contenido como un solo archivo html. Para hacerlo, haga clic en el icono "recuperar carpetas"  , seleccione la carpeta **Conversaciones** deseada y haga clic en **Descargar**.

Puede buscar en los mensajes de la carpeta **Conversación** según los siguientes criterios:

- Remitente
- Contenido
- Nombre de adjunto
- Fecha

© Acronis International GmbH, 2003-2025

Recuperación del buzón de correo de un equipo

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Teams**, seleccione **Todos los equipos**, elija el equipo cuyos buzones quiera recuperar y haga clic en **Recuperación**.
   Puede buscar equipos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
6. Haga clic en el icono "recuperar carpetas"  , seleccione la carpeta raíz del buzón de correo y haga clic en **Recuperar**.

   Nota
   También puede recuperar carpetas individuales desde el buzón de correo seleccionado.

7. Haga clic en **Recuperar**.
8. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.
   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
9. En **Recuperar al buzón de correo**, puede consultar, cambiar o especificar el buzón de correo de destino.
   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona una organización que no es la original, debe indicar el buzón de correo de destino.
10. Haga clic en **Iniciar recuperación**.
11. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir elementos existentes**
    - **No sobrescribir elementos existentes**
12. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de elementos del buzón de correo del equipo en archivos PST

Pasos para recuperar elementos del buzón de correo del equipo

© Acronis International GmbH, 2003-2025

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
4. Amplíe el nodo **Equipos**, seleccione **Todos los equipos**, elija un equipo en cuyo buzón de correo se encontrasen de forma original los elementos que desea recuperar y haga clic en **Recuperación**.
5. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de los elementos necesarios.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.
   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario, nombre del adjunto y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.
7. Seleccione los elementos que desea recuperar. Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 

   También puede optar por una de las siguientes opciones:
   - Cuando un elemento está seleccionado, haga clic en **Mostrar contenido** para ver lo que se incluye, incluidos los adjuntos. Haga clic en el nombre de un archivo adjunto para descargarlo.
   - Cuando un mensaje de correo electrónico o el elemento de un calendario esté seleccionado, haga clic en **Enviar como correo electrónico** para enviar el elemento a la dirección de correo electrónico especificada. Puede seleccionar el remitente y escribir un texto para añadirlo al elemento reenviado.
   - Si la copia de seguridad no está cifrada, ha usado la búsqueda y ha seleccionado un único elemento de la lista de resultados de búsqueda: haga clic en **Mostrar versiones** para ver la versión del elemento. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, independientemente de si es anterior o posterior al punto de recuperación seleccionado.
8. Haga clic en **Recuperar como archivos PST**.
9. Configure la contraseña para cifrar el archivo comprimido con los archivos PST.

   La contraseña debe contener al menos un símbolo.
10. Confirme la contraseña y haga clic en **LISTO**.

Los elementos del buzón de correo seleccionado se recuperarán como archivos de datos PST y se comprimirán en formato zip. El tamaño máximo de un archivo PST se limita a 2 GB, por lo que si los

© Acronis International GmbH, 2003-2025

datos que va a recuperar exceden los 2 GB, se dividirán en varios archivos PST. El archivo zip estará protegido con la contraseña que configure.

Recibirá un correo electrónico con un enlace a un archivo zip que contine los archivos PST creados.

El administrador recibirá un correo electrónico para informarle de que ha realizado el procedimiento de recuperación.

Pasos para descargar el archivo comprimido con los archivos pst y completar la recuperación

1. Realice uno de los siguientes procedimientos:
   - Para descargar el archivo comprimido desde el correo electrónico, siga el enlace **Descargar archivos**.
     El archivo comprimido estará disponible para descargar en un plazo de 24 horas. Si el enlace caduca, repita el procedimiento de recuperación.
   - Para descargar el archivo comprimido de la consola de Cyber Protect:
     a. Vaya a **Almacenamiento de la copia de seguridad** > **Archivos PST**.
     b. Seleccione el archivo destacado más reciente.
     c. En el panel derecho, haga clic en **Descargar**.

   El archivo comprimido se descargará en el directorio de descargas predeterminado de su ordenador.
2. Extraiga los archivos PST del archivo comprimido con la contraseña que configuró para cifrar el archivo comprimido.
3. En Microsoft Outlook, abra o importe los archivos PST. Para obtener más información sobre cómo hacerlo, consulte la documentación de Microsoft.

Recuperar mensajes de correo electrónico y reuniones

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Teams**, seleccione **Todos los equipos**, elija el equipo cuyos mensajes de correo electrónico o reuniones quiera recuperar y haga clic en **Recuperación**.
   Puede buscar equipos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
6. Vaya hasta el elemento requerido o utilice la función de búsqueda para obtener la lista de los elementos necesarios.
   Tiene a su disposición las siguientes opciones de búsqueda:
   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario y fecha.
   - Para reuniones: busque por nombre y fecha del evento.

© Acronis International GmbH, 2003-2025

7. Seleccione los elementos que desea recuperar y, a continuación, haga clic en **Recuperar**.

   Nota
   Puede encontrar las reuniones en la carpeta **Calendario**.

   También puede optar por una de las siguientes opciones:
   - Cuando un elemento está seleccionado, haga clic en **Mostrar contenido** para ver lo que se incluye, incluidos los adjuntos. Haga clic en el nombre de un archivo adjunto para descargarlo.
   - Cuando un mensaje de correo electrónico o una reunión esté seleccionado, haga clic en **Enviar como correo electrónico** para enviar el elemento a la dirección de correo electrónico especificada. Puede seleccionar el remitente y escribir un texto para añadirlo al elemento reenviado.
8. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.
   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
9. En **Recuperar al buzón de correo**, puede consultar, cambiar o especificar el buzón de correo de destino.
   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona una organización que no es la original, debe indicar el buzón de correo de destino.
10. Haga clic en **Iniciar recuperación**.
11. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir elementos existentes**
    - **No sobrescribir elementos existentes**
12. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de un sitio de equipo o de elementos específicos de un sitio

1. Haga clic en **Microsoft 365**.
2. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, seleccione la organización cuyos equipos incluidos en la copia desee recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Teams**, seleccione **Todos los equipos**, seleccione el equipo cuyo sitio quiera recuperar y haga clic en **Recuperación**.
   Puede buscar equipos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Sitio de equipo**.
6. Vaya hasta el elemento requerido o utilice la función de búsqueda para obtener la lista de los elementos necesarios.

© Acronis International GmbH, 2003-2025

7. [Opcional] Para descargar un elemento, selecciónelo, haga clic en **Descargar**, seleccione la ubicación en la que desea guardarlo y, a continuación, haga clic en **Guardar**.
8. Seleccione los elementos que desea recuperar y, a continuación, haga clic en **Recuperar**.
9. Si se añadieron varias organizaciones de Microsoft 365 al servicio Cyber Protection, haga clic en **la organización de Microsoft 365** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización y el equipo originales. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe especificar la organización de destino.
10. En **Recuperar al equipo**, puede consultar, cambiar o especificar el equipo de destino.

    De manera predeterminada, se selecciona el equipo original. Si este equipo no existe o se selecciona una organización que no es la original, debe indicar el sitio de destino.
11. Seleccione si quiere recuperar los permisos para compartir de los elementos recuperados.
12. Haga clic en **Iniciar recuperación**.
13. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir contenido existente si es anterior**
    - **Sobrescribir contenido existente**
    - **No sobrescribir contenido existente**

    Nota
    Al recuperar los blocs de notas de OneNote, tanto la opción **Sobrescribir contenido existente si es anterior** como **Sobrescribir contenido existente** sobrescribirán los blocs de notas de OneNote existentes.
14. Haga clic en **Continuar** para confirmar su decisión.

Protección de cuadernos de OneNote

De forma predeterminada, los cuadernos de OneNote se incluyen en las copias de seguridad de los archivos de OneDrive, Microsoft Teams y los sitios de SharePoint.

Para excluir los cuadernos de OneNote de estas copias de seguridad, deshabilite el conmutador **Incluir OneNote** en el plan de copias de seguridad correspondiente.

Recuperación de blocs de notas de OneNote de los que se han hecho copia de seguridad

Para saber cómo recuperar un bloc de notas de OneNote del que se ha hecho una copia de seguridad, consulte el tema correspondiente:

- Para copias de seguridad de OneDrive, consulte "Recuperación de un OneDrive completo" (p. 871) o "Recuperación de archivos de OneDrive" (p. 872).

© Acronis International GmbH, 2003-2025

- Para copias de seguridad de Teams, consulte "Recuperación de un equipo completo" (p. 881), "Cómo recuperar canales de equipo o archivos de canales de equipo" (p. 882) o "Recuperación de un sitio de equipo o de elementos específicos de un sitio" (p. 888).
- Para copias de seguridad del sitio de SharePoint, consulte "Recuperación de datos de SharePoint Online" (p. 877).

Versiones compatibles

- OneNote (OneNote 2016 y posteriores)
- OneNote para Windows 10

Limitaciones y problemas conocidos

- Los cuadernos de OneNote guardados en OneDrive o SharePoint tienen un límite de 2 GB. No puede recuperar cuadernos de OneNote de mayor tamaño en destinos de OneDrive o SharePoint.
- No se admiten cuadernos de OneNote con grupos de sección.
- En los cuadernos de OneNote de los que se ha hecho una copia de seguridad y que contienen secciones con nombres que no son predeterminados, la primera sección se muestra con el nombre predeterminado (como `Nueva sección` o `Sección sin título`). Esto podría afectar al orden de las secciones en los cuadernos que incluyan varias.
- Al recuperar los blocs de notas de OneNote, tanto la opción **Sobrescribir contenido existente si es anterior** como **Sobrescribir contenido existente** sobrescribirán los blocs de notas de OneNote existentes.
- Cuando recupere todo un equipo, un sitio de equipo o la carpeta `Recursos del sitio` de un sitio de equipo, si ha seleccionado la opción **Sobrescribir contenido existente si es anterior** o **Sobrescribir contenido existente**, el bloc de notas de OneNote predeterminado de ese equipo no se sobrescribirá. La recuperación se realiza correctamente, con la advertencia *No se han podido actualizar las propiedades del archivo "/sites/<Team name>/SiteAssets/<OneNote notebook name>"*.

Protección de licencias de la app de colaboración de Microsoft 365

Puede usar el paquete Advanced Email Security, que protege en tiempo real sus buzones de correo de Microsoft 365, Google Workspace u Open-Xchange:

- Antimalware y antispam
- Análisis de URL en correos electrónicos
- Análisis de DMARC
- Antisuplantación
- Protección contra la suplantación de identidad
- Análisis de adjuntos

© Acronis International GmbH, 2003-2025

- Supresión y reconstrucción de contenido
- Gráfico de confianza

También puede habilitar licencias de la app de colaboración de Microsoft 365, que permiten proteger las aplicaciones de colaboración de la nube de Microsoft 365 frente a amenazas de seguridad de contenido. Estas aplicaciones incluyen OneDrive, SharePoint y Teams.

Advanced Email Security puede habilitarse por carga de trabajo o por gigabyte e influirá en su modelo de licencia.

Pasos para llegar a la incorporación de Advanced Email Security desde la consola de Cyber Protect Cloud

1. Haga clic en **Dispositivos** > **Microsoft 365**.
2. Haga clic en el nodo **Usuarios** y luego en el enlace **Ir a seguridad del correo electrónico** en la parte superior derecha.

Obtenga más información acerca de Advanced Email Security en la ficha técnica de Advanced Email Security.

Para obtener indicaciones sobre la configuración, consulte Advanced Email Security con Perception Point.

Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365

Nota
Esta función está disponible en los inquilinos de cliente para los que se selecciona **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** en la **Protección estándar** de un modo de licencia basado en servicios en el portal de administración.

Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365 proporciona copias de seguridad frecuentes, recuperación rápida y planes de copia de seguridad simplificados.

Las copias de seguridad se realizan cada 10 minutos y nunca salen del límite de confianza de datos de Microsoft 365, ya que se mantienen en el almacenamiento de copia de seguridad de Microsoft 365.

Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365 está disponible para los siguientes tipos de datos:

- Buzones de correo de Exchange
  Todas las copias de seguridad están disponibles para la recuperación durante un año.
- Cuentas de OneDrive
  El período de retención es de un año, con dos semanas de copias de seguridad frecuentes. Durante las dos semanas más recientes, todas las copias de seguridad están disponibles para la

© Acronis International GmbH, 2003-2025

recuperación. Desde el día 15 hasta el final del período de un año, una copia de seguridad semanal está disponible para la recuperación.

- Sitios de SharePoint

  El período de retención es de un año, con dos semanas de copias de seguridad frecuentes. Durante las dos semanas más recientes, todas las copias de seguridad están disponibles para la recuperación. Desde el día 15 hasta el final del período de un año, una copia de seguridad semanal está disponible para la recuperación.

Para obtener más información sobre las diferentes soluciones de copia de seguridad para los datos de Microsoft 365, consulte "Comparación de soluciones de copia de seguridad para datos de Microsoft 365" (p. 833).

Creación y aplicación de un nuevo plan de copias de seguridad

Puede crear un plan de copias de seguridad en la pestaña **Dispositivos** o en **Gestión** > **Copia de seguridad de aplicaciones en la nube**.

Nota
Solo puede tener un plan de copias de seguridad por tipo de datos (buzones de correo de Exchange, cuentas de OneDrive o sitios de SharePoint) en un inquilino de cliente.

Pasos para crear y aplicar un plan de copias de seguridad

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Seleccione los elementos de los que desea realizar una copia de seguridad.

   Puede seleccionar buzones de correo de Exchange, OneDrive y sitios de SharePoint.

   - [Para realizar copias de seguridad de los buzones de correo o cuentas de OneDrive de todos los usuarios, incluidos los buzones de correo y cuentas de OneDrive que se crearán en el futuro] Expanda el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.
   - [Para realizar copias de seguridad de buzones de correo individuales o cuentas de OneDrive] Expanda el nodo **Usuarios**, seleccione **Todos los usuarios**, seleccione las cuentas de usuario y haga clic en **Copia de seguridad**.
   - [Para realizar copias de seguridad de todos los sitios de grupo modernos, incluidos los sitios que se crearán en el futuro] Expanda el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Agrupar copia de seguridad**.
   - [Para realizar copias de seguridad de sitios de grupo modernos individuales] Expanda el nodo **Grupos**, seleccione **Todos los grupos**, seleccione sitios y haga clic en **Copia de seguridad**.

© Acronis International GmbH, 2003-2025

- [Para realizar copias de seguridad de todos los sitios de comunicación clásicos, incluidos los sitios que se crearán en el futuro] Expanda el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios** y haga clic en **Agrupar copia de seguridad**.
- [Para realizar copias de seguridad de sitios de comunicación clásicos individuales] Expanda el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios**, seleccione los sitios y haga clic en **Copia de seguridad**.

4. Para crear un plan de copias de seguridad, haga clic en **Crear nuevo**.

Nota
Esta opción está disponible solo si no hay un plan existente para el tipo de datos seleccionado. Si hay un plan existente, solo puede aplicar ese plan. Para obtener más información, consulte "Aplicación de un plan de copia de seguridad" (p. 895).

5. [Si hay más de un tipo de datos disponibles] En el plan de copias de seguridad, haga clic en **Qué incorporar en la copia de seguridad** y después seleccione **Buzones de correo de Microsoft 365** o **OneDrive**.
6. Haga clic en **Aplicar**.

Nota
La aplicación de un plan de copias de seguridad puede tardar hasta 45 minutos, debido al tiempo de procesamiento requerido por parte del almacenamiento de la copia de seguridad de Microsoft 365.

Gestión > Copia de seguridad de aplicaciones en la nube

1. En la consola de Cyber Protect, vaya a **Gestión** > **Copia de seguridad de aplicaciones en la nube**.
2. Haga clic en **Crear plan**.
3. En **Qué incorporar en la copia de seguridad**, seleccione uno de los siguientes tipos de datos:
   - **Buzones de correo de Microsoft 365**
   - **OneDrive**
   - **Sitios de SharePoint**
4. Junto a **Copia de seguridad directa para Microsoft 365**, habilite el interruptor.

Nota
El interruptor está activo solo si no hay un plan de copias de seguridad para el mismo tipo de datos. Si ya hay un plan de copias de seguridad disponible, solo puede aplicar ese plan. Para obtener más información, consulte "Aplicación de un plan de copia de seguridad" (p. 895).

5. En **Dispositivos**, haga clic en **Sin dispositivos** y, a continuación, agregue los recursos informáticos que desee incluir en la copia de seguridad:

© Acronis International GmbH, 2003-2025

a. Haga clic en **Agregar**.

b. Seleccione los recursos informáticos que quiera añadir y, a continuación, haga clic en **Agregar**.

c. Haga clic en **Listo**.

6. Haga clic en **Aplicar**.

Nota
La aplicación de un plan de copias de seguridad puede tardar hasta 45 minutos, debido al tiempo de procesamiento requerido por parte del almacenamiento de la copia de seguridad de Microsoft 365.

Como resultado, se creará el plan de copias de seguridad y se aplicará a los recursos informáticos seleccionados. Las copias de seguridad se ejecutarán automáticamente cada 10 minutos. Con **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**, no puede ejecutar un plan de copias de seguridad manualmente.

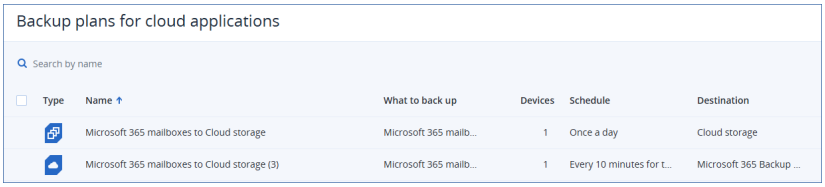
Edición de un plan de copia de seguridad

Puede editar un plan de copias de seguridad para agregar o quitar recursos informáticos o cambiar el nombre del plan.

No puede convertir un plan de copias de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** a un plan para **Microsoft 365 Business (copia de seguridad)**, y viceversa.

Pasos para editar un plan de copias de seguridad para Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365

1. En la consola de Cyber Protect, vaya a **Gestión** > **Copia de seguridad de aplicaciones en la nube**.
2. Seleccione un plan para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** y, a continuación, haga clic en **Editar**.
   Puede distinguir entre los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** y **Microsoft 365 Business (copia de seguridad)** comparando sus iconos y el destino de la copia de seguridad. Los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** solo pueden utilizar el almacenamiento de copia de seguridad de Microsoft 365.



3. [Opcional] Pasos para editar el nombre del plan:

© Acronis International GmbH, 2003-2025

a. Haga clic en el icono del lápiz y, a continuación, edite el nombre.

b. Haga clic en **Aceptar**.

c. Haga clic en **Guardar cambios**.

4. [Opcional] Pasos para añadir recursos informáticos al plan:
   a. Haga clic en **Dispositivos**.
   b. Haga clic en **Agregar**.
   c. Seleccione los recursos informáticos y haga clic en **Agregar**.
   d. Haga clic en **Listo**.
   e. Haga clic en **Guardar cambios**.
5. [Opcional] Pasos para eliminar recursos informáticos del plan:
   a. Haga clic en **Dispositivos**.
   b. Seleccione los recursos informáticos y haga clic en **Eliminar**.
   c. Haga clic en **Listo**.
   d. Haga clic en **Guardar cambios**.

Aplicación de un plan de copia de seguridad

Puede tener un plan de copias de seguridad por tipo de datos (buzones de correo de Exchange, sitios de SharePoint o OneDrive). Si ya se ha creado un plan de copias de seguridad, solo puede aplicar ese plan. No se le permitirá crear un nuevo plan.

Nota
Si revoca y luego vuelve a aplicar un plan de copias de seguridad a una carga de trabajo, las copias de seguridad existentes (puntos de recuperación) quedarán como no disponibles cuando se cree una nueva copia de seguridad.

Puede aplicar un plan de copias de seguridad en la pestaña **Dispositivos** o en la pestaña **Gestión** > **Copia de seguridad de aplicaciones en la nube**.

Pasos para aplicar un plan de copias de seguridad

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Seleccione los elementos a los que desea aplicar un plan de copias de seguridad.
   - [Para seleccionar los buzones de correo o cuentas de OneDrive de todos los usuarios, incluidos los buzones de correo y cuentas de OneDrive que se crearán en el futuro] Expanda el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.

© Acronis International GmbH, 2003-2025

- [Para seleccionar buzones de correo individuales o cuentas de OneDrive] Expanda el nodo **Usuarios**, seleccione **Todos los usuarios**, seleccione las cuentas de usuario y haga clic en **Copia de seguridad**.
- [Para seleccionar todos los sitios de grupo modernos, incluidos los sitios que se crearán en el futuro] Expanda el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Agrupar copia de seguridad**.
- [Para seleccionar sitios de grupo modernos individuales] Expanda el nodo **Grupos**, seleccione **Todos los grupos**, seleccione sitios y, a continuación, haga clic en **Copia de seguridad**.
- [Para seleccionar todos los sitios de comunicación clásicos, incluidos los sitios que se crearán en el futuro] Expanda el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios** y haga clic en **Agrupar copia de seguridad**.
- [Para seleccionar sitios de comunicación clásicos individuales] Expanda el nodo **Recopilaciones de sitios**, seleccione **Todas las recopilaciones de sitios**, seleccione los sitios y haga clic en **Copia de seguridad**.

4. Seleccione un plan de copias de seguridad y haga clic en **Aplicar**.

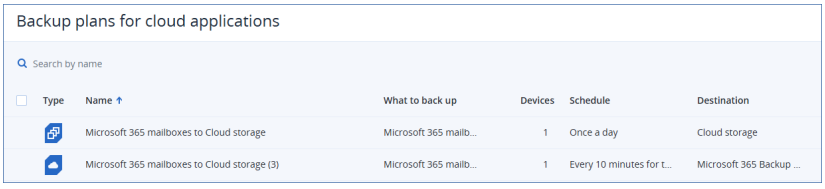
Nota
La aplicación de un plan de copias de seguridad puede tardar hasta 45 minutos, debido al tiempo de procesamiento requerido por parte del almacenamiento de la copia de seguridad de Microsoft 365.

Los planes de copias de seguridad que se muestran dependen del tipo de datos. Por ejemplo, en **Usuarios**, solo están disponibles los planes de copias de seguridad para buzones de correo o cuentas de OneDrive.

Gestión > Copia de seguridad de aplicaciones en la nube

1. En la consola de Cyber Protect, vaya a **Gestión** > **Copia de seguridad de aplicaciones en la nube**.
2. Seleccione un plan de copias de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** y, a continuación, haga clic en **Editar**.

   Puede distinguir entre los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** y **Microsoft 365 Business (copia de seguridad)** comparando sus iconos y el destino de la copia de seguridad. Los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** solo pueden utilizar el almacenamiento de copia de seguridad de Microsoft 365.



3. En el plan de copias de seguridad, haga clic en **Dispositivos**.
4. Haga clic en **Agregar**.

© Acronis International GmbH, 2003-2025

5. Seleccione las cargas de trabajo o los grupos de dispositivos y haga clic en **Agregar**.
6. Haga clic en **Listo**.
7. Haga clic en **Guardar cambios**.

Nota
La aplicación de un plan de copias de seguridad puede tardar hasta 45 minutos, debido al tiempo de procesamiento requerido por parte del almacenamiento de la copia de seguridad de Microsoft 365.

Recuperación de elementos de una copia de seguridad

Puede recuperar buzones de correo de Exchange, cuentas de OneDrive y sitios de SharePoint completos a sus ubicaciones originales. Solo puede recuperar un buzón de correo, una cuenta de OneDrive o un sitio de SharePoint a la vez. Para recuperar varios elementos, repita el procedimiento de recuperación para cada elemento.

Pasos para recuperar elementos de la copia de seguridad de dispositivos

Buzón de correo de Exchange

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Expanda el nodo **Usuarios** y seleccione **Todos los usuarios**.
4. Seleccione una cuenta usuario y haga clic en **Recuperación**.

Nota
Solo puede seleccionar una cuenta a la vez.

5. [Si se realiza la copia de seguridad del buzón de correo y de la cuenta de OneDrive] En **Filtrar por contenido**, seleccione **Buzones de correo de Microsoft 365**.
6. Seleccione una copia de seguridad (punto de recuperación) y haga clic en **Recuperar todo el buzón de correo**.
7. Haga clic en **Iniciar recuperación**.

Como resultado, los elementos que se modifican o eliminan del buzón de correo se reemplazan por los elementos de la copia de seguridad. Los elementos nuevos y los elementos sin cambios no se sobrescriben. No puede cambiar la configuración de sobrescritura porque dependen de la integración de Microsoft. Para obtener más información, consulte Restaurar datos en copia de seguridad de Microsoft 365 en la documentación de Microsoft.

Cuenta de OneDrive

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.

© Acronis International GmbH, 2003-2025

2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Expanda el nodo **Usuarios** y seleccione **Todos los usuarios**.
4. Seleccione una cuenta usuario y haga clic en **Recuperación**.

   Nota
   Solo puede seleccionar una cuenta a la vez.

5. [Si se realiza la copia de seguridad del buzón de correo y de la cuenta de OneDrive] En **Filtrar por contenido**, seleccione **OneDrive**.
6. Seleccione una copia de seguridad (punto de recuperación) y haga clic en **Recuperar todo OneDrive**.
7. Haga clic en **Iniciar recuperación**.

Como resultado, el contenido de OneDrive se sobrescribe completamente con el contenido de la copia de seguridad. Se pierden todos los cambios que no se incluyan en la copia de seguridad. No puede cambiar la configuración de sobrescritura, ya que dependen de la integración de Microsoft. Para obtener más información, consulte Restaurar datos en Microsoft 365 Copia de seguridad en la documentación de Microsoft.

Sitio de SharePoint

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Copia de seguridad directa para Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. [Para recuperar sitios modernos] Expanda el nodo **Grupos** y seleccione **Todos los grupos**.
4. [Para recuperar sitios clásicos] Expanda el nodo **Recopilaciones de sitios** y seleccione **Todas las recopilaciones de sitios**.
5. Seleccione un grupo o una recopilación de sitios y, a continuación, haga clic en **Recuperación**.

   Nota
   Solo puede seleccionar un elemento a la vez.

6. Seleccione una copia de seguridad (punto de recuperación) y, a continuación, haga clic en **Recuperar todo el sitio de SharePoint**.
7. Haga clic en **Iniciar recuperación**.

Como resultado, el sitio de SharePoint se sobrescribe completamente con el contenido de la copia de seguridad. Se pierden todos los cambios que no se incluyen en la copia de seguridad. No puede cambiar la configuración de sobrescritura, ya que dependen de la integración de Microsoft. Para obtener más información, consulte Restaurar datos en copia de seguridad de Microsoft 365 en la documentación de Microsoft.

© Acronis International GmbH, 2003-2025

Pasos para recuperar elementos de la copia de seguridad desde el almacenamiento de copia de seguridad

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad** y, a continuación, seleccione **Almacenamiento de copia de seguridad de Microsoft 365**.
2. Seleccione un archivo de la copia de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione una copia de seguridad (punto de recuperación) y, a continuación, haga clic en **Recuperar todo el sitio de SharePoint**, **Recuperar todo OneDrive** o **Recuperar todo el buzón de correo**.

   El nombre del botón depende del tipo de datos que se están respaldando.
4. Haga clic en **Iniciar recuperación**.

Al recuperar buzones de correo, los elementos que se han cambiado o eliminado se reemplazan por los elementos de la copia de seguridad. Los elementos nuevos y los elementos sin cambios no se sobrescriben. Al recuperar cuentas de OneDrive y sitios de SharePoint, la copia de seguridad sobrescribe completamente los archivos existentes. Se perderán todos los cambios que no se incluyan en la copia de seguridad.

No puede cambiar la configuración de sobrescritura porque dependen de la integración de Microsoft. Para obtener más información, consulte Restaurar datos en copia de seguridad de Microsoft 365 en la documentación de Microsoft.

Revocar un plan de copias de seguridad para Copia de seguridad directa en Microsoft 365

Puede revocar un plan de copias de seguridad en la pestaña **Gestión** > **Copias de seguridad de aplicaciones en la nube** o en la pestaña **Dispositivos**.

Puede revocar un plan de copias de seguridad de una carga de trabajo individual o de un grupo de dispositivos.

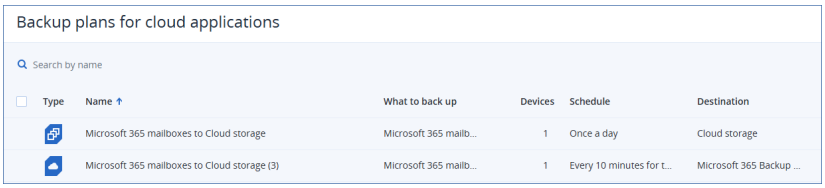
Pasos para revocar un plan de copias de seguridad

Gestión > Copias de seguridad de aplicaciones en la nube

1. En la consola de Cyber Protect, vaya a **Gestión** y luego pulse en **Copias de seguridad de aplicaciones en la nube**.
2. Seleccione un plan de copias de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365** y, a continuación, haga clic en **Editar**.

   Puede distinguir entre los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** y **Microsoft 365 Business (copia de seguridad)** comparando sus iconos y el destino de la copia de seguridad. Los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** solo pueden utilizar el almacenamiento de copia de seguridad de Microsoft 365.

© Acronis International GmbH, 2003-2025



3. En el plan de copias de seguridad, haga clic en **Dispositivos**.
4. Seleccione las cargas de trabajo en las que quiera revocar el plan y luego haga clic en **Eliminar**.
5. Haga clic en **Listo**.
6. Haga clic en **Guardar cambios**.
   Como resultado, el plan de copias de seguridad se revoca de todas las cargas de trabajo que se eliminan.

Nota
La revocación de un plan de copias de seguridad puede tardar unos minutos, debido al tiempo de procesamiento necesario por parte del almacenamiento de copias de Seguridad de Microsoft 365.

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** y pulse en **Copia de seguridad directa para Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. [Para cargas de trabajo individuales] Seleccione una carga de trabajo en la que desee revocar un plan de copias de seguridad y, a continuación, haga clic en **Copia de seguridad**.
4. [Para grupos de dispositivos] Seleccione un grupo en el que desee revocar un plan de copias de seguridad y, a continuación, haga clic en **Agrupar copia de seguridad**.
5. Pulse en el icono de engranaje situado junto al nombre del plan de copias de seguridad y, a continuación, haga clic en **Revocar**.

Nota
La revocación de un plan de copias de seguridad puede tardar unos minutos, debido al tiempo de procesamiento necesario por parte del almacenamiento de copias de seguridad de Microsoft 365.

Eliminación de un plan de copias de seguridad

Puede eliminar un plan de copias de seguridad en la pestaña **Gestión** > **Copias de seguridad de aplicaciones en la nube** o en la pestaña **Dispositivos**.

Nota
En la pestaña **Dispositivos**, no puede eliminar los planes que se aplican a grupos de dispositivos.

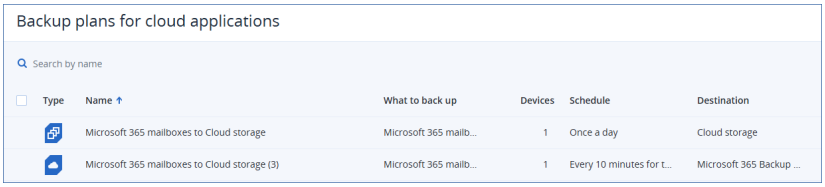
Pasos para borrar un plan de copias de seguridad

© Acronis International GmbH, 2003-2025

Gestión > Copias de seguridad de aplicaciones en la nube

1. En la consola de Cyber Protect, vaya a **Gestión** > **Copias de seguridad de aplicaciones en la nube**.
2. Seleccione un plan de copias de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365**.

   Puede distinguir entre los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** y **Microsoft 365 Business (copia de seguridad)** comparando sus iconos y el destino de la copia de seguridad. Los planes de copia de seguridad para **Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft** solo pueden utilizar el almacenamiento de copia de seguridad de Microsoft 365.



3. Haga clic en **Eliminar**.
4. Seleccione la casilla de verificación para confirmar su decisión y, a continuación, haga clic en **Eliminar**.

Nota
La eliminación de un plan de copias de seguridad puede tardar unos minutos debido al tiempo de procesamiento necesario por parte del almacenamiento de copias de seguridad de Microsoft 365.

Dispositivos

1. En la consola de Cyber Protect, en **Dispositivos**, haga clic en **Copia de seguridad directa para Microsoft 365**.
2. [Si se han añadido varias organizaciones de Microsoft 365] Seleccione una organización de Microsoft 365.
3. Seleccione una carga de trabajo a la que se aplique el plan que desee eliminar y, a continuación, haga clic en **Copia de seguridad**.
4. Haga clic en el icono de engranaje situado junto al nombre del plan de copias de seguridad y, a continuación, pulse en **Eliminar**.
5. Seleccione la casilla de verificación para confirmar su decisión y, a continuación, haga clic en **Eliminar**.

Nota
La eliminación de un plan de copias de seguridad puede tardar unos minutos debido al tiempo de procesamiento necesario por parte del almacenamiento de copias de seguridad de Microsoft 365.

© Acronis International GmbH, 2003-2025

Agente instalado de forma local para Office 365

Cómo añadir una organización de Microsoft 365

Para añadir una organización de Microsoft 365

1. Inicie sesión en la consola de Cyber Protect como administrador de la empresa.
2. Haga clic en el icono de la cuenta que hay en la esquina superior derecha y, a continuación, haga clic en **Descargas** > **Agente para Office 365**.
3. Descargue el agente e instálelo en un equipo que ejecute Windows y esté conectado a Internet.
4. En la consola de Cyber Protect, vaya a **Dispositivos** > **Microsoft Office 365**.
5. En la ventana que se abra, introduzca su ID de la aplicación, el código secreto y la ID de inquilino de Microsoft 365. Consulte "Obtener el ID y el secreto de la aplicación" (p. 902) para obtener más información sobre cómo obtenerlos.
6. Haga clic en **Aceptar**.

Los elementos de datos de su organización aparecerán en la consola de Cyber Protect de la pestaña **Microsoft Office 365**.

Importante
Solo puede haber un Agente para Office 365 instalado localmente en una organización (grupo empresarial).

Obtener el ID y el secreto de la aplicación

Para utilizar la autenticación moderna para Office 365, debe crear una aplicación personalizada en el centro de administración de Entra y otorgarle permisos específicos para la API. Así, obtendrá el **ID de la aplicación**, el **secreto de la aplicación** y el **ID del directorio (inquilino)** que necesita para entrar en la consola de Cyber Protect.

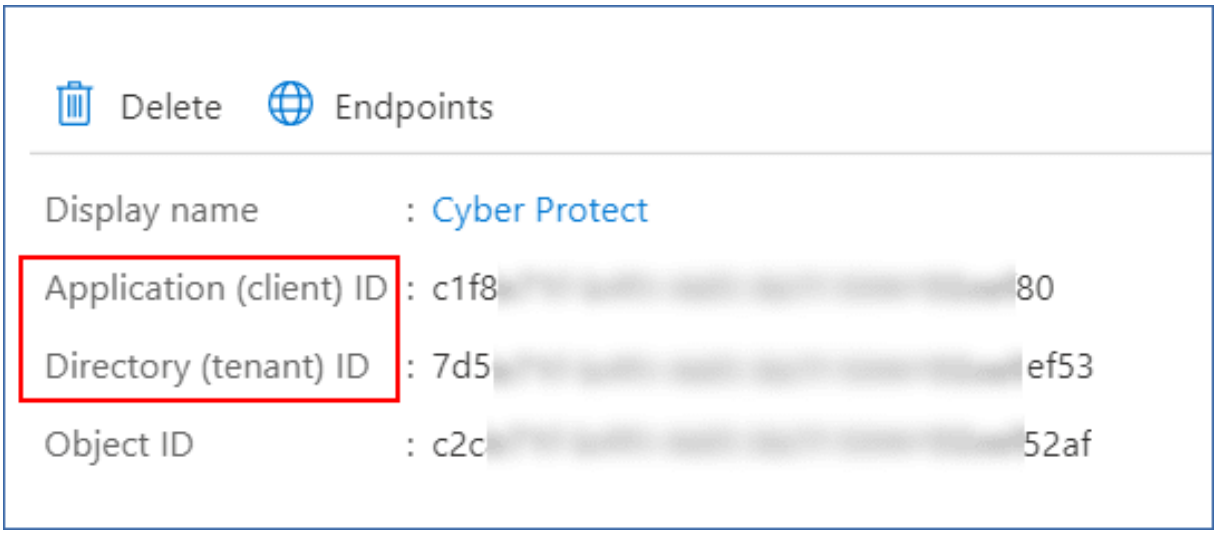
Nota
En el equipo donde está instalado el Agente para Office 365, asegúrese de permitir el acceso a graph.microsoft.com a través del puerto 443.

Para crear una aplicación en el centro de administración de Entra

1. Inicie sesión en el Centro de administración de Entra como administrador.
2. Vaya a **Azure Active Directory** > **Registros de aplicaciones**, y haga clic en **Nuevo registro**.
3. Especifique un nombre para su aplicación personalizada, por ejemplo, Cyber Protection.
4. En **Tipos de cuenta compatibles**, seleccione **Solo cuentas de este directorio organizativo**.
5. Haga clic en **Registrar**.

© Acronis International GmbH, 2003-2025

Su aplicación ya está creada. En el centro de administración de Entra, navegue hasta la página de **Información general** de la aplicación y verifique su ID de aplicación (cliente) y su ID de directorio (inquilino).



Para obtener más información sobre cómo crear una aplicación en el centro de administración de Entra, consulte la Documentación de Microsoft.

Pasos para otorgar los permisos API necesarios a su aplicación

1. En el centro de administración de Entra, navegue hasta los **Permisos de la API** de la aplicación y, a continuación, haga clic en **Añadir un permiso**.
2. Seleccione la pestaña **API que usa mi organización** y luego busque **Office 365 Exchange Online**.
3. Haga clic en **Office 365 Exchange Online** y luego en **Permisos de aplicación**.
4. Seleccione la casilla **full_access_as_app** y haga clic en **Añadir permisos**.
5. En **Permisos API**, haga clic en **Añadir un permiso**.
6. Seleccione **Microsoft Graph**.
7. Seleccione **Permisos de aplicación**.
8. Expanda la pestaña **Directorio**, y seleccione la casilla de verificación **Directory.Read.All**. Haga clic en **Agregar permisos**.
9. Compruebe todos los permisos y haga clic en **Conceder permiso de administrador para <your application's name>**.
10. Haga clic en **Sí** para confirmar su elección.

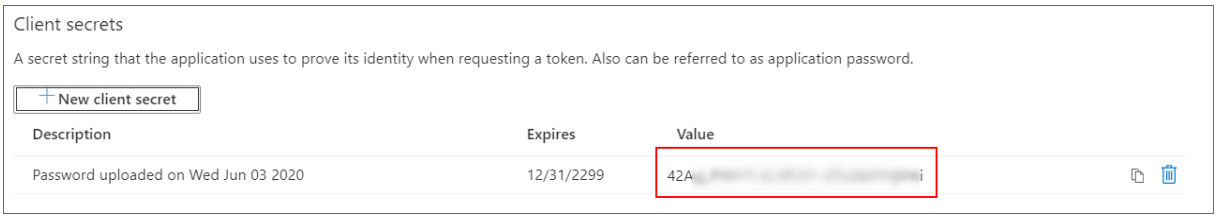
Pasos para crear un secreto de la aplicación

1. En el centro de administración de Entra, acceda a los **Certificados y secretos** > **Nuevo secreto de cliente** de su aplicación.
2. En el cuadro de diálogo que se abra, seleccione Caduca: **Nunca**, y, a continuación, haga clic en

© Acronis International GmbH, 2003-2025

Agregar.

3. Compruebe el secreto de su aplicación en el campo **Valor** y asegúrese de recordarlo.



Para obtener más información sobre el secreto de la aplicación, consulte la documentación de Microsoft.

Cambio de las credenciales de acceso de Microsoft 365

Puede cambiar las credenciales de acceso de Microsoft 365 sin tener que volver a instalar el agente.

Pasos para cambiar las credenciales de acceso de Microsoft 365

1. Haga clic en **Dispositivos** > **Microsoft Office 365**.
2. Seleccione la organización de Microsoft 365.
3. Haga clic en **Especificar credenciales**.
4. Introduzca su ID de la aplicación, el código secreto y la ID de inquilino de Microsoft 365. Consulte "Obtener el ID y el secreto de la aplicación" (p. 902) para obtener más información sobre cómo obtenerlos.
5. Haga clic en **Aceptar**.

Protección de los buzones de correo de Exchange Online

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de los buzones de correo de usuario y compartidos. No se puede realizar una copia de seguridad de los buzones de correo de archivos comprimidos (**Archivo comprimido local**) ni de los de grupos.

¿Qué elementos de datos pueden recuperarse?

Los siguientes elementos pueden recuperarse de la copia de seguridad de buzones de correo:

- Buzones de correo
- Carpetas de correo electrónico
- Mensajes de correo electrónico
- Eventos del calendario
- Tareas
- Contactos

© Acronis International GmbH, 2003-2025

- Entradas del diario
- Notas

Puede usar la búsqueda para localizar los elementos.

Cuando se recupera un buzón de correo sobre un buzón de correo existente, los elementos anteriores que tengan los mismos ID se sobrescriben.

Al recuperar elementos de buzón de correo no se sobrescribe nada. En su lugar, en la carpeta de destino se reproduce la ruta completa al elemento del buzón de correo.

Seleccionar buzones de correo de Microsoft 365

Seleccione los buzones de correo tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar buzones de correo

1. Haga clic en **Microsoft Office 365**.
2. Seleccione los buzones de correo de los que desea realizar una copia de seguridad.
3. Haga clic en **Copia de seguridad**.

Recuperación de buzones de correo y elementos de los buzones

Recuperación de buzones de correo

1. Haga clic en **Microsoft Office 365**.
2. Seleccione el buzón de correo que desea recuperar y, a continuación, haga clic en **Recuperación**.
   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.
   Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Buzón de correo**.
5. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.
   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe, debe indicar el buzón de correo de destino.
6. Haga clic en **Iniciar recuperación**.

© Acronis International GmbH, 2003-2025

Recuperación de elementos de buzón de correo

1. Haga clic en **Microsoft Office 365**.
2. Seleccione el buzón de correo que contenía originalmente los elementos que desea recuperar y, a continuación, haga clic en **Recuperación**.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.

   Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
5. Seleccione los elementos que desea recuperar.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario, nombre del adjunto y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Mostrar contenido** para ver el contenido, incluidos los documentos adjuntos.

   Nota
   Haga clic en el nombre de un archivo adjunto para descargarlo.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Enviar como correo electrónico** para enviar el mensaje a una dirección de correo electrónico. El mensaje se envía desde el correo electrónico de su cuenta de administrador.

   Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 
6. Haga clic en **Recuperar**.
7. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.

   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe, debe indicar el buzón de correo de destino.
8. Haga clic en **Iniciar recuperación**.
9. Confirme su decisión.

Los elementos de buzón de correo siempre se recuperan en la carpeta **Elementos recuperados** del buzón de correo de destino.

© Acronis International GmbH, 2003-2025

Protección de los datos de Google Workspace

Nota
Esta función no está disponible para inquilinos en modo de cumplimiento. Para obtener más información, consulte "Modo de cumplimiento" (p. 1568).

¿Qué implica la protección de Google Workspace?

- Copias de seguridad de cloud a cloud y recuperación de los datos de usuario de Google Workspace (buzones de correo de Gmail, Calendar, Contactos, cuentas de Google Drive) y unidades compartidas de Google Workspace.
- La recuperación granular de correos electrónicos, archivos, contactos y otros elementos.
- Compatibilidad con varias organizaciones de Google Workspace y recuperación entre organizaciones.
- Notarización opcional en los archivos incluidos en la copia de seguridad dentro de la base de datos de cadena de bloques de Ethereum. Cuando está habilitada, sirve para demostrar que un archivo es auténtico y que no ha cambiado desde su copia de seguridad.
- Búsqueda en todo el texto opcional. Cuando está habilitada, puede buscar correos electrónicos por su contenido.
- Se pueden proteger hasta 5000 elementos (buzones de correo, cuentas de Google Drive y unidades compartidas) por empresa sin que ello implique una degradación del rendimiento.
- Los datos de la copia de seguridad se comprimen automáticamente y utilizan menos espacio en la ubicación de la copia de seguridad que en su ubicación original. La tasa de compresión para las copias de seguridad de la nube a la nube es fija y corresponde al nivel **Normal** de las copias de seguridad que no son de la nube a la nube. Para obtener más información sobre estos niveles, consulte "Tasa de compresión" (p. 605).

Derechos de usuario necesarios

En Cyber Protection

En Cyber Protection, usted debe ser un administrador de la empresa que actúe a nivel de inquilino del cliente. Los administradores de la empresa que actúen a nivel de la unidad, los administradores de la unidad y los usuarios no pueden realizar copias de seguridad ni recuperar datos de Google Workspace.

En Google Workspace

Para añadir su organización de Google Workspace al servicio Cyber Protection, debe haber iniciado sesión como superadministrador con acceso a la API habilitado (en la consola de administración de Google, **Seguridad** > **Referencia de API** > **Habilitar acceso a API**).

© Acronis International GmbH, 2003-2025

La contraseña del superadministrador no se almacena en ningún lugar y no se usa para llevar a cabo la copia de seguridad y la recuperación. Cambiar esta contraseña en Google Workspace no afecta a la operación del servicio Cyber Protection.

Si el superadministrador que añadió la organización de Google Workspace se elimina de Google Workspace o se le asigna un rol con menos privilegios, se producirá un error en las copias de seguridad del tipo "Acceso denegado". En este caso, repita el procedimiento descrito en "Incorporación de una organización de Google Workspace" (p. 909) y especifique las credenciales válidas de superadministrador. Para evitar este caso, le recomendamos que cree un usuario superadministrador dedicado a fines de copias de seguridad y recuperación.

Para descubrir y realizar copias de seguridad de las unidades compartidas, el usuario de superadministrador debe tener asignada al menos una licencia "Google Workspace Business Standard".

Acerca de la planificación de copia de seguridad

Dado que el agente en la nube sirve a varios clientes, determina la hora de inicio para cada plan de protección por su cuenta con el fin de garantizar una carga uniforme durante un día y un servicio de la misma calidad para todos los clientes.

Cada plan de protección se ejecuta todos los días a la misma hora.

Con las funciones estándar incluidas, la opción predeterminada es **Una vez por día**. Con el paquete de Advanced Backup, la opción predeterminada es **Dos veces por día**. Puede planificar hasta seis copias de seguridad por día. Las copias de seguridad se inician a intervalos aproximados en función de la carga actual del agente de la nube, que gestiona varios clientes en un centro de datos. De este modo, se garantiza una carga equilibrada durante el día y la misma calidad de servicio para todos los clientes.

Limitaciones

- La consola de Cyber Protect muestra solo usuarios que tienen asignada una licencia de Google Workspace y un buzón de correo o Google Drive.
- Los usuarios de Google Workspace archivados o suspendidos se muestran como inactivos (en gris) en la consola de Cyber Protect después de la operación de búsqueda que sigue al cambio de su estado. No puede aplicar nuevos planes de copia de seguridad a usuarios inactivos. Los planes de copia de seguridad existentes siguen activos durante 72 horas.

  Después de la operación de detección que sigue al período de 72 horas, los usuarios archivados o suspendidos se eliminan de la consola de Cyber Protect y sus datos ya no se incluyen en las copias de seguridad, pero las copias de seguridad existentes siguen estando disponibles.
- Las copias de seguridad de las cuentas de usuario de Google Workspace eliminadas no se borran automáticamente del almacenamiento en la nube. Estas copias de seguridad se facturan por el espacio de almacenamiento que usan.
- La copia de seguridad de los documentos con formatos nativos de Google se realiza como documentos de oficina genéricos y se muestra con una extensión diferente en la consola de

© Acronis International GmbH, 2003-2025

Cyber Protect, como .docx o .pptx, por ejemplo. Los documentos se convierten de nuevo a su formato original durante la recuperación.

- Puede ejecutar manualmente hasta 10 copias de seguridad por hora. Para obtener más información, consulte "Ejecución de copias de seguridad de nube a nube de forma manual" (p. 278).
- Puede ejecutar hasta 10 operaciones de recuperación de la nube a la nube simultáneamente. Esta cantidad incluye las operaciones de recuperación de Microsoft 365 y Google Workspace.
- No puede recuperar elementos de diferentes puntos de recuperación de forma simultánea, incluso aunque pueda seleccionar esos elementos en los resultados de búsqueda.
- Solo puede aplicar un plan de copias de seguridad individual a un recurso informático.
- Cuando se aplican un plan de copias de seguridad individual y un plan de copias de seguridad en grupo al mismo recurso informático, la configuración del plan individual tiene prioridad.

Importante
Las acciones con recursos de la nube a la nube como ver el contenido de los correos electrónicos con copia de seguridad, descargar adjuntos o archivos, recuperar correos electrónicos de buzones de correo no originales o enviarlos como correos electrónicos podrían infringir la privacidad del usuario. Estas acciones se registran en **Supervisión** > **Registro de auditoría** en el portal de administración.

Incorporación de una organización de Google Workspace

Para añadir una organización de Google Workspace al servicio de Cyber Protection, necesita un proyecto personal especializado de Google Cloud. Para obtener más información sobre cómo crear y configurar dicho proyecto, consulte "Cree un proyecto personal de Google Cloud" (p. 910).

Para añadir una organización de Google Workspace mediante un proyecto personal especializado de Google Cloud

1. Inicie sesión en la consola de Cyber Protect como administrador de la empresa.
2. Haga clic en **Dispositivos** > **Agregar** > **Google Workspace**.
3. Especifique la dirección de correo electrónico de un superadministrador de su cuenta de Google Workspace.
   Para este procedimiento, es irrelevante si la verificación en dos pasos está habilitada para la cuenta del correo electrónico de superadministrador.
4. Busque el archivo JSON que contiene la clave privada de la cuenta del servicio que ha creado en su proyecto de Google Cloud.
   También puede pegar el contenido del archivo como texto.
5. Haga clic en **Confirmar**.

Como resultado, su organización de Google Workspace aparecerá en la pestaña **Dispositivos** de la consola de Cyber Protect.

© Acronis International GmbH, 2003-2025

Consejos útiles

- Después de añadir una organización de Google Workspace, se realizará una copia de seguridad de los datos del usuario y las unidades compartidas tanto en el dominio principal como en todos los secundarios, si hay alguno. Los recursos de los que se ha realizado la copia de seguridad se mostrarán en una lista y no se agruparán por dominio.
- El agente de la nube se sincroniza con Google Workspace cada 24 horas desde el momento en que la organización se añade al servicio de Cyber Protection. Si añade o elimina un usuario o una unidad compartida, no verá este cambio en la consola de Cyber Protect inmediatamente. Para sincronizar el cambio de manera inmediata, seleccione la organización en la página de **Google Workspace** y, a continuación, haga clic en **Actualizar**.

  Para obtener más información sobre la sincronización de los recursos de una organización de Google Workspace y la consola de Cyber Protect, consulte "Detección de los recursos de Google Workspace" (p. 914).
- Si aplicó un plan de protección a los grupos **Todos los usuarios** o **Todas las unidades compartidas**, los elementos añadidos recientemente se incluirán en la copia de seguridad después de la sincronización.
- Según la directiva de Google, cuando se elimina un usuario o una unidad compartida de la interfaz gráfica de usuario de Google Workspace, sigue estando disponible durante varios días a través de la API. Durante ese periodo, el elemento eliminado está inactivo (en gris) en la consola de Cyber Protect y no se realiza ninguna copia de seguridad de este. Cuando el elemento eliminado deja de estar disponible a través de la API, desaparece de la consola de Cyber Protect. Sus copias de seguridad (si existen) se pueden encontrar en **Almacenamiento de la copia de seguridad** > **Copias de seguridad de aplicaciones en la nube**.

Cree un proyecto personal de Google Cloud

Para añadir su organización de Google Workspace al servicio Cyber Protection mediante un proyecto especializado de Google Cloud, haga lo siguiente:

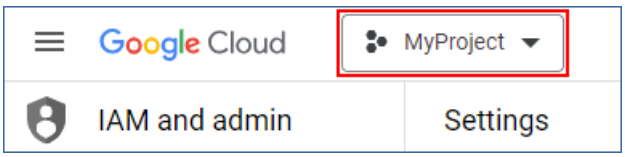
1. Cree un nuevo proyecto de Google Cloud.
2. Habilite las API necesarias para el proyecto.
3. Configure las credenciales del proyecto:
   a. Configure la pantalla de consentimiento de OAuth.
   b. Cree y configure la cuenta del servicio Cyber Protection.
4. Otorgue acceso al nuevo proyecto a su cuenta de Google Workspace.

Nota
Este tema contiene una descripción de interfaz de usuario de terceros que puede estar sujeta a cambios sin previo aviso.

Para crear un nuevo proyecto de Google Cloud

© Acronis International GmbH, 2003-2025

1. Inicie sesión en Google Cloud Platform (console.cloud.google.com) como superadministrador.
2. En la consola de Google Cloud Platform, haga clic en el selector de proyectos en la esquina superior izquierda.



3. En la pantalla que se abra, seleccione una organización y haga clic en **Nuevo proyecto**.



4. Especifique un nombre para su nuevo proyecto.
5. Haga clic en **Crear**.

Se creará su nuevo proyecto de Google Cloud.

Para habilitar las API necesarias para el proyecto

1. En la consola de Google Cloud Platform, seleccione su nuevo proyecto.
2. En el menú de navegación, seleccione **API y servicios** > **API y servicios habilitados**.
3. Deshabilite todas las API habilitadas de manera predeterminada en el proyecto, una por una:
   a. Desplácese hacia abajo en la página **API y servicios habilitados** y, a continuación, haga clic en el nombre de una API habilitada.
   Se abrirá la página **Detalles de la API o del servicio** de la API seleccionada.
   b. Haga clic en **Deshabilitar API** y haga clic en **Deshabilitar** para confirmar su elección.
   c. [Si se le solicita] Haga clic en **Confirmar** para confirmar su elección.
   d. Vuelva a **API y servicios** > **API y servicios habilitados** y deshabilite la siguiente API.
4. En el menú de navegación, seleccione **API y servicios** > **Biblioteca**.
5. En la biblioteca de API, habilite estas API una por una:
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

   Utilice la barra de búsqueda para encontrar las API solicitadas. Para habilitar una API, haga clic en su nombre y, a continuación, en **Habilitar**. Para buscar la siguiente API, vuelva a la biblioteca de API seleccionando **API y servicios** > **Biblioteca** en el menú de navegación.

Para configurar la pantalla de consentimiento de OAuth

1. En el menú de navegación de Google Cloud Platform, seleccione **API y servicios** > **Pantalla de consentimiento de OAuth**.

© Acronis International GmbH, 2003-2025

2. En la ventana que se abre, seleccione el tipo de usuario **Interno** y, a continuación, haga clic en **Crear**.
3. En el campo **Nombre de aplicación**, especifique un nombre para su aplicación.
4. En el campo **Correo electrónico de soporte del usuario**, introduzca el correo electrónico del superadministrador.
5. En el campo **Información de contacto del desarrollador**, introduzca el correo electrónico del superadministrador.
6. Deje el resto de los campos en blanco y haga clic en **Guardar y continuar**.
7. En la página **Ámbitos**, haga clic en **Guardar y continuar** sin cambiar nada.
8. En la página **Resumen**, verifique la configuración y, a continuación, haga clic en **Volver al panel de control**.

Para crear y configurar la cuenta del servicio Cyber Protection

1. En el menú navegación de Google Cloud Platform, seleccione **IAM y Admin** > **Cuentas del servicio**.
2. Haga clic en **Crear cuenta del servicio**.
3. Especifique un nombre para la cuenta del servicio.
4. [Opcional] Especifique una descripción para la cuenta del servicio.
5. Haga clic en **Crear y continuar**.
6. No cambie nada en los pasos **Conceder acceso al proyecto a esta cuenta del servicio** y **Conceder acceso a esta cuenta del servicio a los usuarios**.
7. Haga clic en **Listo**.
   Se abrirá la página **Cuentas del servicio**.
8. En la página **Cuentas del servicio**, seleccione la nueva cuenta del servicio y, en **Acciones**, haga clic en **Gestionar claves**.
9. En **Claves**, haga clic en **Añadir clave** > **Crear nueva clave** y seleccione el tipo de clave **JSON**.
10. Haga clic en **Crear**.
    Se descargará automáticamente un archivo JSON con la clave privada de la cuenta del servicio en su equipo. Almacene el archivo de forma segura, ya que lo necesitará para añadir su organización de Google Workspace al servicio Cyber Protection.

Para otorgar acceso al nuevo proyecto a su cuenta de Google Workspace

1. En el menú de navegación de Google Cloud Platform, seleccione **IAM y Admin** > **Cuentas del servicio**.
2. En la lista, busque la cuenta del servicio que creó y copie el ID de cliente que se muestra en la columna **ID del cliente de OAuth 2.0**.
3. Inicie sesión en la consola de administración de Google (admin.google.com) como superadministrador.
4. En el menú de navegación, seleccione **Seguridad** > **Control de acceso y datos** > **Controles de API**.

© Acronis International GmbH, 2003-2025

5. Desplace hacia abajo la página **Controles de API** y, en **Delegación en todo el dominio**, haga clic en **Gestionar la delegación en todo el dominio**.
   Se abrirá la página **Delegación en todo el dominio**.
6. En la página **Delegación en todo el dominio**, haga clic en **Añadir nuevo**.
   Se abrirá la ventana **Añadir un ID del cliente nuevo**.
7. En el campo **ID del cliente**, escriba el ID del cliente de su cuenta del servicio.
8. En el campo **Ámbitos de OAuth**, copie y pegue la siguiente lista de ámbitos separados por comas:

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   También puede añadir los ámbitos uno a uno:
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. Haga clic en **Autorizar**.

Como resultado, su nuevo proyecto de Google Cloud podrá acceder a los datos de su cuenta de Google Workspace. Para realizar una copia de seguridad de los datos, deberá enlazar el proyecto con el servicio Cyber Protection. Para obtener más información sobre cómo hacerlo, consulte "Para añadir una organización de Google Workspace mediante un proyecto personal especializado de Google Cloud" (p. 909).

Si necesita revocar el acceso de su proyecto de Google Cloud a su cuenta de Google Workspace y, respectivamente, el acceso del servicio Cyber Protection, elimine el cliente API que use su proyecto.

Para revocar el acceso a su cuenta de Google Workspace

1. Inicie sesión en la consola de administración de Google (admin.google.com) como superadministrador.
2. En el menú de navegación, seleccione **Seguridad** > **Control de acceso y datos** > **Controles de API**.
3. Desplace hacia abajo la página **Controles de API** y, en **Delegación en todo el dominio**, haga clic en **Gestionar la delegación en todo el dominio**.
   Se abrirá la página **Delegación en todo el dominio**.

© Acronis International GmbH, 2003-2025

4. En la página **Delegación en todo el dominio**, seleccione el cliente de la API que utilice su producto y, a continuación, haga clic en **Eliminar**.
   Como resultado, su proyecto de Google Cloud y el servicio de Cyber Protection no podrán acceder a su cuenta de Google Workspace ni hacer una copia de seguridad de sus datos.

Detección de los recursos de Google Workspace

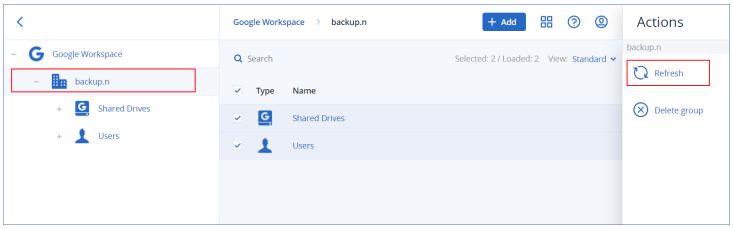
Cuando añade una organización de Google Workspace al servicio de Cyber Protection, los recursos de esta organización, como los buzones de correo y Google Drive, se sincronizan con la consola de Cyber Protect. Esta operación se llama detección y se registra en **Supervisión** > **Actividades**.

Cuando se complete la operación de detección, verá los recursos de la organización de Google Workspace en la pestaña **Dispositivos** > **Google Workspace** de la consola de Cyber Protect y podrá aplicarles planes de copias de seguridad.

Una operación de detección automática se ejecuta una vez al día para mantener actualizada la lista de recursos de la consola de Cyber Protect. También puede sincronizar la lista bajo demanda si vuelve a ejecutar una operación de detección manualmente.

Para volver a ejecutar una operación de detección manualmente

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Google Workspace**.
2. Seleccione su organización de Google Workspace y, a continuación, en el panel **Acciones**, haga clic en **Actualizar**.



Nota
Puede ejecutar manualmente una operación de detección hasta 10 veces por hora. Cuando se alcance este número, las ejecuciones permitidas se restablecen durante una hora, y después una ejecución adicional pasa a estar disponible por cada hora, hasta que se alcanza de nuevo un total de 10 ejecuciones por hora.

Configuración de la frecuencia de las copias de seguridad de Google Workspace

Por defecto, las copias de seguridad de Google Workspace se ejecutan una vez al día y no hay otras opciones de programación disponibles.

Si el paquete Advanced Backup está habilitado en su inquilino, la opción **Dos veces al día** está habilitada de forma predeterminada y hay más frecuencias disponibles entre las que seleccionar.

© Acronis International GmbH, 2003-2025

Puede seleccionar el número de copias de seguridad por día, pero no puede configurar la hora de inicio de la copia de seguridad. Las copias de seguridad se inician automáticamente a intervalos aproximados en función de la carga actual del agente de la nube, que gestiona varios clientes en un centro de datos. De este modo, se garantiza una carga equilibrada durante el día y la misma calidad de servicio para todos los clientes.

Las siguientes opciones están disponibles.

Opciones de planificación	Intervalo aproximado entre cada copia de seguridad
Una vez al día*	24 horas
Dos veces al día (predeterminado)**	12 horas
Tres veces al día**	8 horas
Seis veces al día**	4 horas

* Aunque la opción **Dos veces al día** es la predeterminada cuando Advanced Backup está habilitado, la opción **Una vez al día** podría habilitarse de forma temporal en algunos centros de datos, según la disponibilidad de almacenamiento.

** Se requiere el paquete Advanced Backup

Nota
Según la carga del agente de la nube y la posible limitación de Google Workspace, puede que las copias de seguridad se inicien más tarde de lo previsto o tarden más en completarse. Si una copia de seguridad tarda más que el intervalo medio entre dos copias de seguridad, se reprogramará la siguiente y, por tanto, podría haber menos copias de seguridad por día de las que se habían seleccionado. Por ejemplo, es posible que solo se puedan completar dos copias de seguridad, aunque haya seleccionado seis por día.

Protección de los datos de Gmail

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de los buzones de correo de los usuarios de Gmail. En la copia de seguridad de un buzón de correo también se incluyen los datos de Calendar y de los Contactos. También puede llevar a cabo copias de seguridad de calendarios compartidos.

Los siguientes elementos *no se incluyen* al realizar una copia de seguridad:

- Los calendarios de **cumpleaños**, **recordatorios** y **tareas**.
- Las carpetas adjuntas a los eventos de los calendarios.
- La carpeta **Directorio** en Contactos.

© Acronis International GmbH, 2003-2025

Los siguientes elementos de Calendar se *omiten* debido a las limitaciones de la API de Google Calendar:

- Elementos de las citas
- El campo de conferencias de un evento.
- La configuración del calendario sobre las **notificaciones de evento que duran todo el día**.
- La configuración del calendario sobre las **invitaciones que se aceptan automáticamente** (en calendarios para salas o espacios compartidos).

Los siguientes elementos de los Contactos se *omiten* debido a las limitaciones de la API de Google People:

- La carpeta **Otros contactos**.
- Los perfiles externos de un contacto (**perfil de Directory**, **perfil de Google**).
- El campo de contacto **Archivo como**.

¿Qué elementos de datos pueden recuperarse?

Los siguientes elementos pueden recuperarse de la copia de seguridad de buzones de correo:

- Buzones de correo
- Carpetas de correo electrónico (según la terminología de Google, "etiquetas". Las **etiquetas** aparecen en al software de copia de seguridad como carpetas, para que sean coherentes con la presentación de otros datos).
- Mensajes de correo electrónico
- Eventos del calendario
- Contactos

Puede usar la búsqueda para localizar elementos en una copia de seguridad.

Al recuperar elementos de buzones de correo y buzones de correo, puede seleccionar si quiere sobrescribir los elementos en la ubicación de destino.

Limitaciones

- Las fotos de los contactos no se pueden recuperar
- El elemento de Calendar **Fuera de la oficina** se recupera como un evento del calendario habitual, debido a las limitaciones de la API de Google Calendar.

Seleccionar buzones de correo de Gmail

Seleccione los buzones de correo tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar buzones de correo de Gmail

© Acronis International GmbH, 2003-2025

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos de los usuarios quiera recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para realizar una copia de seguridad de los buzones de correo de todos los usuarios (incluidos los buzones de correo que se crearan en el futuro), amplíe el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de los buzones de correo de usuarios individuales, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los usuarios cuyos buzones de correo quiera recuperar y haga clic en **Copia de seguridad**.
4. En el plan de copias de seguridad, configure lo siguiente:
   - [Si está disponible] En **Qué incorporar en la copia de seguridad**, seleccione **Gmail**.
   - [Opcional] Si quiere realizar una copia de seguridad de los calendarios que se comparten con los usuarios seleccionados, habilite el conmutador **Incluir calendarios compartidos**.
   - En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.
   - En **Cifrado**, haga clic en **Especificar contraseña**.
     - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
     - Haga clic en **Aceptar**.

Recuperación de buzones de correo y elementos de los buzones

Recuperación de buzones de correo

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia quiere recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario cuyo buzón de correo quiera recuperar y haga clic en **Recuperación**.

   Si se ha eliminado el usuario, seleccione el usuario de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

Nota
Para ver únicamente los puntos de recuperación que incluyan buzones de correo, seleccione **Gmail** en **Filtrar por contenido**.

© Acronis International GmbH, 2003-2025

5. Haga clic en **Recuperar** > **Todo el buzón de correo**.
6. Si se han añadido varias organizaciones de Google Workspace al servicio Cyber Protection, haga clic en **la organización de Google Workspace** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe seleccionar una nueva organización de destino de entre las que se encuentran registradas y disponibles.
7. En **Recuperar al buzón de correo**, puede consultar, cambiar o especificar el buzón de correo de destino.

   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona una organización que no es la original, debe indicar el buzón de correo de destino.

   No puede crear un nuevo buzón de correo de destino durante la recuperación. Para recuperar un buzón de correo en uno nuevo, primero debe crear el buzón de correo de destino en la organización de Google Workspace que desee y, a continuación, dejar que el agente en la nube sincronice el cambio. El agente en la nube se sincroniza automáticamente con Google Workspace cada 24 horas. Para sincronizar el cambio de manera inmediata, en la consola de Cyber Protect, seleccione la organización en la página de **Google Workspace** y, a continuación, haga clic en **Actualizar**.
8. Haga clic en **Iniciar recuperación**.
9. Seleccione una de las opciones de sobreescritura:
   - **Sobrescribir elementos existentes**
   - **No sobrescribir elementos existentes**
10. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de elementos de buzón de correo

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia quiere recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario en cuyo buzón de correo se encontraban al principio los elementos que quiera recuperar y haga clic en **Recuperación**.

   Si se ha eliminado el usuario, seleccione el usuario de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios y grupos por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

© Acronis International GmbH, 2003-2025

Nota
Para ver únicamente los puntos de recuperación que incluyan buzones de correo, seleccione **Gmail** en **Filtrar por contenido**.

5. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
6. Busque la carpeta requerida. Si la copia de seguridad no está cifrada, puede usar la búsqueda para obtener la lista de elementos necesarios.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, fecha, nombre del archivo adjunto y contenido del mensaje.

     Al buscar por fecha, puede seleccionar una fecha de inicio o de fin, o ambas fechas, para buscar dentro de un intervalo de tiempo.

     La búsqueda por el nombre de los archivos adjuntos o en el contenido del mensaje solo arroja resultados si se ha activado la opción **Búsqueda en todo el texto** durante la copia de seguridad. Puede especificar el idioma del fragmento de mensaje que se buscará como parámetro adicional.
   - Para los eventos: búsqueda por título y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.
7. Seleccione los elementos que desea recuperar. Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 

   También puede optar por una de las siguientes opciones:

   - Cuando un elemento está seleccionado, haga clic en **Mostrar contenido** para ver lo que se incluye, incluidos los adjuntos. Haga clic en el nombre de un archivo adjunto para descargarlo.
   - Únicamente si la copia de seguridad no está cifrada, ha usado la búsqueda y ha seleccionado un único elemento de la lista de resultados de búsqueda: haga clic en **Mostrar versiones** para seleccionar la versión del elemento que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.
8. Haga clic en **Recuperar**.
9. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, haga clic en **Organización de Google Workspace** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe seleccionar una nueva organización de destino de entre las que se encuentran registradas y disponibles.
10. En **Recuperar al buzón de correo**, puede consultar, cambiar o especificar el buzón de correo de destino.

© Acronis International GmbH, 2003-2025

De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona una organización que no es la original, debe indicar el buzón de correo de destino.

11. En **Ruta** puede consultar o cambiar la carpeta de destino en el buzón de correo de destino. De manera predeterminada se selecciona la carpeta original.
12. Haga clic en **Iniciar recuperación**.
13. Seleccione una de las opciones de sobreescritura:
    - **Sobrescribir elementos existentes**
    - **No sobrescribir elementos existentes**
14. Haga clic en **Continuar** para confirmar su decisión.

Protección de archivos de Google Drive

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de un Google Drive completo, o bien de archivos o carpetas individuales. Los archivos se incluyen en la copia de seguridad junto con sus permisos para compartir.

Importante
Los siguientes elementos no se incluyen en las copias de seguridad:

- Carpeta **Compartido conmigo**
- Carpeta **Equipos** (creada por el cliente de realización de copias de seguridad y sincronización)

Limitaciones

De los formatos de archivo específicos de Google, los de Documentos de Google, Hojas de cálculo de Google y Presentaciones de Google son totalmente compatibles para la copia de seguridad y recuperación. Es posible que otros formatos específicos de Google no sean totalmente compatibles o no lo sean en absoluto. Por ejemplo, los archivos de Dibujos de Google se recuperan como archivos `.svg`, los de Sitios de Google como archivos `.txt`, los de Google Jamboard como archivos `.pdf` y los de Google My Maps se omiten durante una copia de seguridad.

Nota
Los formatos de archivos que no son específicos de Google, por ejemplo, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png` o `.zip`, son totalmente compatibles para la copia de seguridad y recuperación.

¿Qué elementos de datos pueden recuperarse?

Puede recuperar un Google Drive completo, o bien cualquier archivo o carpeta incluida en una copia de seguridad.

© Acronis International GmbH, 2003-2025

Puede elegir entre recuperar los permisos para compartir o permitir que los archivos hereden los permisos de la carpeta desde donde se recuperan.

Limitaciones

- Los comentarios de los archivos no se pueden recuperar.
- Los enlaces para compartir para los archivos y las carpetas no se recuperan.
- Las **opciones de configuración del propietario** de solo lectura para archivos compartidos (**Evitar que los editores cambien el acceso y añadan nuevos usuarios** and **No permitir descargar, imprimir ni copiar elementos a lectores ni a personas que añaden comentarios**) no se puede cambiar durante una recuperación.
- La propiedad de una carpeta compartida no se puede cambiar durante una recuperación si la opción **Evitar que los editores cambien el acceso y añadan nuevos usuarios** está habilitada para ella. Esta configuración evita que la API de Google Drive enumere los permisos de las carpetas. La propiedad de los archivos de la carpeta se recupera correctamente.

Selección de archivos de Google Drive

Seleccione los archivos tal como se describe a continuación y, luego, especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar archivos de Google Drive

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos de los usuarios quiera recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para realizar una copia de seguridad de los archivos de todos los usuarios (incluidos los que se crearan en el futuro), amplíe el nodo **Usuarios**, seleccione **Todos los usuarios** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de los archivos de usuarios individuales, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los usuarios cuyos archivos quiera recuperar y haga clic en **Copia de seguridad**.
4. En el plan de copias de seguridad, configure lo siguiente:
   - [Si está disponible] En **Qué incorporar en la copia de seguridad**, seleccione **Google Drive**.
   - En **Elementos que se incluirán en la copia de seguridad**, realice uno de los siguientes procedimientos:
     - Mantenga los ajustes predeterminados **[Todos]** (todos los archivos).
     - Especifique los archivos y las carpetas que quiere incluir en la copia de seguridad. Para ello, añada sus nombres o rutas.

© Acronis International GmbH, 2003-2025

Puede usar los caracteres comodín (*, ** y ?). Para obtener más información sobre la especificación de rutas y el uso de los caracteres comodín, consulte "Filtros de archivo (inclusiones y exclusiones)" (p. 607).

- Examine los archivos y las carpetas para especificar cuáles quiere incluir en la copia de seguridad.

  El enlace **Examinar** está disponible únicamente cuando se crea un plan de protección para un solo usuario.

- [Opcional] Para especificar los archivos y carpetas que se omitirán durante la copia de seguridad, en **Elementos que se incluirán en la copia de seguridad**, haga clic en **Mostrar exclusiones**.

  Las exclusiones de archivos sobrescriben la selección de estos. Si especifica el mismo archivo en ambos campos, este archivo se omitirá durante el proceso de realización de la copia de seguridad.
- En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.
- En **Cifrado**, haga clic en **Especificar contraseña**.
  - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
  - Haga clic en **Aceptar**.

Recuperación de Google Drive y archivos de Google Drive

Recuperación de un Google Drive completo

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia quiere recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario cuyo Google Drive quiera recuperar y haga clic en **Recuperación**.

   Si se ha eliminado el usuario, seleccione el usuario de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.

   Nota
   Para ver únicamente los puntos de recuperación que incluyan archivos de Google Drive, seleccione **Google Drive** en **Filtrar por contenido**.

5. Haga clic en **Recuperar** > **Todo Drive**.

© Acronis International GmbH, 2003-2025

6. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, haga clic en **Organización de Google Workspace** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe seleccionar una nueva organización de destino de entre las que se encuentran registradas y disponibles.
7. En **Recuperar a la unidad** puede consultar, cambiar o especificar el usuario de destino o la unidad compartida de destino.

   De manera predeterminada, se selecciona el usuario original. Si este usuario no existe o se selecciona una organización que no es la original, debe indicar el usuario de destino o la unidad compartida de destino.

   Si la copia de seguridad incluye archivos compartidos, los archivos se recuperarán en la carpeta raíz de la unidad de destino.
8. Seleccione si quiere recuperar los permisos para compartir de los archivos.
9. Haga clic en **Iniciar recuperación**.
10. Seleccione una de las opciones de sobreescritura:

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir archivos existentes	Todos los archivos existentes en la ubicación de destino se sobrescribirán, independientemente de la última fecha de modificación.
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

11. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de archivos de Google Drive

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia quiere recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija el usuario cuyos archivos de Google Drive quiera recuperar y haga clic en **Recuperación**.

   Si se ha eliminado el usuario, seleccione el usuario de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar usuarios por el nombre. No se pueden usar caracteres comodín.

© Acronis International GmbH, 2003-2025

4. Seleccione un punto de recuperación.

   Nota
   Para ver únicamente los puntos de recuperación que incluyan archivos de Google Drive, seleccione **Google Drive** en **Filtrar por contenido**.

5. Haga clic en **Recuperar** > **Archivos/carpetas**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de archivos y carpetas deseados.
7. Seleccione los archivos que desea recuperar.

   Si la copia de seguridad no está cifrada y ha seleccionado un único archivo, puede hacer clic en **Mostrar versiones** para seleccionar la versión del archivo que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.
8. Si desea descargar un archivo, selecciónelo, haga clic en **Descargar**, seleccione la ubicación en la que se guardará y, a continuación, haga clic en **Guardar**. De lo contrario, omita este paso.
9. Haga clic en **Recuperar**.
10. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, haga clic en **Organización Google Workspace** para verla, modificarla o especificar la organización de destino.

    De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe seleccionar una nueva organización de destino de entre las que se encuentran registradas y disponibles.
11. En **Recuperar a la unidad** puede consultar, cambiar o especificar el usuario de destino o la unidad compartida de destino.

    De manera predeterminada, se selecciona el usuario original. Si este usuario no existe o se selecciona una organización que no es la original, debe indicar el usuario de destino o la unidad compartida de destino.
12. En **Ruta** puede consultar o cambiar la carpeta de destino en el Google Drive del usuario de destino o en la unidad compartida de destino. De manera predeterminada se selecciona la ubicación original.
13. Seleccione si quiere recuperar los permisos para compartir de los archivos.
14. Haga clic en **Iniciar recuperación**.
15. Seleccione una de las opciones de sobreescritura de archivos:

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir	Todos los archivos existentes en la ubicación de destino se sobrescribirán,

© Acronis International GmbH, 2003-2025

Opción	Descripción
archivos existentes	independientemente de la última fecha de modificación.
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

16. Haga clic en **Continuar** para confirmar su decisión.

Protección de archivos de unidades compartidas

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copias de seguridad de una unidad compartida completa, o bien de archivos o carpetas individuales. Los archivos se incluyen en la copia de seguridad junto con sus permisos para compartir.

Importante
No se ha hecho una copia de seguridad de la carpeta **Compartido conmigo**.

Limitaciones

- No se pueden realizar copias de seguridad de una unidad compartida sin miembros por las limitaciones de la API de Google Drive.
- De los formatos de archivo específicos de Google, los de Documentos de Google, Hojas de cálculo de Google y Presentaciones de Google son totalmente compatibles para la copia de seguridad y recuperación. Es posible que otros formatos específicos de Google no sean totalmente compatibles o no lo sean en absoluto. Por ejemplo, los archivos de Dibujos de Google se recuperan como archivos `.svg`, los de Sitios de Google como archivos `.txt`, los de Google Jamboard como archivos `.pdf` y los de Google My Maps se omiten durante una copia de seguridad.

  Nota
  Los formatos de archivos que no son específicos de Google, por ejemplo, `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png` o `.zip`, son totalmente compatibles para la copia de seguridad y recuperación.

¿Qué elementos de datos pueden recuperarse?

Puede recuperar una unidad compartida completa, o bien cualquier archivo o carpeta incluida en una copia de seguridad.

Puede elegir entre recuperar los permisos para compartir o permitir que los archivos hereden los permisos de la carpeta desde donde se recuperan.

Los siguientes elementos no se recuperan:

© Acronis International GmbH, 2003-2025

- Los permisos compartidos de un archivo que se compartió con un usuario de fuera de la organización no se recuperan si la opción de compartir fuera de la organización está deshabilitada en la unidad compartida de destino.
- Los permisos compartidos de un archivo que se compartió con un usuario que no forma parte de la unidad compartida de destino no se recuperan si la opción **Compartir con usuarios que no sean miembros** está deshabilitada en la unidad compartida de destino.

Limitaciones

- Los comentarios de los archivos no se pueden recuperar.
- Los enlaces para compartir para los archivos y las carpetas no se recuperan.

Selección de archivos de unidades compartidas

Seleccione los archivos tal como se describe a continuación y, luego, especifique otros ajustes del plan de protección según corresponda.

Para seleccionar archivos de unidades compartidas:

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos de los usuarios quiera recuperar. De lo contrario, omita este paso.
3. Realice uno de los siguientes procedimientos:
   - Para realizar una copia de seguridad de todas las unidades compartidas (incluidas las que se crearán en el futuro), amplíe el nodo **Unidades compartidas**, seleccione **Todas las unidades compartidas** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de unidades compartidas individuales, amplíe el nodo **Unidades compartidas**, seleccione **Todas las unidades compartidas**, seleccione las unidades compartidas que quiera incluir en la copia de seguridad y haga clic en **Copia de seguridad**.
4. En el plan de copias de seguridad, configure lo siguiente:
   - En **Elementos que se incluirán en la copia de seguridad**, realice uno de los siguientes procedimientos:
     - Mantenga los ajustes predeterminados **[Todos]** (todos los archivos).
     - Especifique los archivos y las carpetas que quiere incluir en la copia de seguridad. Para ello, añada sus nombres o rutas.

       Puede usar los caracteres comodín (*, **, y ?). Para obtener más información sobre la especificación de rutas y el uso de los caracteres comodín, consulte la sección "Filtros de archivo".
     - Examine los archivos y las carpetas para especificar cuáles quiere incluir en la copia de seguridad.

       El enlace **Examinar** está disponible únicamente cuando se crea un plan de protección para una sola unidad compartida.

© Acronis International GmbH, 2003-2025

- [Opcional] Para especificar los archivos y carpetas que se omitirán durante la copia de seguridad, en **Elementos que se incluirán en la copia de seguridad**, haga clic en **Mostrar exclusiones**.

  Las exclusiones de archivos sobrescriben la selección de estos. Si especifica el mismo archivo en ambos campos, este archivo se omitirá durante el proceso de realización de la copia de seguridad.
- En **Cuánto tiempo mantenerlo**, configure las reglas de retención para las copias de seguridad.
- En **Cifrado**, haga clic en **Especificar contraseña**.
  - Especifique y confirme la contraseña de cifrado y, a continuación, seleccione el algoritmo de cifrado.
  - Haga clic en **Aceptar**.

Recuperación de unidades compartidas y archivos de unidades compartidas

Recuperación de una unidad compartida completa

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia quiere recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Unidades compartidas**, seleccione **Todas las unidades compartidas**, elija la unidad compartida que quiera recuperar y haga clic en **Recuperación**.

   Si se ha eliminado la unidad compartida, selecciónela en la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

   Puede buscar unidades compartidas por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Toda la unidad compartida**.
6. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, haga clic en **Organización de Google Workspace** para verla, modificarla o especificar la organización de destino.

   De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe seleccionar una nueva organización de destino de entre las que se encuentran registradas y disponibles.
7. En **Recuperar a la unidad** puede consultar, cambiar o especificar el usuario de destino o la unidad compartida de destino. Si especifica un usuario, los archivos se recuperarán en el Google Drive de ese usuario.

   De manera predeterminada, se selecciona la unidad compartida original. Si esta unidad compartida no existe o se selecciona una organización que no es la original, debe indicar el usuario de destino o la unidad compartida de destino.

© Acronis International GmbH, 2003-2025

8. Seleccione si quiere recuperar los permisos para compartir de los archivos.
9. Haga clic en **Iniciar recuperación**.
10. Seleccione una de las opciones de sobreescritura:

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir archivos existentes	Todos los archivos existentes en la ubicación de destino se sobrescribirán, independientemente de la última fecha de modificación.
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

11. Haga clic en **Continuar** para confirmar su decisión.

Recuperación de archivos de unidades compartidas

1. Haga clic en **Google Workspace**.
2. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, seleccione la organización cuyos datos incluidos en la copia quiere recuperar. De lo contrario, omita este paso.
3. Amplíe el nodo **Unidades compartidas**, seleccione **Todas las unidades compartidas**, elija la unidad compartida que contenía los archivos que quiere recuperar y haga clic en **Recuperación**.
   Si se ha eliminado la unidad compartida, selecciónela en la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
   Puede buscar unidades compartidas por el nombre. No se pueden usar caracteres comodín.
4. Seleccione un punto de recuperación.
5. Haga clic en **Recuperar** > **Archivos/carpetas**.
6. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de archivos y carpetas deseados.
7. Seleccione los archivos que desea recuperar.
   Si la copia de seguridad no está cifrada y ha seleccionado un único archivo, puede hacer clic en **Mostrar versiones** para seleccionar la versión del archivo que quiera recuperar. Puede elegir cualquier versión de la que se haya realizado una copia de seguridad, anterior o posterior al punto de recuperación seleccionado.
8. Si desea descargar un archivo, selecciónelo, haga clic en **Descargar**, seleccione la ubicación en la que se guardará y, a continuación, haga clic en **Guardar**. De lo contrario, omita este paso.
9. Haga clic en **Recuperar**.

© Acronis International GmbH, 2003-2025

10. Si se añadieron varias organizaciones de Google Workspace al servicio Cyber Protection, haga clic en **Organización de Google Workspace** para verla, modificarla o especificar la organización de destino.

    De manera predeterminada, se selecciona la organización original. Si esta organización ya no se encuentra registrada en el servicio Cyber Protection, debe seleccionar una nueva organización de destino de entre las que se encuentran registradas y disponibles.
11. En **Recuperar a la unidad** puede consultar, cambiar o especificar el usuario de destino o la unidad compartida de destino. Si especifica un usuario, los archivos se recuperarán en el Google Drive de ese usuario.

    De manera predeterminada, se selecciona la unidad compartida original. Si esta unidad compartida no existe o se selecciona una organización que no es la original, debe indicar el usuario de destino o la unidad compartida de destino.
12. En **Ruta** puede consultar o cambiar la carpeta de destino en el Google Drive del usuario de destino o en la unidad compartida de destino. De manera predeterminada se selecciona la ubicación original.
13. Seleccione si quiere recuperar los permisos para compartir de los archivos.
14. Haga clic en **Iniciar recuperación**.
15. Seleccione una de las opciones de sobreescritura de archivos:

Opción	Descripción
Sobrescribir un archivo existente si es más antiguo	Si hay un archivo con el mismo nombre en la ubicación de destino y es más antiguo que el archivo de origen, el archivo de origen se guardará en la ubicación de destino y reemplazará la versión anterior.
Sobrescribir archivos existentes	Todos los archivos existentes en la ubicación de destino se sobrescribirán, independientemente de la última fecha de modificación.
No sobrescribir archivos existentes	Si hay un archivo con el mismo nombre en la ubicación de destino, no se le aplicarán cambios, y el archivo de origen no se guardará en la ubicación de destino.

16. Haga clic en **Continuar** para confirmar su decisión.

Notarización

La notarización permite demostrar que un archivo es auténtico y que no ha cambiado desde su copia de seguridad. Se recomienda habilitar la notarización cuando realice la copia de seguridad de documentos legales u otros archivos cuya autenticidad se desee demostrar.

La notarización solo está disponible para copias de seguridad de archivos de Google Drive y archivos de unidad compartida de Google Workspace.

© Acronis International GmbH, 2003-2025

Cómo utilizar la notarización

Para activar la certificación de todos los archivos seleccionados para copias de seguridad, active el conmutador **Notarización** cuando cree un plan de protección.

Al configurar la recuperación, los archivos notarizados se marcarán con un icono especial y podrá verificar la autenticidad del archivo.

Cómo funciona

Durante una copia de seguridad, el agente calcula los códigos de cifrado de los archivos de los que se ha realizado la copia de seguridad, crea un árbol de cifrado (en función de la estructura de carpetas), guarda el árbol en la copia de seguridad y envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización guarda la raíz del árbol de cifrado en la base de datos de cadenas de bloques de Ethereum para garantizar que este valor no cambie.

Al verificar la autenticidad del archivo, el agente calcula su cifrado y lo compara con el almacenado en el árbol de cifrado de la copia de seguridad. Si los cifrados no coinciden, se considerará que el archivo no es auténtico. De lo contrario, la autenticidad del archivo queda garantizada por el árbol de cifrado.

Para verificar que el propio árbol de cifrado no se haya visto alterado, el agente envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización lo compara con el almacenado en la base de datos de cadenas de bloques. Si los cifrados coinciden, se garantiza que el archivo seleccionado es auténtico. De lo contrario, el software muestra un mensaje para indicar que el archivo no es auténtico.

Verificar la autenticidad del archivo con Notary Service

Si se ha habilitado la notarización durante la copia de seguridad, puede verificar la autenticidad de un archivo del que se ha realizado la copia de seguridad.

Para verificar la autenticidad del archivo

1. Realice uno de los siguientes procedimientos:
   - Para comprobar la autenticidad de un archivo de Google Drive, seleccione el archivo tal como se describe en los pasos de 1 a 7 de la sección "Recuperación de archivos de Google Drive".
   - Para comprobar la autenticidad de un archivo de unidad compartida de Google Workspace, seleccione el archivo tal como se describe en los pasos de 1 a 7 de la sección "Recuperación de archivos de unidades compartidas".
2. Asegúrese de que el archivo seleccionado esté marcado con el siguiente icono:  . Esto significa que el archivo está notarizado.
3. Realice uno de los siguientes procedimientos:
   - Haga clic en **Verificar**.
     El software comprueba la autenticidad del archivo y muestra el resultado.

© Acronis International GmbH, 2003-2025

- Haga clic en **Obtener certificado**.

  Se abre un certificado que confirma la notarización del archivo en una ventana de navegador web. La ventana también incluye instrucciones que le permiten verificar la autenticidad del archivo manualmente.

Búsqueda en copias de seguridad de nube a nube

Al recuperar datos, puede realizar una búsqueda de elementos específicos respaldados en lugar de navegar por el archivo de copia de seguridad.

Las capacidades de búsqueda tienen dependencia de lo siguiente:

- Tipo de búsqueda: mejorada (basada en índices) o típica (no basada en índices)

  La búsqueda basada en índices es más rápida y proporciona opciones adicionales, como mostrar versiones de los elementos con copia de seguridad, buscar en los nombres de los archivos adjuntos y la búsqueda de texto completo en las copias de seguridad de Gmail.
- Tipo de archivo comprimido: cifrado o no cifrado
  - En las copias de seguridad no cifradas, la búsqueda siempre está disponible. Solo se soporta la búsqueda mejorada (basada en índice).
  - En las copias de seguridad cifradas, la búsqueda mejorada (basada en índices) está disponible como opción.

    Si no habilita la búsqueda mejorada, la búsqueda básica estará disponible para las copias de seguridad de los buzones de correo de Microsoft 365. Para todos los demás recursos informáticos, la búsqueda no estará disponible. La tabla que aparece a continuación resume las opciones disponibles para las copias de seguridad cifradas.

Tipo de carga de trabajo	Qué recuperar	La búsqueda mejorada está desactivada	La búsqueda mejorada está habilitada
Cargas de trabajo de Microsoft 365			
Casilla de correo	Mensajes de correo electrónico	La búsqueda básica (no basada en índice) está disponible	La búsqueda mejorada (basada en índice) está disponible.
OneDrive	Archivos/carpetas	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible.
Sitio de SharePoint	Archivos de SharePoint	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible
Teams	Canales	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible.

© Acronis International GmbH, 2003-2025

Tipo de carga de trabajo	Qué recuperar	La búsqueda mejorada está desactivada	La búsqueda mejorada está habilitada
	Mensajes de correo electrónico	La búsqueda básica (no basada en índice) está disponible	La búsqueda mejorada (basada en índice) está disponible.
	Sitio de equipo	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible.
Cargas de trabajo de Google Workspace			
Casilla de correo	Mensajes de correo electrónico	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible.
Google Drive	Archivos/carpetas	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible.
Unidades compartidas	Archivos/carpetas	La búsqueda no está disponible	La búsqueda mejorada (basada en índice) está disponible.

Búsqueda en todo el texto

La búsqueda de texto completo está disponible solo para las copias de seguridad de Gmail y está habilitada por defecto. Con ella, puede buscar en el texto del cuerpo de los correos electrónicos respaldados. Si esta opción está desactivada, puede buscar solo por asunto, remitente, destinatario y fecha.

Un índice de búsqueda de texto completo ocupa entre el 10 y el 30 por ciento del espacio de almacenamiento que utiliza la copia de seguridad de Gmail. Un índice sin datos de búsqueda de texto completo es significativamente más pequeño. Para ahorrar espacio de almacenamiento, puede desactivar la búsqueda de texto completo y limpiar la porción del índice que contiene los datos de búsqueda de texto completo.

Índices de búsqueda

Los índices de búsqueda ofrecen funciones de búsqueda mejoradas en los archivos de copia de seguridad de la nube a la nube.

Los archivos comprimidos se indexan automáticamente después de cada operación de copia de seguridad. El proceso de indexación no afecta al rendimiento de la copia de seguridad porque la indexación y la copia de seguridad se realizan por diferentes componentes de software.

Mostrar los resultados de búsqueda aparece disponible después de que se complete la operación de indexación, lo cual podría tardar hasta 24 horas. Indexar la primera copia de seguridad, que es

© Acronis International GmbH, 2003-2025

completa, generalmente lleva más tiempo que indexar las copias de seguridad incrementales sucesivas.

Todos los índices contienen metadatos compatibles con la funcionalidad principal de búsqueda: búsqueda por asunto, remitente, destinatario o fecha. Los índices para las copias de seguridad de Gmail contienen datos adicionales si la búsqueda de texto completo está habilitada.

Comprobar el tamaño de un índice de búsqueda

Los índices de búsqueda se amplían con el tiempo. Los índices de los archivos de copia de seguridad en los que se habilita la búsqueda de texto completo podrían ocupar hasta el 30 % del tamaño del archivo comprimido.

Para comprobar el tamaño de un índice de búsqueda

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. En la pestaña **Almacenamiento de la copia de seguridad**, haga clic en **Copia de seguridad de aplicaciones en la nube**.
3. Verifique el valor de la columna **Tamaño del índice**.

Actualizar, reconstruir o eliminar índices

Para solucionar problemas relacionados con la búsqueda en las copias de seguridad de la nube a la nube, puede actualizar, reconstruir o eliminar índices de búsqueda.

Nota
Las operaciones con índices no son compatibles con las copias de seguridad cifradas.

Estas operaciones pueden llevar mucho tiempo y solo están disponibles para los administradores, como se indica a continuación:

Tipo de inquilino	Rol	Puede actualizar índices	Puede reconstruir índices	Puede eliminar índices
Inquilino de partner	Administrador de la empresa	+	+	+
	Administrador de ciberprotección	+	-	-
	Administrador de protección	+	-	-
	Administrador de protección (de) solo lectura	-	-	-

© Acronis International GmbH, 2003-2025

Tipo de inquilino	Rol	Puede actualizar índices	Puede reconstruir índices	Puede eliminar índices
Inquilino de cliente	Administrador de la empresa	+	-	-
	Administrador de protección	+	-	-
	Administrador de protección (de) solo lectura	-	-	-
Unidad	Administrador de la unidad	+	-	-
	Administrador de protección	+	-	-
	Administrador de protección (de) solo lectura	-	-	-

Para actualizar, reconstruir o eliminar un índice

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. En la pestaña **Almacenamiento de la copia de seguridad**, haga clic en **Copia de seguridad de aplicaciones en la nube**.
3. Seleccione el archivo comprimido cuyo índice desea actualizar, reconstruir o eliminar.
4. En el panel **Acciones**, seleccione la acción que desea realizar:
   - **Actualizar índice**: los puntos de recuperación en el archivo comprimido se verifican y se agregan los índices restantes.
   - **Reconstruir índice**: los índices de todos los puntos de recuperación del archivo se eliminan y luego se crean nuevamente.
   - **Eliminar índice**: se eliminan los índices de todos los puntos de recuperación del archivo.
5. Seleccione el ámbito de la acción y luego haga clic en **OK**.
   Dependiendo del archivo comprimido y la acción seleccionada, una o más de las siguientes opciones están disponibles:
   - **Solo metadatos**
   - **Solo contenido**
   - **Búsqueda de metadatos y contenido**

Habilitar la búsqueda mejorada en copias de seguridad cifradas

Puede habilitar la búsqueda mejorada (basada en índices) en un nuevo plan de copias de seguridad o en un plan de copias de seguridad existente.

Si no activa la búsqueda mejorada, la búsqueda básica estará disponible para las copias de seguridad de los buzones de correo de Microsoft 365. Para todas las demás cargas de trabajo, la búsqueda no estará disponible. Para obtener más información sobre las opciones disponibles, consulte "Búsqueda en copias de seguridad de nube a nube" (p. 931).

© Acronis International GmbH, 2003-2025

Pasos para habilitar la búsqueda mejorada

En un nuevo plan de copia de seguridad

1. En la consola de Cyber Protect, vaya a **Gestión** > **Copias de seguridad de aplicaciones de la nube**.
2. Haga clic en **Crear plan**.
3. Habilite el interruptor **Cifrado** y, a continuación, especifique y confirme la contraseña de cifrado.
4. Seleccione el algoritmo de cifrado.
5. Seleccione la casilla de verificación **Permitir búsqueda mejorada en copias de seguridad cifradas**.
6. Configure las opciones restantes en el plan de copias de seguridad y haga clic en **Listo**.

Nota
No puede deshabilitar el cifrado, cambiar la contraseña de cifrado o deshabilitar la búsqueda mejorada más adelante. Para crear una copia de seguridad sin cifrar, cambiar la contraseña de cifrado o crear una copia de seguridad en la que la búsqueda mejorada esté deshabilitada, cree un nuevo plan de copias de seguridad.

En un plan de copias de seguridad existente

1. En la consola de Cyber Protect, vaya a **Gestión** > **Copias de seguridad de aplicaciones de la nube**.
2. Seleccione el plan de copias de seguridad en el que desea habilitar la búsqueda mejorada y haga clic en **Editar**.
3. Haga clic en el icono de engranaje junto al nombre del plan y, a continuación, seleccione la pestaña **Opciones de búsqueda**.
4. Habilite el interruptor y haga clic en **Listo**.
5. Haga clic en **Guardar configuración**.

Como resultado, una operación de indexación se iniciará después de que se complete la próxima copia de seguridad.

Nota
No podrá deshabilitar la búsqueda mejorada más adelante. Para crear una copia de seguridad en la que la búsqueda mejorada esté deshabilitada, cree un nuevo plan de copias de seguridad.

Deshabilitar la búsqueda de texto completo para las copias de seguridad de Gmail

Es posible que quiera deshabilitar la búsqueda de texto completo si necesita mantener el tamaño del índice de búsqueda al mínimo.

© Acronis International GmbH, 2003-2025

Si más adelante vuelve a habilitar la búsqueda de texto completo, todos los archivos comprimidos creados por este plan de copias de seguridad se indexarán de nuevo. Esta es una operación que consume mucho tiempo.

Para deshabilitar la búsqueda de texto completo

1. Al crear o editar un plan de copias de seguridad, haga clic en el icono de engranaje en la esquina superior derecha.
2. En la pestaña **Búsqueda en todo el texto**, deshabilite el interruptor.
3. Haga clic en **Listo**.
4. [Al crear un plan] Haga clic en **Aplicar**.
5. [Al editar un plan] Haga clic en **Guardar configuración**.

Protección de base de datos de Oracle

Nota
Esta función está disponible con el paquete Advanced Backup.

La protección de la base de datos de Oracle se describe en un documento independiente disponible en https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

Protección de SAP HANA

Nota
Esta función está disponible con el paquete Advanced Backup.

Puede consultar información sobre la protección de SAP HANA en otro documento disponible en https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

Protección de datos de MySQL y MariaDB

Puede proteger los datos de MySQL y MariaDB mediante la copia de seguridad con información de aplicaciones. Recopila metadatos de aplicaciones y permite una recuperación granular en el nivel de la instancia, base de datos o tabla.

Nota
La copia de seguridad con información de aplicaciones de los datos de MySQL o MariaDB está disponible con el paquete Advanced Backup.

Para proteger una máquina virtual o física que ejecute instancias MySQL o MariaDB con copia de seguridad con información de aplicaciones, deberá instalar Agente para MySQL/MariaDB en este equipo. Agente para MySQL/MariaDB se incluye en el paquete de Agente para Linux (64 bits) y por

© Acronis International GmbH, 2003-2025

lo tanto solo puede instalarse en sistemas operativos basados en Linux de 64 bits. Consulte "Sistemas operativos y entornos compatibles para la copia de seguridad y la recuperación" (p. 499).

Cómo descargar el archivo de instalación de Agente para Linux (64 bits)

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en el icono de la cuenta en la esquina superior derecha y seleccione **Descargas**.
3. Haga clic en **Agente para Linux (64 bits)**.

El archivo de instalación se descargará en su equipo. Para instalar el agente, proceda como se describe en "Instalación de agentes de protección en Linux" (p. 70) o "Instalación y desinstalación de agentes de protección en Linux" (p. 93). Asegúrese de que ha seleccionado Agente para MySQL/MariaDB, que es un componente opcional.

Para recuperar bases de datos y tablas de una instancia activa, Agente para MySQL/MariaDB necesita un almacenamiento temporal para funcionar. De manera predeterminada, se utiliza el directorio `/tmp`. Puede cambiar este directorio configurando la variable de entorno `ACRONIS_MYSQL_RESTORE_DIR`.

Limitaciones

- Los clústeres MySQL o MariaDB no son compatibles.
- Las instancias de MySQL o MariaDB que se ejecutan en contenedores de Docker no son compatibles.
- Las instancias de MySQL o MariaDB que se ejecutan en sistemas operativos que usan el sistema de archivos BTRFS no son compatibles.
- Las bases de datos del sistema (`sys`, `mysql`, `information-schema` y `performance_schema`) y las bases de datos que no contienen ninguna tabla no se pueden recuperar de las instancias activas. Sin embargo, estas bases de datos pueden recuperarse como archivos cuando se recupera toda al instancia.
- La recuperación solo es compatible en instancias de destino de la misma versión que la instancia con copia de seguridad o posterior, con las siguientes restricciones:
  - La recuperación de instancias de MySQL 5.x a MySQL 8.x no es compatible.
  - La recuperación a una versión de MySQL 5.x posterior (incluidas las versiones menores) es compatible solo mediante recuperación de toda la instancia como archivos. Antes de intentar realizar la recuperación, consulte la guía de actualización de MySQL oficial para la versión de destino, por ejemplo, la guía de actualización de MySQL 5.7.
- La recuperación de copias de seguridad almacenadas en Secure Zone no es compatible.
- Agente para MySQL/MariaDB que se ejecuta en un equipo en el que está instalado AppArmor no puede recuperar bases de datos ni tablas. Pero puede recuperar una instancia como archivos o todo el equipo.
- La recuperación de bases de datos de destino configuradas con vínculos simbólicos no es compatible. Puede recuperar las bases de datos con copia de seguridad como bases de datos nuevas si cambia el nombre.

© Acronis International GmbH, 2003-2025

Problemas conocidos

Si tiene algún problema al recuperar los datos de recursos compartidos de Samba protegidos con contraseña, cierre y vuelva a iniciar la sesión de la consola de Cyber Protect. Seleccione el punto de recuperación y haga clic en **Bases de datos de MySQL o MariaDB**. No haga clic en **Todo el equipo** ni en **Archivos/carpetas**.

Configurar una copia de seguridad con información de aplicaciones

Requisitos previos

- Debe haber, por lo menos, una instancia de MySQL o MariaDB ejecutándose en el equipo seleccionado.
- Se debe iniciar el agente de protección con el usuario raíz en el equipo donde se esté ejecutando la instancia de MySQL o MariaDB.
- La copia de seguridad con información de aplicaciones solo está disponible si se selecciona **Todo el equipo** como fuente de copia de seguridad en el plan de protección.
- Se deberá deshabilitar la opción de copia de seguridad **Sector por sector** del plan de protección. De lo contrario, no se podrán recuperar los datos de las aplicaciones.

Cómo configurar una copia de seguridad con información de aplicaciones

1. En la consola de Cyber Protect, seleccione uno o más equipos en los que se estén ejecutando instancias de MySQL o MariaDB.
   Puede tener una o más instancias en cada equipo.
2. Cree un plan de protección con el módulo de copia de seguridad habilitado.
3. En **Qué incorporar en la copia de seguridad**, seleccione **Todo el equipo**.
4. Haga clic en **Copia de seguridad de aplicación** y active el conmutador que se encuentra junto a **MySQL/MariaDB Server**.
5. Seleccionar cómo especificar las instancias de MySQL o MariaDB:
   - **Para todas las cargas de trabajo**
     Use esta opción si ejecuta instancias con la misma configuración en varios servidores. Se usarán los mismos parámetros de conexión y credenciales de acceso para todas las instancias.
   - **Para cargas de trabajo específicas**
     Use esta opción para especificar los parámetros de conexión y credenciales de acceso de cada instancia.
6. Haga clic en **Añadir instancia** para configurar los parámetros de conexión y las credenciales de acceso.
   a. Seleccione el tipo de conexión de la instancia y especifique la siguiente información:
      - [Para el socket TCP] Dirección IP y puerto.
      - [Para el socket Unix] Ruta de socket.

© Acronis International GmbH, 2003-2025

b. Especifique las credenciales de una cuenta de usuario que tenga los siguientes privilegios para la instancia:
   - `FLUSH_TABLES` O `RELOAD` para todas las bases de datos y tablas (`*.*`)
   - `SELECT` para `information_schema.tables`

c. Haga clic en **Aceptar**.

7. Haga clic en **Listo**.

Recuperación de datos a partir de una copia de seguridad con información de aplicaciones

Puede recuperar instancias, bases de datos y tablas de MySQL o MariaDB a partir de una copia de seguridad con información de aplicaciones. También puede recuperar todo el servidor en el que se ejecutan las instancias o los archivos y carpetas de este servidor.

En la tabla siguiente se resumen todas las opciones de recuperación.

Qué recuperar	Recuperar como	Recuperar a
Servidor MySQL Servidor MariaDB	Todo el equipo	Equipo* en el que está instalado Agente para Linux
Servidor MySQL Servidor MariaDB	Archivos o carpetas	Equipo* en el que está instalado Agente para Linux
Instancia	Archivos	Equipo* en el que está instalado Agente para MySQL/MariaDB
Base de datos	La misma base de datos Nueva base de datos	Equipo* en el que está instalado Agente para MySQL/MariaDB • Instancia original • Otra instancia • Base de datos original • Nueva base de datos
Tabla	La misma tabla Nueva tabla	Equipo* en el que está instalado Agente para MySQL/MariaDB • Instancia original • Otra instancia • Base de datos original • Tabla original • Nueva tabla

© Acronis International GmbH, 2003-2025

* Una máquina virtual con un agente dentro se trata como un equipo físico desde el punto de vista de copia de seguridad.

Recuperación de todo el servidor

Para obtener información sobre cómo recuperar todo el servidor en el que se ejecutan las instancias de MySQL o MariaDB, consulte "Recuperación" (p. 653).

Recuperación de instancias

Puede recuperar instancias de MySQL o MariaDB como archivos a partir de una copia de seguridad con información de aplicaciones.

Cómo recuperar una instancia

1. En la consola de Cyber Protect, seleccione el equipo que contenía originalmente los datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:

   - Si la copia de seguridad se encuentra en el almacenamiento compartido o en la nube (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para MySQL/MariaDB y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña **Almacenamiento de la copia de seguridad**.

   El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación.
4. Haga clic en **Recuperar** > **Bases de datos de MySQL o MariaDB**.
5. Seleccione la instancia que desea recuperar y, a continuación, haga clic en **Recuperar como archivos**.
6. En **Ruta**, seleccione el directorio en el que se recuperarán los archivos.
7. Haga clic en **Iniciar recuperación**.

Recuperación de bases de datos

Puede recuperar bases de datos a partir de una copia de seguridad con información de aplicaciones en instancias activas de MySQL o MariaDB.

1. En la consola de Cyber Protect, seleccione el equipo que contenía originalmente los datos que desea recuperar.
2. Haga clic en **Recuperación**.

© Acronis International GmbH, 2003-2025

3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:

   - Si la copia de seguridad se encuentra en el almacenamiento compartido o en la nube (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para MySQL/MariaDB y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña **Almacenamiento de la copia de seguridad**.

   El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación.
4. Haga clic en **Recuperar** > **Bases de datos de MySQL o MariaDB**.
5. Haga clic en el nombre de la instancia deseada para profundizar en sus bases de datos.
6. Seleccione una o más bases datos que desee recuperar.
7. Haga clic en **Recuperar**.
8. Haga clic en **Instancia de destino MySQL/MariaDB** para especificar los parámetros de conexión y credenciales de acceso de la instancia de destino.
   - Compruebe la instancia en la que desea recuperar los datos. De manera predeterminada, se selecciona la instancia original.
   - Especifique las credenciales de una cuenta de usuario que pueda acceder a la instancia de destino. Esta cuenta de usuario debe tener los siguientes privilegios asignados para todas las bases de datos y tablas (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Haga clic en **Aceptar**.
9. Compruebe la base de datos de destino.

   De manera predeterminada, se selecciona la base de datos original.

   Para recuperar una base de datos como una nueva, haga clic en el nombre de la base de datos de destino y cámbielo. Esta acción solo está disponible si recupera una única base de datos.
10. En **Sobrescribir las bases de datos existentes**, seleccione el modo de sobrescritura.

    La sobrescritura está habilitada de forma predeterminada y la base de datos con copia de seguridad sustituirá a la de destino que tiene el mismo nombre.

    Si se desactiva la sobrescritura, la base de datos con copia de seguridad se omitirá durante la operación de recuperación y no sustituirá a la de destino que tiene el mismo nombre.

© Acronis International GmbH, 2003-2025

11. Haga clic en **Iniciar recuperación**.

Recuperación de tablas

Puede recuperar tablas a partir de una copia de seguridad con información de aplicaciones en instancias activas de MySQL o MariaDB.

1. En la consola de Cyber Protect, seleccione el equipo que contenía originalmente los datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:

   - Si la copia de seguridad se encuentra en el almacenamiento compartido o en la nube (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para MySQL/MariaDB y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña **Almacenamiento de la copia de seguridad**.

   El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación.
4. Haga clic en **Recuperar** > **Bases de datos de MySQL o MariaDB**.
5. Haga clic en el nombre de la instancia deseada para profundizar en sus bases de datos.
6. Haga clic en el nombre de la base de datos deseada para profundizar en sus tablas.
7. Seleccione una o más tablas que desee recuperar.
8. Haga clic en **Recuperar**.
9. Haga clic en **Instancia de destino MySQL/MariaDB** para especificar los parámetros de conexión y credenciales de acceso de la instancia de destino.
   - Compruebe la instancia en la que desea recuperar los datos. De manera predeterminada, se selecciona la instancia original.
   - Especifique las credenciales de una cuenta de usuario que pueda acceder a la instancia de destino. Esta cuenta de usuario debe tener los siguientes privilegios asignados para todas las bases de datos y tablas (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`

© Acronis International GmbH, 2003-2025

- Haga clic en **Aceptar**.

10. Compruebe la tabla de destino.

    De manera predeterminada, se selecciona la tabla original.

    Para recuperar una tabla como una nueva, haga clic en el nombre de la tabla de destino y cámbielo. Esta acción solo está disponible si recupera una única tabla.
11. En **Sobrescribir tablas existentes**, seleccione el modo de sobrescritura.

    La sobrescritura está habilitada de forma predeterminada y la tabla con copia de seguridad sustituirá a la de destino que tiene el mismo nombre.

    Si se desactiva la sobrescritura, la tabla con copia de seguridad se omitirá durante la operación de recuperación y no sustituirá a la de destino que tiene el mismo nombre.
12. Haga clic en **Iniciar recuperación**.

Recuperación de rutinas almacenadas

Cuando se recupera una instancia de MySQL completa, las rutinas almacenadas se recuperan automáticamente.

Cuando se recupera una base de datos individual a una instancia no original, o bien cuando se recupera como una base de datos nueva, las rutinas almacenadas no se recuperan automáticamente. Puede recuperarlas de forma manual al exportarlas en un archivo SQL y al añadirlas posteriormente a la base de datos recuperada.

Para exportar las rutinas almacenadas y añadirlas a una base de datos recuperada

1. En el equipo con la instancia original de MySQL, abra el Terminal.
2. Ejecute el siguiente comando para exportar las rutinas almacenadas.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data > [exported_db_routines.sql]
   ```
4. En el equipo donde se haya recuperado la base de datos, abra el cliente de línea de comandos de MySQL.
5. Ejecute los siguientes comandos para añadir las rutinas a la base de datos recuperada.

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```

Protección de los equipos virtuales y contenedores Proxmox

Puede realizar copias de seguridad sin agente de máquinas virtuales y contenedores de Proxmox instalando el Agente para Proxmox en el host protegido.

© Acronis International GmbH, 2003-2025
   ```

El agente para Proxmox se incluye en el paquete del agente para Linux (64 bits) y requiere que el agente para Linux también esté instalado en el host. Para obtener más información sobre cómo descargar el archivo de instalación, consulte "Descarga de agentes de protección" (p. 49).

Se admiten los hosts que ejecutan Proxmox VE 8.2 o posterior. En entornos de clúster, debe instalar un agente en cada nodo.

Se requiere una cuota de **Máquina virtual** por máquina virtual o contenedor de Proxmox VE. No se requiere cuota para el equipo en el que se ejecuta el Agente para Proxmox.

Se admiten los siguientes almacenes de Proxmox para la copia de seguridad y la recuperación:

- Para máquinas virtuales: todos los equipos de almacenamiento en los que se puede crear una máquina virtual
- Para contenedores: LVM Thin, Ceph/RBD, BtrFS

Las siguientes ubicaciones de copia de seguridad están disponibles para máquinas virtuales y contenedores de Proxmox:

- El almacenamiento en la nube (incluido el almacenamiento alojado por socios)
- Almacenamiento en la nube pública
- Carpetas de red en recursos compartidos de SMB y NFS
- Carpetas locales

Limitaciones para cargas de trabajo de Proxmox

Las siguientes limitaciones se aplican a la copia de seguridad y recuperación de máquinas virtuales y contenedores de Proxmox.

General

- Las siguientes operaciones no son compatibles:
  - Ejecutar como VM
  - Conversión a VM
  - Copia de seguridad compatible con la aplicación
  - Replicación de equipos virtuales
- No puede recuperar discos virtuales o contenedores en el almacenamiento CephFS.
- No se hará copia de seguridad de los discos para los que la opción de copia de seguridad está deshabilitada en Proxmox VE.
- Durante una recuperación, seleccionar el tipo de aprovisionamiento de disco (fino/grueso) solo funcionará si el almacenamiento de destino admite el tipo seleccionado. Por ejemplo, el almacenamiento LVM solo admite discos gruesos. Si selecciona la asignación de disco fino, esta opción se ignorará.

Equipos virtuales

© Acronis International GmbH, 2003-2025

- Los siguientes elementos no se incluyen en las copias de seguridad:
  - Plantillas de VM
  - Discos separados
  - Instantáneas
  - Contenido del dispositivo del estado TPM.
    Cuando recupera una máquina virtual como un nuevo equipo, tendrá un nuevo dispositivo de estado TPM vacío. Por ejemplo, si BitLocker está habilitado en dicho equipo, debe usar la clave de recuperación de BitLocker.
- Se requiere al menos un almacenamiento de `Directory` para los archivos temporales.
- El seguimiento de bloques modificados (CBT) no está disponible para máquinas virtuales apagadas y máquinas virtuales que han pasado por un ciclo de energía (apagado y encendido). La falta de información de CBT puede provocar copias de seguridad más lentas.
- Durante una copia de seguridad, las máquinas virtuales apagadas se encienden y se mantienen en un estado congelado que no utiliza recursos de RAM o CPU en el host.
- No se puede realizar una copia de seguridad de la máquina virtual bloqueada. Por ejemplo, las máquinas virtuales en hibernación están bloqueadas.

Contenedores

- Sólo se admiten los siguientes tipos de almacenamiento para la copia de seguridad y la recuperación: LVM Thin, Ceph/RBD, BtrFS.
- No se admite el uso de contenedores para los que se deshabilitan las instantáneas.
- El seguimiento de los bloques modificados (CBT) no está disponible.
- No se recupera la propiedad `OS type`.

Instalación de Agente para Proxmox

El agente para Proxmox se incluye en el paquete del agente para Linux (64 bits) y requiere que el agente para Linux también esté instalado en el host protegido.

Debe instalar el agente para Proxmox localmente, en el host protegido, utilizando una de las siguientes opciones:

- Interfaz gráfica de usuario
  Para obtener más información, consulte "Instalación de agentes de protección en Linux" (p. 70).
- Interfaz de la línea de comandos
  Para obtener más información, consulte "Instalación y desinstalación de agentes de protección en Linux" (p. 93).

Después de instalar el agente en el host, puede ver todas las máquinas virtuales y contenedores que están disponibles en ese host en la consola de Cyber Protect, en la pestaña **Dispositivos** > **Proxmox**.

© Acronis International GmbH, 2003-2025

Copia de seguridad de cargas de trabajo de Proxmox

Puede realizar copias de seguridad de máquinas virtuales y contenedores de Proxmox.

Para hacer una copia de seguridad de una carga de trabajo, cree un plan de protección. Para obtener más información, consulte "Creación de un plan de protección" (p. 250).

En los planes de protección para cargas de trabajo de Proxmox, solo está disponible el módulo **Copia de seguridad**.

También puede realizar una copia de seguridad del host de Proxmox por separado, como un servidor Linux. Para evitar copias de seguridad duplicadas, puede configurar filtros de archivos en el plan de protección para el host y excluir los directorios que contienen los datos de la máquina virtual.

Recuperación de cargas de trabajo de Proxmox

Puede recuperar una copia de seguridad de la máquina virtual de Proxmox como:

- Máquina física.
- La máquina virtual original o una nueva en el mismo hipervisor.
- Una nueva máquina en un hipervisor diferente. Ver "Recuperación multiplataforma" (p. 655).

Para obtener más información sobre la recuperación de una máquina virtual, consulte "Recuperación de una máquina virtual como un equipo físico" (p. 679) y "Recuperación de una máquina virtual como máquina virtual" (p. 680).

Puede recuperar un contenedor de Proxmox respaldado como:

- El contenedor original.
- Un nuevo contenedor Proxmox. La recuperación multiplataforma no es compatible.

Para obtener más información sobre la recuperación de un contenedor, consulte "Recuperación de contenedores" (p. 691).

Puede recuperar archivos de las copias de seguridad de las máquinas virtuales y contenedores de Proxmox en el host de Proxmox o en el almacenamiento en red conectado a él. No puede realizar la recuperación a nivel de archivo en una máquina virtual o contenedor.

Protección de sitios web y servidores de alojamiento

Protección de los sitios web

Un sitio web puede resultar dañado como resultado de un acceso no autorizado o un ataque de malware. Realice una copia de seguridad de su sitio web si desea revertirlo con facilidad a un estado saludable, en caso de que resulte dañado.

© Acronis International GmbH, 2003-2025

¿Qué necesito para realizar una copia de seguridad de un sitio web?

El sitio web tiene que ser accesible mediante el protocolo SFTP o SSH. No necesita instalar un agente, solo añada el sitio web como se ha descrito anteriormente en esta sección.

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copia de seguridad de los siguientes elementos:

- **Archivos de contenido del sitio web**
  Todos los archivos accesibles para la cuenta que especifique para la conexión SFTP o SSH.
- **Bases de datos enlazadas (si hay alguna) alojadas en servidores MySQL.**
  Todas las bases de datos accesibles para la cuenta MySQL que especifique.

Si su sitio web emplea bases de datos, le recomendamos que haga copias de seguridad de los archivos y las bases de datos, para poder recuperarlas a un estado consistente.

Limitaciones

- La única ubicación de copia de seguridad disponible para la copia de seguridad del sitio web es el almacenamiento en la nube.
- Es posible aplicar varios planes de protección a un sitio web, pero solo uno de ellos puede ejecutarse de forma planificada. Otros planes deben iniciarse de forma manual.
- La única opción de copia de seguridad disponible es "Nombre del archivo de la copia de seguridad".
- Los planes de protección de sitios web no aparecen en la pestaña **Gestión** > **Planes de protección**.

Copia de seguridad de un sitio web

Cómo añadir un sitio web

1. Haga clic en **Dispositivos** > **Agregar**.
2. Haga clic en **Sitio web**.
3. Configure los siguientes parámetros de acceso para el sitio web:
   - En **Nombre del sitio web**, cree y escriba un nombre para su sitio web. Este nombre aparecerá en la consola de Cyber Protect.
   - En **Servidor**, especifique el nombre del host o la dirección IP que se usará para acceder al sitio web mediante SFTP o SSH. Por ejemplo, `my.server.com` o `10.250.100.100`.
   - En **Puerto**, especifique el número de puerto.
   - En **Nombre de usuario** y **Contraseña**, especifique las credenciales de la cuenta que se puede utilizar para acceder al sitio web mediante SFTP o SSH.

© Acronis International GmbH, 2003-2025

Importante
Solo se realizará copia de seguridad de los archivos a los que pueda acceder la cuenta especificada.

En lugar de una contraseña, puede especificar su clave SSH privada. Para ello, seleccione la opción **Usar clave SSH privada en lugar de una contraseña** y luego especifique la clave.

4. Haga clic en **Siguiente**.
5. Si su sitio web utiliza bases de datos MySQL, configure los parámetros de acceso para las bases de datos. En caso contrario, haga clic en **Omitir**.
   a. En **Tipo de conexión**, seleccione cómo acceder a las bases de datos desde la nube:
      - **Mediante SSH desde el host**: Se accederá a las bases de datos mediante el host especificado en el paso 3.
      - **Conexión directa**: Se accederá a las bases de datos directamente. Seleccione esta configuración solo si se puede acceder a las bases de datos desde Internet.
   b. En **Servidor**, especifique el nombre o la dirección IP del host donde se está ejecutando el servidor MySQL.
   c. En **Puerto**, especifique el número de puerto para la conexión TCP/IP al servidor. El número del puerto predeterminado es 3306.
   d. En **Nombre de usuario** y **Contraseña**, especifique las credenciales de la cuenta de MySQL.

      Importante
      Solo se realizará copia de seguridad de las bases de datos a los que pueda acceder la cuenta especificada.

   e. Haga clic en **Crear**.

   El sitio web aparece en la consola de Cyber Protect en **Dispositivos** > **Sitios web**.

Para cambiar la configuración de la conexión

1. Seleccione el sitio web en **Dispositivos** > **Sitios web**.
2. Haga clic en **Detalles**.
3. Haga clic en el icono de lápiz situado al lado del sitio web o en los parámetros de conexión de la base de datos.
4. Realice los cambios necesarios y luego haga clic en **Guardar**.

Pasos crear un plan de protección para sitios web

1. Seleccione uno o varios sitios web en **Dispositivos** > **Sitios web**.
2. Haga clic en **Proteger**.
3. [Opcional] Habilite la copia de seguridad de bases de datos.
   Si se seleccionan varios sitios web, la copia de seguridad de bases de datos se deshabilita de forma predeterminada.

© Acronis International GmbH, 2003-2025

4. [Opcional] Cambie las reglas de retención.
5. [Opcional] Habilite el cifrado de copias de seguridad.
6. [Opcional] Haga clic en el icono de engranaje para editar la opción **Nombre del archivo de la copia de seguridad**. Esto es conveniente en dos casos:
   - Si hizo una copia de seguridad de este sitio web con anterioridad y desea continuar con la secuencia de copias de seguridad existente
   - Si desea ver los nombres personalizados en la pestaña **Almacenamiento de la copia de seguridad**
7. Haga clic en **Aplicar**.

Puede editar, revocar y eliminar planes de protección de sitios web del mismo modo que en el caso de los equipos. Estas operaciones se describen en el apartado "Operaciones con los planes de protección".

Recuperación de un sitio web

Para recuperar un sitio web

1. Realice uno de los siguientes procedimientos:
   - En **Dispositivos** > **Sitios web**, seleccione el sitio web que desee recuperar y haga clic en **Recuperación**.

     Puede buscar los sitios web por el nombre. No se pueden usar caracteres comodín.
   - Si se eliminó el sitio web, selecciónelo de la sección **Copias de seguridad de aplicaciones en la nube** de la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

     Para recuperar un sitio web eliminado, debe añadir el sitio de destino como un dispositivo.
2. Seleccione el punto de recuperación.
3. Haga clic en **Recuperar** y luego seleccione lo que desea recuperar: **Todo el sitio web**, **Bases de datos** (si los hubiera) o **Archivos/carpetas**.

   Para asegurarse de que su sitio web está en buen estado, le recomendamos que recupere los archivos y las bases de datos, no importa el orden.
4. Dependiendo de su elección en el paso anterior, siga uno de los procedimientos descritos a continuación:

Cómo recuperar todo el sitio web

1. En **Recuperar en sitio web**, consulte o cambie el sitio web de destino.

   De manera predeterminada, se selecciona el sitio web original. Si no existe, debe seleccionar el sitio web de destino.
2. Seleccione si quiere recuperar los permisos para compartir de los elementos recuperados.
3. Haga clic en **Iniciar recuperación** y confirme la acción.

Para recuperar las base de datos

© Acronis International GmbH, 2003-2025

1. Seleccione las bases datos que desea recuperar.
2. Si desea descargar una base de datos como archivo, haga clic en **Descargar**, seleccione la ubicación donde desee guardar el archivo y haga clic en **Guardar**. De lo contrario, omita este paso.
3. Haga clic en **Recuperar**.
4. En **Recuperar en sitio web**, consulte o cambie el sitio web de destino.
   De manera predeterminada, se selecciona el sitio web original. Si no existe, debe seleccionar el sitio web de destino.
5. Haga clic en **Iniciar recuperación** y confirme la acción.

Para recuperar los archivos/carpetas del sitio web

1. Seleccione los archivos/carpetas que desee recuperar.
2. Si desea guardar un archivo, haga clic en **Descargar**, seleccione la ubicación donde desee guardar el archivo y haga clic en **Guardar**. De lo contrario, omita este paso.
3. Haga clic en **Recuperar**.
4. En **Recuperar en sitio web**, consulte o cambie el sitio web de destino.
   De manera predeterminada, se selecciona el sitio web original. Si no existe, debe seleccionar el sitio web de destino.
5. Seleccione si quiere recuperar los permisos para compartir de los elementos recuperados.
6. Haga clic en **Iniciar recuperación** y confirme la acción.

Protección de servidores de alojamiento web

Puede proteger servidores de alojamiento web basados en Linux que ejecuten paneles de control Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager. Los servidores que ejecutan paneles de control de alojamiento web desde otros proveedores están protegidos con cargas de trabajo regulares.

Cuotas

Los servidores que ejecutan paneles de control Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager se consideran servidores de alojamiento web. Cada servidor de alojamiento web del que se realice la copia de seguridad consume la cuota de **servidores de alojamiento web**. Si la cuota se deshabilita o se supera el uso por encima del límite para esta cuota, se generará un error de copia de seguridad o se asignará una cuota como sigue:

- En el caso de un servidor físico, se usará la cuota de **servidores**. Si la cuota se deshabilita o se supera el uso por encima del límite para esta cuota, se generará un error de copia de seguridad.
- En el caso de un servidor virtual, se usará la cuota de **Equipos virtuales**. Si la cuota se deshabilita o se supera el uso por encima del límite para esta cuota, se generará un error de copia de seguridad.

© Acronis International GmbH, 2003-2025

Integraciones para DirectAdmin, cPanel y Plesk

Los administradores de alojamiento web que usan DirectAdmin, Plesk o cPanel pueden integrar estos paneles de control al servicio de Cyber Protection para disponer de distintas funciones potentes, entre las que se incluyen:

- Copia de seguridad de todo el servidor de alojamiento web en el almacenamiento en la nube mediante la copia de seguridad a nivel de disco
- Recuperación de todo el servidor, incluidos todos los sitios web y las cuentas
- Recuperación granular y descarga de cuentas, sitios web, archivos individuales, buzones de correo y bases de datos
- Habilitación de revendedores y clientes para realizar una recuperación de autoservicio de sus propios datos

Para llevar a cabo la integración, debe usar una extensión de servicio de Cyber Protection. Para obtener información detallada, consulte las guías de integración correspondientes:

- Guía de integración de DirectAdmin
- Guía de integración de WHM y cPanel
- Guía de integración de Plesk

Operaciones especiales con equipos virtuales

Ejecución de un equipo virtual desde una copia de seguridad (Instant Restore)

Puede ejecutar un equipo virtual desde una copia de seguridad a nivel de disco que contenga un sistema operativo. Esta operación, también conocida como "restauración instantánea", le permite iniciar un servidor virtual en cuestión de segundos. Las unidades de disco virtual se emulan directamente desde la copia de seguridad y, por consiguiente, no consumen espacio en el almacén de datos (almacenamiento). El espacio de almacenamiento es necesario solo para mantener los cambios en las unidades de disco virtuales.

Le recomendamos que deje esta máquina virtual temporal funcionando durante un plazo máximo de tres días. Entonces puede eliminarlo por completo o convertirlo en un equipo virtual normal (finalizarlo) sin tiempo de inactividad.

Mientras exista el equipo virtual temporal, las reglas de retención no podrán aplicarse a la copia de seguridad que use dicho equipo. Las copias de seguridad del equipo original pueden seguir en ejecución.

© Acronis International GmbH, 2003-2025

Ejemplos de uso

- **Recuperación ante desastres**

  Coloque una copia de un equipo con error en línea de forma instantánea.
- **Prueba de una copia de seguridad**

  Ejecute el equipo desde la copia de seguridad y asegúrese de que el SO invitado y las aplicaciones huéspedes funcionan correctamente.
- **Acceso a los datos de la aplicación**

  Mientras el equipo está en ejecución, use las herramientas de gestión nativas de la aplicación para acceder y extraer los datos necesarios.

Requisitos previos

- Debe haber por lo menos un Agente para VMware o un Agente para Hyper-V registrado en el servicio de Cyber Protection.
- La copia de seguridad puede almacenarse en una carpeta de red o en una carpeta local del equipo en el que está instalado el Agente para VMware o el Agente para Hyper-V. Si selecciona una carpeta de red, debe ser accesible desde ese equipo. Un equipo virtual también se puede ejecutar desde una copia de seguridad almacenada en la cloud, pero el rendimiento será más lento porque la operación requiere una lectura intensa mediante accesos aleatorios de la copia de seguridad.
- La copia de seguridad debe contener un equipo completo o todos los volúmenes necesarios para que el sistema operativo se inicie.
- Pueden usarse las copias de seguridad tanto de los equipos físicos como de los virtuales. No pueden usarse las copias de seguridad de *contenedores* Virtuozzo.
- Las copias de seguridad que contienen volúmenes lógicos (LVM) de Linux deben crearse con Agente para VMware o Agente para Hyper-V. El equipo virtual debe ser del mismo tipo que el equipo original (ESXi o Hyper-V).

Ejecución del equipo

1. Realice uno de los siguientes procedimientos:
   - Seleccione un equipo incluido en la copia de seguridad, haga clic en **Recuperación** y luego seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.
2. Haga clic en **Ejecutar como equipo virtual**.

   El software selecciona automáticamente el servidor y otros parámetros necesarios.
3. [Opcional] Haga clic en **Equipo de destino** y, a continuación, cambie el tipo de equipo virtual (ESXi o Hyper-V), el servidor o el nombre del equipo virtual.
4. [Opcional] Haga clic en **Almacén de datos** para ESXi o **Ruta** para Hyper-V y, a continuación, seleccione el almacén de datos para el equipo virtual.

© Acronis International GmbH, 2003-2025

Los cambios realizados a los discos virtuales se acumulan durante la ejecución del equipo. Asegúrese de que el almacén de datos seleccionado tiene suficiente espacio libre. Si desea mantener los cambios al hacer que el equipo virtual sea permanente, seleccione un almacén de datos adecuado para ejecutar el equipo de producción.

5. [Opcional] Haga clic en **Configuración de equipo virtual** para modificar el tamaño de la memoria y las conexiones de red del equipo virtual.
6. [Opcional] Seleccione el estado de energía del equipo virtual (**Activado**/**Desactivado**).
7. Haga clic en **Ejecutar ahora**.

Como resultado, el equipo aparecerá en la interfaz web con uno de los siguientes iconos:  o 

. Los equipos virtuales de este tipo no se pueden seleccionar para hacer una copia de seguridad.

Nota
Puede llevar a cabo la operación Ejecutar como máquina virtual (Restauración instantánea) con las copias de seguridad de Microsoft Azure. Sin embargo, esta operación aumenta el tráfico de salida,.que se añadirá a la factura de su suscripción de Microsoft Azure. El tráfico de salida habitual de un equipo de Windows que se ejecuta desde una copia de seguridad de Microsoft Azure sería de unos 5 GB desde que se enciende la máquina virtual hasta que se inicia sesión.

Eliminación del equipo

Le recomendamos no eliminar ningún equipo virtual temporal directamente en vSphere/Hyper-V porque podrían originarse anomalías en la interfaz web. Además, la copia de seguridad desde la que se ejecutaba el equipo podría permanecer bloqueada por un tiempo (no puede eliminarse mediante reglas de retención).

Para eliminar un equipo virtual que se ejecuta desde una copia de seguridad

1. En la pestaña **Todos los dispositivos**, seleccione un equipo que se ejecute desde una copia de seguridad.
2. Haga clic en **Eliminar**.

El equipo se elimina de la interfaz web. También se elimina del inventario y del almacén de datos (almacenamiento) de vSphere o Hyper-V. Se perderán todos los cambios que se realicen a los datos durante la ejecución del equipo.

Finalización del equipo

Mientras un equipo virtual se ejecuta desde una copia de seguridad, el contenido de los discos virtuales se toma directamente de dicha copia de seguridad. Por tanto, el equipo se volverá inaccesible o incluso corrupto si se pierde la conexión a la ubicación de la copia de seguridad o al agente de protección.

© Acronis International GmbH, 2003-2025

Puede optar por hacer el equipo permanente, es decir, recuperar todos sus discos virtuales junto con los cambios que tuvieron lugar mientras se ejecutaba el equipo, en el almacén de datos que almacena dichos cambios. Este proceso se denomina "finalización".

La finalización se lleva a cabo sin tiempo de inactividad. El equipo virtual *no* se apagará durante la finalización.

La ubicación de los discos virtuales finales se define en los parámetros de la operación **Ejecutar como VM** (**Almacén de datos** para ESXi o **Ruta** para Hyper-V). Antes de completar la finalización, garantice que el espacio libre, las capacidades para compartir y el rendimiento de este almacén de datos son adecuados para ejecutar el equipo en la producción.

Nota
La finalización no es compatible con Hyper-V ejecutándose en Windows Server 2008/2008 R2 y Microsoft Hyper-V Server 2008/2008 R2 porque la API necesaria falta en estas versiones de Hyper-V.

Para finalizar un equipo que se ejecuta desde una copia de seguridad

1. En la pestaña **Todos los dispositivos**, seleccione un equipo que se ejecute desde una copia de seguridad.
2. Haga clic en **Finalizar**.
3. [Opcional] Especifique un nuevo nombre para el equipo.
4. [Opcional] Cambie el modo de aprovisionamiento del disco. El valor predeterminado es el de **Ligero**.
5. Haga clic en **Finalizar**.

El nombre del equipo cambia inmediatamente. El proceso de recuperación se muestra en la pestaña **Actividades**. Una vez completada la recuperación, el icono del equipo cambia al de un equipo virtual normal.

Lo que necesita saber sobre la finalización

Comparación entre la finalización y una recuperación estándar

El proceso de finalización es más lento que la recuperación estándar debido a estos motivos:

- Durante la finalización, el agente accede aleatoriamente a varias partes de la copia de seguridad. Al recuperar todo un equipo, el agente lee los datos de la copia de seguridad de forma secuencial.
- Si el equipo virtual se está ejecutando durante la finalización, el agente lee los datos de la copia de seguridad más a menudo para mantener ambos procesos al mismo tiempo. Durante una recuperación estándar, se detiene el equipo virtual.

Finalización de equipos en ejecución a partir de copias de seguridad en la nube

Debido al acceso intensivo a los datos de la copia de seguridad, la velocidad de finalización depende enormemente del ancho de banda de la conexión entre la ubicación de la copia de seguridad y el

© Acronis International GmbH, 2003-2025

agente. La finalización será más lenta para las copias de seguridad ubicadas en la nube que para aquellas locales. Si la conexión a Internet es muy lenta o inestable, la finalización de un equipo en ejecución desde una copia de seguridad en la nube puede generar errores. Si quiere realizar la finalización y puede elegir, le recomendamos que ejecute equipos virtuales desde copias de seguridad locales.

Nota
La velocidad de la finalización depende de si el agente está conectado a un host de VMware ESXi o vCenter, según se describe en el paso 3 de "Configuración del dispositivo virtual" (p. 138). La conexión a VMware vCenter puede ralentizar la operación de finalización debido a las características específicas de las API de VMware. Para acelerar la operación de finalización, utilice un agente para VMware independiente con el fin de ejecutar la operación **Ejecutar como VM** seguida de la finalización, en la que ese Agente se conectará a un host ESXi en lugar de un vCenter.

Trabajar en VMware vSphere

Esta sección describe operaciones que son específicas para entornos de VMware vSphere.

Replicación de equipos virtuales

La replicación solo está disponible para los equipos virtuales VMware ESXi.

Es el proceso de crear una copia exacta (réplica) de un equipo virtual y mantener luego la réplica sincronizada con el equipo original. Al replicar un equipo virtual crítico, siempre dispondrá de una copia del equipo en un estado "listo para comenzar".

La replicación se puede iniciar manualmente o según la planificación que especifique. La primera replicación es completa (se copia todo el equipo). Las siguientes replicaciones son incrementales y se realizan con Seguimiento de bloques modificados cuando esta opción está habilitada.

Diferencias entre la replicación y la copia de seguridad

A diferencia de las copias de seguridad, las réplicas solo conservan el último estado del equipo virtual. Una réplica consume espacio del almacén de datos, mientras que las copias de seguridad se pueden guardar en un almacenamiento más económico.

Sin embargo, encender una réplica es mucho más rápido que realizar una recuperación y más veloz que ejecutar un equipo virtual desde una copia de seguridad. Cuando se enciende, la réplica funciona más rápido que un equipo virtual que se ejecuta desde una copia de seguridad y no carga el Agente para VMware.

Ejemplos de uso

- **Replicar equipos virtuales en un sitio remoto**.
  La replicación permite hacer frente a los errores parciales o completos que surgen en centros de datos mediante la clonación de los equipos virtuales de un sitio primario a otro secundario. El sitio secundario suele encontrarse en una instalación remota que tiene poca probabilidad de

© Acronis International GmbH, 2003-2025

verse afectada por factores medioambientales o de infraestructura, entre otros, que podrían provocar fallos en el sitio primario.

- **Replicar equipos virtuales dentro de un solo sitio (de un servidor/almacén de datos a otro)**.

  La replicación in situ se puede usar en escenarios de alta disponibilidad y recuperación ante desastres.

Lo que se puede hacer con una réplica

- **Realizar pruebas en una réplica**

  La réplica se encenderá para la realización de las pruebas. Use vSphere Client u otras herramientas para comprobar si la réplica funciona correctamente. La replicación se suspende mientras se están realizando pruebas.
- **Conmutar por error a una réplica**

  La conmutación por error es una transición de la carga de trabajo del equipo virtual original a su réplica. La replicación se suspende mientras la conmutación por error está en marcha.
- **Hacer una copia de seguridad de la réplica**

  Tanto la copia de seguridad como la replicación requieren el acceso a los discos virtuales, por lo que afectan al rendimiento del servidor donde se ejecuta el equipo virtual. Si quiere disponer de la réplica de un equipo virtual y, además, de las copias de seguridad, pero no quiere someter el servidor de producción a una carga extra, replique el equipo en otro servidor y configure la replicación de las copias de seguridad.

Limitaciones

- Los siguientes tipos de equipos virtuales no se pueden replicar:
  - Equipos tolerantes a errores que se ejecutan en ESXi 5.5 y versiones anteriores.
  - Equipos que se ejecutan desde copias de seguridad.
  - Réplicas de equipos virtuales.
- Algunos cambios que se realizan en el hardware, como agregar una tarjeta de interfaz de red (NIC) al host ESXi o eliminar una NIC de él, tienen como resultado el cambio de los ID internos del host. Este cambio afecta a los planes de replicación de VM. Después de dicho cambio, deberá volver a crear los planes de replicación de VM en los que el host ESXi se haya seleccionado como fuente o destino. De lo contrario, los planes de replicación de VM no funcionarán correctamente.

Creación de un plan de replicación

Se debe crear un plan de replicación individual para cada equipo. No se puede aplicar un plan existente a otros equipos.

Para crear un plan de replicación

1. Seleccione un equipo virtual que quiera replicar.
2. Haga clic en **Replicación**.

© Acronis International GmbH, 2003-2025

El software muestra una nueva plantilla de plan de replicación.

3. [Opcional] Para modificar el nombre del plan de replicación, haga clic en el nombre predeterminado.
4. Haga clic en **Equipo de destino** y luego haga lo siguiente:
   a. Seleccione si desea crear una réplica nueva o utilizar una réplica existente del equipo original.
   b. Seleccione el servidor ESXi y especifique el nombre de la réplica nueva o seleccione una réplica existente.
      El nombre predeterminado de una réplica nueva es **[Nombre del equipo original]_replica**.
   c. Haga clic en **Aceptar**.
5. [Solo al replicar en un equipo nuevo] Haga clic en **Almacén de datos** y luego seleccione el almacén de datos para el equipo virtual.
6. [Opcional] Haga clic en **Planificación** para cambiar la planificación de la replicación.
   De forma predeterminada, la replicación se realiza a diario de lunes a viernes. Puede seleccionar la hora a la que la replicación se ejecutará.
   Si quiere cambiar la frecuencia con que se realiza la replicación, mueva el control deslizante y especifique la planificación.
   También puede hacer lo siguiente:
   - Fije el rango de fechas en el que la planificación tendrá efecto. Seleccione la casilla de verificación **Ejecutar el plan en un rango de fechas** y especifique el rango de fechas.
   - Deshabilite la planificación. En este caso, la replicación se puede iniciar manualmente.
7. [Opcional] Haga clic en el icono de engranaje para modificar las opciones de replicación.
8. Haga clic en **Aplicar**.
9. [Opcional] Para ejecutar el plan manualmente, haga clic en **Ejecutar ahora** en el panel del plan.

Al ejecutar un plan de replicación, la réplica del equipo virtual aparece en la lista **Todos los dispositivos** con el icono siguiente: 

Realización de pruebas en una réplica

Para preparar una réplica para la realización de pruebas

1. Seleccione la réplica que desea someter a prueba.
2. Haga clic en **Probar réplica**.
3. Haga clic en **Iniciar pruebas**.
4. Seleccione si desea conectar la réplica encendida a una red. De forma predeterminada, la réplica no se conectará a ninguna red.
5. [Opcional] Si elige conectar la réplica a la red, desactive la casilla de verificación **Detener equipo virtual original** para detener el equipo original antes de encender la réplica.
6. Haga clic en **Iniciar**.

Para detener las pruebas de una réplica

© Acronis International GmbH, 2003-2025

1. Seleccione una réplica en la que se estén realizando pruebas.
2. Haga clic en **Probar réplica**.
3. Haga clic en **Detener comprobación**.
4. Confirme su decisión.

Conmutación por error en una réplica

Para conmutar por error un equipo en una réplica

1. Seleccione la réplica donde quiera realizar la conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Conmutación por error**.
4. Seleccione si desea conectar la réplica encendida a una red. De forma predeterminada, la réplica se conectará a la misma red que el equipo original.
5. [Opcional] Si elige conectar la réplica a la red, desactive la casilla de verificación **Detener equipo virtual original** para mantener conectado el equipo original.
6. Haga clic en **Iniciar**.

Mientras la réplica está en un estado de conmutación por error, puede elegir una de las siguientes acciones:

- **Detener conmutación por error**
  Detenga la conmutación por error si el equipo original se ha arreglado. La réplica se apagará. Se reanudará la replicación.
- **Ejecutar conmutación por error permanente en la réplica**
  Esta operación instantánea elimina la marca "réplica" del equipo virtual para que ya no se pueda realizar ninguna replicación. Si quiere reanudar la replicación, edite el plan de replicación para seleccionar este equipo como origen.
- **Conmutación por recuperación**
  Realice una conmutación por recuperación si ejecutó una conmutación por error en el sitio que no está destinado a las operaciones continuas. La réplica se recuperará en el equipo original o en un equipo virtual nuevo. Cuando se completa la recuperación en el equipo original, se enciende y la replicación se reanuda. Si elige recuperar en un equipo nuevo, edite el plan de replicación para seleccionar este equipo como origen.

Detención de una conmutación por error

Para detener conmutación por error

1. Seleccione una réplica en estado de conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Detener conmutación por error**.
4. Confirme su decisión.

© Acronis International GmbH, 2003-2025

Ejecución de una conmutación por error permanente

Para ejecutar una conmutación por error permanente

1. Seleccione una réplica en estado de conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Conmutación por error permanente**.
4. [Opcional] Cambie el nombre del equipo virtual.
5. [Opcional] Active la casilla de verificación **Detener equipo virtual original**.
6. Haga clic en **Iniciar**.

Conmutación por recuperación

Para conmutar por recuperación desde una réplica

1. Seleccione una réplica en estado de conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Conmutación por recuperación desde la réplica**.
   El software selecciona automáticamente el equipo original como equipo de destino.
4. [Opcional] Haga clic en **Equipo de destino** y luego haga lo siguiente:
   a. Seleccione si desea realizar la conmutación por recuperación en un equipo nuevo o existente.
   b. Seleccione el servidor ESXi y especifique el nombre del equipo nuevo o seleccione un equipo existente.
   c. Haga clic en **Aceptar**.
5. [Opcional] Al realizar una conmutación por recuperación en un equipo nuevo, también puede hacer lo siguiente:
   - Haga clic en **Almacén de datos** para seleccionar el almacén de datos para el equipo virtual.
   - Haga clic en **Configuración de VM** para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red del equipo virtual.
6. [Opcional] Haga clic en **Opciones de recuperación** para modificar las opciones de conmutación por recuperación.
7. Haga clic en **Iniciar recuperación**.
8. Confirme su decisión.

Opciones de replicación

Para modificar las opciones de replicación, haga clic en el icono del engranaje que se encuentra al lado del nombre del plan de replicación y, a continuación, haga clic en **Opciones de replicación**.

© Acronis International GmbH, 2003-2025

Seguimiento de bloques modificados (CBT)

Esta opción se parece a la opción de copia de seguridad "Seguimiento de bloques modificados (CBT)".

Aprovisionamiento del disco

Esta opción define los ajustes de aprovisionamiento del disco para la réplica.

El valor predeterminado es el siguiente: **Disposición ligera**.

Los valores disponibles son los siguientes: **Disposición ligera**, **Disposición densa**, **Mantener la configuración original**.

Control de errores

Esta opción se parece a la opción de copia de seguridad "Control de errores".

Comandos previos/posteriores

Esta opción se parece a la opción de copia de seguridad "Comandos previos/posteriores".

Volume Shadow Copy Service VSS para equipos virtuales

Esta opción se parece a la opción de copia de seguridad "Volume Shadow Copy Service VSS para equipos virtuales".

Opciones de recuperación tras error

Para modificar las opciones de conmutación por recuperación, haga clic en **Opciones de recuperación** al configurar la conmutación por recuperación.

Control de errores

Esta opción se parece a la opción de recuperación "Control de errores".

Rendimiento

Esta opción se parece a la opción de recuperación "Rendimiento".

Comandos previos/posteriores

Esta opción se parece a la opción de recuperación "Comandos previos/posteriores".

Gestión de energía de VM

Esta opción se parece a la opción de recuperación "Gestión de energía del equipo virtual".

Recopilación de una réplica inicial

Para acelerar la replicación en una ubicación remota y ahorrar ancho de banda en la red, puede realizar recopilación de réplicas.

© Acronis International GmbH, 2003-2025

Importante
Para realizar la recopilación de réplicas, Agente para VMware (dispositivo virtual) debe ejecutarse en el ESXi de destino.

Para recopilar una réplica inicial

1. Realice uno de los siguientes procedimientos:
   - Si el equipo virtual original puede desconectarse, hágalo y luego vaya directamente al paso 4.
   - Si el equipo virtual original no se puede desconectar, continúe en el paso siguiente.
2. Cree un plan de replicación.
   Al crear el plan, en **Equipo de destino**, seleccione **Réplica nueva** y el ESXi que aloja el equipo original.
3. Ejecute el plan una vez.
   Se crea una réplica en el ESXi original.
4. Exporte los archivos del equipo virtual (o de la réplica) a un disco duro externo.
   a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
   b. Conecte vSphere Client al vCenter\ESXi original.
   c. Seleccione la réplica recién creada en el inventario.
   d. Haga clic en **Archivo** > **Exportar** > **Exportar plantilla de OVF**.
   e. En **Directorio**, especifique la carpeta del disco rígido externo.
   f. Haga clic en **Aceptar**.
5. Transfiera el disco duro a la ubicación remota.
6. Importe la réplica al ESXi de destino.
   a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
   b. Conecte vSphere Client al vCenter\ESXi de destino.
   c. Haga clic en **Archivo** > **Implementar plantilla de OVF**.
   d. En **Implementar desde un archivo o URL**, especifique la plantilla que exportó en el paso 4.
   e. Complete el procedimiento de importación.
7. Edite el plan de replicación que creó en el paso 2. En **Equipo de destino**, seleccione **Réplica existente** y, a continuación, seleccione la réplica importada.

Como resultado, el software continuará actualizando la réplica. Todas las replicaciones serán incrementales.

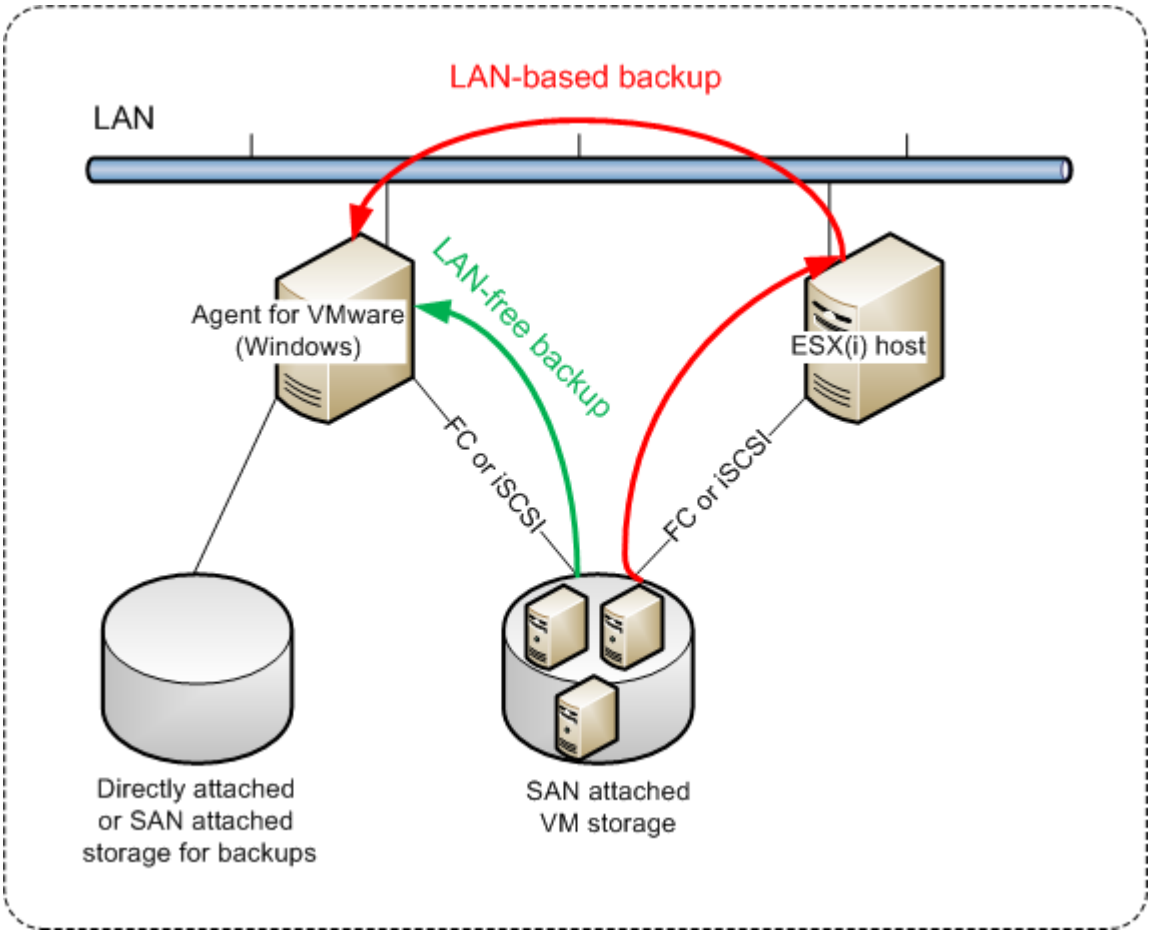
Agente para VMware: copia de seguridad sin LAN

Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el

© Acronis International GmbH, 2003-2025

almacenamiento en vez de mediante el servidor ESXi y LAN. Esta capacidad se llama copia de seguridad sin LAN.

El diagrama a continuación ilustra una copia de seguridad basada en LAN y sin LAN. El acceso sin LAN a los equipos virtuales está disponible si posee canal de fibra (FC) o red de área de almacenamiento iSCSI. Para eliminar completamente la transferencia de los datos incluidos en la copia de seguridad a través de la LAN, almacene las copias de seguridad en un disco local del equipo del agente o en un almacenamiento SAN conectado.



Para permitir que el agente acceda al almacén de datos directamente

1. Instale el Agente para VMware en un equipo que ejecute Windows y esté conectado a vCenter Server.
2. Conecte el número de unidad lógica (LUN) que aloja el almacén de datos en el equipo. Considere el siguiente escenario:
   - Use el mismo protocolo (iSCSI o FC) que se utiliza para la conexión del almacén de datos con el ESXi.
   - *No debe* iniciar el LUN y, además, debe mostrarse como disco "desconectado" en **Gestión del disco**. Si Windows inicia el LUN, este puede resultar dañado o ilegible en VMware vSphere.

© Acronis International GmbH, 2003-2025

Como resultado, el agente utilizará el modo de transporte SAN para acceder a los discos virtuales, es decir, leerá los sectores LUN sin procesar en iSCSI/FC sin reconocer el sistema de archivos VMFS, que Windows no detecta.

Limitaciones

- En vSphere 6.0 y versiones posteriores, el agente no puede utilizar el modo de transporte de SAN si algunos de los discos de equipo virtual están ubicados en un Volumen Virtual de VMware (VVol) y otros no. Las copias de seguridad de dichos equipos virtuales fallarán.
- Los equipos virtuales cifrados, presentados en VMware vSphere 6.5, se incluirán en la copia de seguridad mediante LAN, incluso si configura el modo de transporte SAN para el agente. El agente recurrirá al transporte NBD, pues VMware no es compatible con el transporte SAN para realizar copias de seguridad de discos virtuales cifrados.

Ejemplo

Si está utilizando un SAN de iSCSI, configure el iniciador de iSCSI en el equipo que ejecute Windows y en el que esté instalado Agente para VMware.

Para configurar la directiva SAN

1. Inicie sesión como administrador, ejecute el símbolo del sistema, escriba `diskpart` y, a continuación, pulse **Intro**.
2. Escriba `san`, y, a continuación, pulse **Intro**. Asegúrese de que se muestra la **Directiva SAN: Se muestran Todos los que están fuera de línea**.
3. Si se establece otro valor para la directiva SAN:
   a. Escriba `san policy=offlineall`.
   b. Pulse **Intro**.
   c. Para comprobar que la configuración se haya aplicado correctamente, siga el paso 2.
   d. Reinicie el equipo.

Para configurar un iniciador iSCSI

1. Vaya al **Panel de control** > **Herramientas administrativas** > **Iniciador de iSCSI**.

   Nota
   Para encontrar el applet **Herramientas administrativas**, es posible que necesite cambiar la vista del **Panel de control** a una diferente de **Inicio** o **Categoría**. También puede utilizar la búsqueda.

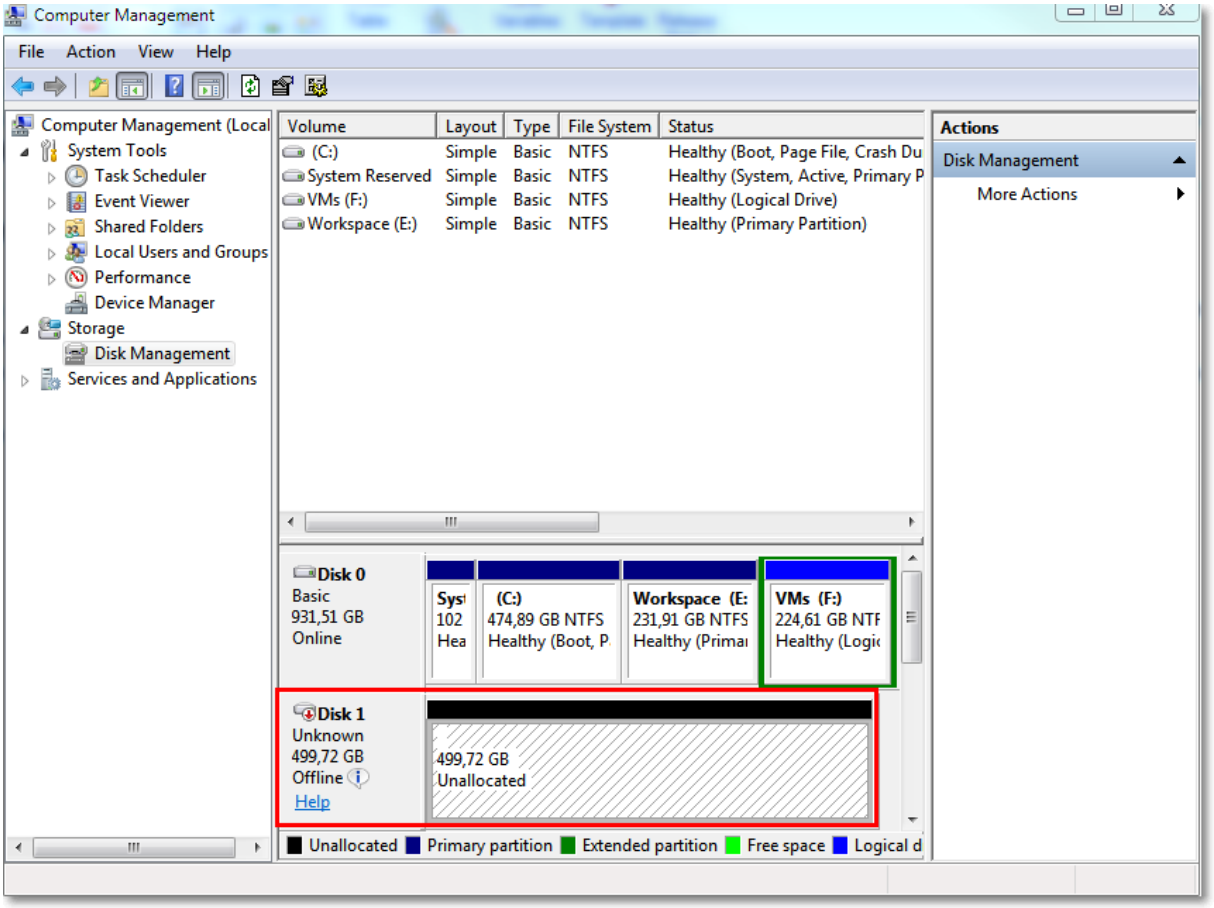
2. Si es la primera vez que ejecuta el iniciador de iSCSI, confirme que desea iniciar el servicio del iniciador de iSCSI de Microsoft.
3. En la pestaña **Destinos**, escriba el nombre de dominio completo (FQDN) o la dirección IP del dispositivo SAN de destino y, después, haga clic en **Conexión rápida**.
4. Seleccione el LUN que aloja el almacén de datos y, a continuación, haga clic en **Conectar**.

© Acronis International GmbH, 2003-2025

Si no se muestra el LUN, asegúrese de que la división en zonas en el objetivo de iSCSI permite al equipo que está ejecutando el agente acceder el LUN. Debe añadir el equipo a la lista de iniciadores de iSCSI permitidos en este destino.

5. Haga clic en **Aceptar**.

El SAN o LUN listo debería aparecer en **Gestión del disco**, tal y como se muestra en la captura de pantalla de abajo.



Utilización de almacenamiento conectado localmente

Con el Agente para VMware (dispositivo virtual) o el Agente para Scale Computing HC3, puede utilizar el almacenamiento conectado localmente para eliminar el tráfico de red entre el agente de protección y la ubicación de la copia de seguridad.

© Acronis International GmbH, 2003-2025

Importante
El almacenamiento conectado localmente (LAS) está diseñado para entornos pequeños con un único agente de protección (dispositivo virtual). Utilizar múltiples agentes de protección con almacenamiento conectado localmente en el mismo entorno puede resultar en copias de seguridad duplicadas, porque las máquinas virtuales se distribuyen aleatoriamente entre los agentes y cada agente utiliza su propio almacenamiento conectado localmente.

En entornos VMware, puede utilizar múltiples dispositivos virtuales si enlaza manualmente cada dispositivo virtual a todas las máquinas virtuales que este dispositivo respaldará. Para obtener más información, consulte "Enlace de equipos virtuales" (p. 966).

Nota
El tamaño de disco recomendado para el almacenamiento conectado localmente es de hasta 5 TB. Los discos más grandes también pueden funcionar, pero no se han probado tales configuraciones. Puede conectar discos más grandes bajo su propio riesgo.

Si necesita realizar copias de seguridad de más de 5 TB de datos, le recomendamos que utilice un tipo de almacenamiento diferente. Por ejemplo, puede adjuntar un disco virtual a una máquina virtual en el entorno y, a continuación, crear un recurso compartido de red en este disco. Luego, puede utilizar el recurso compartido de red como destino de las copias de seguridad, en lugar de utilizar almacenamiento conectado localmente.

Puede configurar el almacenamiento conectado localmente cuando despliega un dispositivo virtual o bien configurar el almacenamiento más tarde.

Para obtener más información sobre la configuración del almacenamiento local al desplegar un dispositivo virtual, consulte "Configuración del dispositivo virtual" (p. 138) (para VMware) y "Configuración del dispositivo virtual" (p. 143) (para Scale Computing).

Pasos para configurar el almacenamiento local después de desplegar un dispositivo virtual

1. En su entorno de máquina virtual, seleccione el dispositivo virtual y, a continuación, abra su configuración para ajustarla.
2. Agregue un nuevo disco duro al dispositivo virtual.
   La capacidad del disco debe ser de al menos 10 GB.

   Advertencia.
   Si utiliza un disco que contiene datos, se eliminarán los datos.
3. En su entorno de máquina virtual, abra la consola del dispositivo virtual.
4. En **Almacenamientos locales**, haga clic en **Actualizar**.
   Se activará el botón **Crear almacenamiento**.
5. Haga clic en **Crear almacenamiento** y, a continuación, seleccione el disco que agregó al dispositivo virtual.

© Acronis International GmbH, 2003-2025

- Seleccione una letra de unidad.
- [Opcional] Especifique una etiqueta de disco.
  La longitud de la etiqueta está limitada a 16 caracteres debido a las restricciones del sistema de archivos.

6. Haga clic en **Aceptar**.
7. Haga clic en **Sí**.

Pasos para seleccionar el almacenamiento conectado localmente como destino de copia de seguridad

- Cuando crea un plan de protección, en **Dónde guardar las copias de seguridad**, seleccione **Carpetas locales** y luego especifique la letra de unidad del almacenamiento conectado localmente. Por ejemplo, **D:**.

Enlace de equipos virtuales

Este tema describe cómo el servicio Cyber Protection organiza la operación de múltiples agentes dentro de VMware vCenter.

El algoritmo de distribución especificado a continuación funciona para dispositivos virtuales y agentes instalados en Windows.

Algoritmo de distribución

Los equipos virtuales están distribuidos uniformemente entre Agentes para VMware. Por uniformemente queremos decir que cada agente gestiona un número igual de equipos. La cantidad de espacio de almacenamiento ocupado por un equipo virtual no se cuenta.

Sin embargo, al escoger un agente para un equipo, el software intenta optimizar el rendimiento general del sistema. En particular, el software tiene en cuenta la ubicación del agente y el equipo virtual. Es preferible un agente alojado en el mismo servidor. Si no hay ningún agente en el mismo servidor, se prefiere un agente del mismo clúster.

Una vez que el equipo virtual se ha asignado a un agente, todas las copias de seguridad del equipo se delegarán a este agente.

Redistribución

La redistribución se realiza cada vez que se rompe el equilibrio establecido o, más precisamente, cuando el desequilibrio de cargas entre los agentes llega al 20 por ciento. Esto sucede cuando un equipo o un agente se añade o retira, o un equipo se migra a un servidor o clúster diferente, o si enlaza manualmente un equipo a un agente. Si ocurre esto, el servicio de Cyber Protection redistribuye los equipos utilizando el mismo algoritmo.

Por ejemplo, se da cuenta que necesita más agentes para ayudar al rendimiento y para implementar dispositivos virtuales adicionales en el clúster. El servicio de Cyber Protection asignará los equipos más adecuados al nuevo agente. La carga de los agentes anteriores se reducirá.

© Acronis International GmbH, 2003-2025

Cuando retira un agente del servicio Cyber Protection, los equipos asignados al agente se distribuyen entre los agentes restantes. Sin embargo, esto no sucederá si un agente se daña o elimina manualmente de vSphere. La redistribución comenzará solo después de eliminar dicho agente de la interfaz web.

Visualización del resultado de distribución

Puede ver el resultado de la distribución automática:

- en la columna **Agente** para cada equipo virtual en la sección **Todos los dispositivos**
- en la sección **Equipos virtuales asignados** del panel **Detalles** cuando un agente está seleccionado en la sección **Configuración** > **Agentes**

Enlace manual

El enlace de Agente para VMware le permite excluir un equipo virtual de este proceso de distribución al especificar el agente que siempre debe realizar la copia de seguridad de este equipo. Se continuará manteniendo el equilibrio general, pero este equipo concreto se puede pasar a un agente diferente solo si el agente original se elimina.

Para enlazar un equipo con un agente:

1. Seleccione el equipo.
2. Haga clic en **Detalles**.
   En la sección **Agente asignado**, el software muestra el agente que actualmente gestiona el equipo seleccionado.
3. Haga clic en **Modificar**.
4. Seleccione **Manual**.
5. Seleccione el agente al que desea enlazar el equipo.
6. Haga clic en **Guardar**.

Para desenlazar un equipo de un agente:

1. Seleccione el equipo.
2. Haga clic en **Detalles**.
   En la sección **Agente asignado**, el software muestra el agente que actualmente gestiona el equipo seleccionado.
3. Haga clic en **Modificar**.
4. Seleccione **Automático**.
5. Haga clic en **Guardar**.

Deshabilitar la asignación automática para un agente

Puede deshabilitar la asignación automática para Agente para VMware para excluirla del proceso de distribución especificando la lista de equipos de los que debe realizar la copia de seguridad este

© Acronis International GmbH, 2003-2025

agente. Se mantendrá el equilibrio general entre otros agentes.

La asignación automática no se puede deshabilitar para un agente si no hay otros agentes registrados o si una asignación automática está deshabilitada para el resto de agentes.

Para deshabilitar la asignación automática para un agente

1. Haga clic en **Configuración** > **Agentes**.
2. Seleccione Agente para VMware para el cual desea deshabilitar la asignación automática.
3. Haga clic en **Detalles**.
4. Deshabilite el conmutador **Asignación automática**.

Ejemplos de uso

- El enlace manual es práctico si desea que Agente para VMware (Windows) realice la copia de seguridad de un equipo (muy grande) en particular a través del canal de fibra, mientras que los dispositivos virtuales realicen la copia de seguridad de los demás equipos.
- Es necesario enlazar las máquinas virtuales a un agente si el agente utiliza almacenamiento conectado localmente.
- Deshabilitando la asignación automática es posible asegurarse de que previsiblemente la copia de seguridad de un equipo virtual se realiza según la planificación especificada. El agente que solo realiza la copia de seguridad de un VM no puede estar ocupado con la copia de seguridad de otros VM cuando llega la hora planificada.
- Deshabilitar la asignación automática es útil si existen varios servidores ESXi que están geográficamente separados. Si se deshabilita la asignación automática y luego se enlazan los VM de cada servidor al agente que se ejecuta en el mismo servidor, se puede garantizar que el agente nunca realizará copias de seguridad de ningún equipo que se ejecute en servidores ESXi remotos, lo que ahorra tráfico en la red.

Ejecución de comandos anteriores y posteriores a la instantánea automáticamente

Con herramientas de VMware, puede ejecutar automáticamente los comandos anteriores y posteriores a la instantánea que haya personalizado en las máquinas virtuales de las que realizó la copia de seguridad en el modo sin agente. De este modo, por ejemplo, puede ejecutar comandos inactivos personalizados y crear copias de seguridad consistentes con las aplicaciones para las máquinas virtuales que ejecutan aplicaciones que no son compatibles con VSS.

Requisitos previos

Los comandos anteriores y posteriores a la instantánea deben ubicarse en una carpeta específica de la máquina virtual.

- Para las máquinas virtuales de Windows, la ubicación de esta carpeta depende de la versión ESXi del host.

© Acronis International GmbH, 2003-2025

Por ejemplo, para las máquinas virtuales que funcionan en un host ESXi 6.5, esta carpeta es `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. Debe crear la carpeta `backupScritps.d` manualmente. No almacene otros tipos de archivos en esta carpeta, ya que esto puede hacer que VMware Tools se vuelva inestable.

Para obtener más información acerca de la ubicación de los comandos anteriores y posteriores a la instantánea para otras versiones ESXi, consulte la documentación de VMware.

- Para las máquinas virtuales de Linux, copia sus comandos en los directorios `/usr/sbin/pre-freeze-script` y `/usr/sbin/post-thaw-script`, respectivamente. Los comandos en `/usr/sbin/pre-freeze-script` se ejecutan al crear una instantánea y los que están en `/usr/sbin/post-thaw-script` se ejecutan cuando la instantánea ha terminado. El usuario de herramientas de VMware debe poder ejecutar los comandos.

Para ejecutar comandos anteriores y posteriores a la instantánea automáticamente

1. Asegúrese de que las herramientas de VMware están instaladas en la máquina virtual.
2. En la máquina virtual, coloque sus comandos personalizados en la carpeta correspondiente.
3. En el plan de protección de esta máquina, habilite la opción **Servicio de instantáneas de volumen (VSS) para equipos virtuales**.

   Así se crea una instantánea de VMware con la opción **Inmovilizar el sistema de archivos invitado** habilitada, que a su vez activa los comandos anteriores y posteriores a la instantánea en la máquina virtual.

No es necesario que ejecute comandos de inmovilización personalizados en máquinas virtuales que ejecuten aplicaciones compatibles con VSS, como Microsoft SQL Server o Microsoft Exchange. Para crear una copia de seguridad consistente con la aplicación para esas máquinas, habilite la opción **Servicio de instantáneas de volumen (VSS) para equipos virtuales** en el plan de protección.

Soporte técnico para la migración de máquinas virtuales

Este apartado contiene información sobre la migración de máquinas virtuales dentro de un entorno de vSphere, incluido cuando migran entre hosts ESXi que forman parte de un clúster vSphere.

vMotion permite mover el estado y la configuración de una máquina virtual a otro servidor mientras el disco del equipo continua estando en la misma ubicación en un almacenamiento compartido. Storage vMotion permite mover los discos de una máquina virtual de un almacenamiento de datos a otro.

- La migración con vMotion, incluido Storage vMotion, no es compatible con una máquina virtual que ejecute el agente para VMware (dispositivo virtual) y debe deshabilitarse después de la implementación del aparato. Debe agregar esta máquina virtual a la lista de anulaciones de VM en la configuración del clúster de vSphere para evitar la migración de la máquina virtual del aparato a través de los nodos del clúster de vSphere.
- Cuando se inicia la copia de seguridad de una máquina virtual, la migración con vMotion, que incluye Storage vMotion, se deshabilita automáticamente. Esta máquina virtual se añade temporalmente a la lista **Anulaciones de máquinas virtuales** de la configuración del clúster de

© Acronis International GmbH, 2003-2025

vSphere. Cuando la copia de seguridad termina, la configuración de las **Anulaciones de máquinas virtuales** se revierte automáticamente a su estado anterior.

- No se puede iniciar una copia de seguridad de una máquina virtual mientras su migración con vMotion, que incluye Storage vMotion, está en progreso. La copia de seguridad de esta máquina se iniciará cuando acabe su migración.

Protección de entornos de virtualización

En la consola de Cyber Protect, puede ver los entornos de vSphere, Hyper-V y Virtuozzo en su presentación nativa. Después de instalar y registrar el agente correspondiente, la pestaña **VMware**, **Hyper-V** o **Virtuozzo** aparece bajo **Dispositivos**.

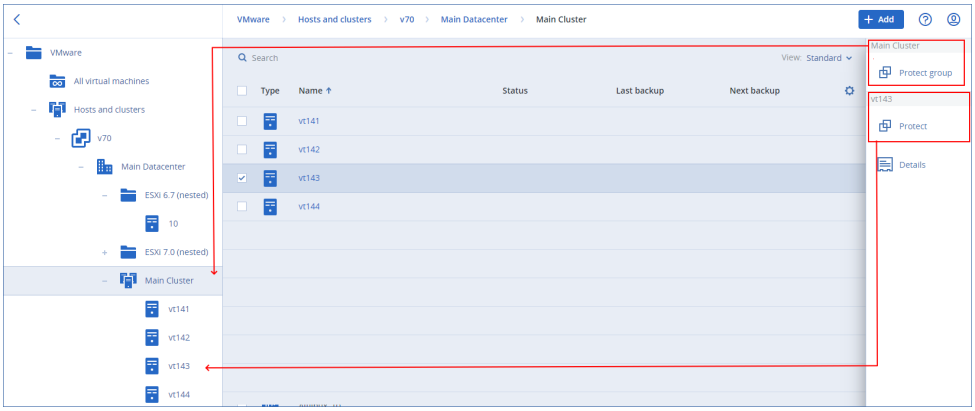
Por ejemplo, en la pestaña de **VMware**, puede hacer una copia de seguridad de los siguientes objetos de infraestructura de vSphere:

- vCenter
- Centro de datos
- Carpeta
- Clúster
- Servidor ESXi
- Grupo de recursos
- Equipo virtual

Para aplicar un plan a un objeto de infraestructura seleccionado, haga clic en **Proteger**. Se hará una copia de seguridad de todos los objetos secundarios.

Para aplicar un plan al objeto primario del objeto de infraestructura seleccionado, haga clic en **Proteger grupo**. Se hará una copia de seguridad de todos los objetos secundarios del objeto primario.

Por ejemplo, si aplica un plan a un host ESXi, se hará una copia de seguridad de todas las máquinas virtuales del host. Si aplica un plan al clúster primario, se hará una copia de seguridad de todas las máquinas virtuales de todos los hosts de este clúster.



© Acronis International GmbH, 2003-2025

Visualización del estado de la copia de seguridad en vSphere Client

Puede ver el estado de la copia de seguridad y el momento en el que se llevó a cabo la última copia de seguridad de un equipo virtual en vSphere Client.

Esta información aparece en el resumen del equipo virtual (**Resumen** > **Atributos personalizados**/**Anotaciones**/**Notas**, según el tipo de cliente y la versión de vSphere). También puede habilitar las columnas **Última copia de seguridad** y **Estado de la copia de seguridad** en la pestaña **Equipos virtuales** para cualquier host, centro de datos, carpeta, pool de recursos o todo el vCenter Server.

Para proporcionar estos atributos, el Agente para VMware debe tener los siguientes privilegios, además de los descritos en "Agente para VMware: privilegios necesarios":

- **Global** > **Gestionar atributos personalizados**
- **Global** > **Establecer atributos personalizados**

Privilegios necesarios para el agente para VMware

Nota
Para habilitar las copias de seguridad de las máquinas virtuales, instale las APIs de vStorage en el host ESXi. Para obtener más información, consulte este artículo de la base de conocimientos.

El agente para VMware se autentica en vCenter o el host ESXi mediante una cuenta de usuario que se especifica durante la implementación del agente. La cuenta de usuario debe tener un rol que incluya los privilegios enumerados en la tabla a continuación. Recomendamos que utilice una cuenta y un rol dedicados, en lugar de usar una cuenta existente que tenga el rol de administrador.

La cuenta de usuario debe tener permiso para acceder a todos los niveles de la infraestructura de vSphere, como vCenter, centros de datos, clústeres, hosts ESXi, grupos de recursos y máquinas virtuales. Para aprender cómo añadir un permiso en el nivel de vCenter y propagarlo a los otros niveles, consulte "Concesión de permiso de acceso a la cuenta de usuario" (p. 977).

Puede cambiar la cuenta de usuario que utiliza el agente para VMware sin tener que volver a desplegar el agente. Para aprender cómo se cambia la cuenta, consulte "Cambio de la cuenta de usuario para agente para VMware" (p. 978).

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
Operaciones					

© Acronis International GmbH, 2003-2025

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
criptográficas (primeros pasos con vSphere 6.5)					
	Agregar disco	+*			
	Acceso directo	+*			
Almacén de datos					
	Asignar espacio		+	+	+
	Examinar almacén de datos				+
	Configurar los almacenes de datos	+	+	+	+
	Operaciones con archivos de bajo nivel				+
Global					
	Deshabilitar métodos	+	+	+	
	Habilitar métodos	+	+	+	
	Licencias	+	+	+	+
	Gestionar atributos personalizados	+	+	+	
	Establecer atributo personalizado	+	+	+	

© Acronis International GmbH, 2003-2025

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
Servidor > Configuración					
	Configuración de partición de almacenamiento				+
	Modificar clúster				
Servidor > Operaciones locales					
	Crear máquina virtual				+
	Eliminar máquina virtual				+
	Reconfigurar máquina virtual				+
Red					
	Asignar red		+	+	+
Recurso					
	Asignar máquina virtual al grupo de recursos		+	+	+
Máquina virtual > Cambiar configuración					
	Adquirir	+		+	

© Acronis International GmbH, 2003-2025

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
	arrendamiento de disco				
	Añadir disco existente	+	+		+
	Añadir disco nuevo		+	+	+
	Añadir o quitar dispositivo		+		+
	Configuración avanzada	+	+	+	
	Cambiar recuento de CPU		+		
	Cambiar memoria		+		
	Cambiar configuración		+	+	+
	Cambiar recurso	+	+		
	Modificar la configuración del dispositivo	+	+		
	Quitar disco	+	+	+	+
	Cambiar nombre		+		
	Establecer anotación				+
	Activar seguimiento de cambio de disco	+		+	

© Acronis International GmbH, 2003-2025

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
Máquina virtual > **Operaciones de invitado**					
	Modificaciones de operación de invitado	+**			
	Ejecución del programa de operación de invitado	+**			
	Consultas de operación de invitado	+**			
Máquina virtual > **Interacción**					
	Adquirir vale de control de huésped (en vSphere 4.1 y 5.0)				+
	Configurar dispositivo de CD		+	+	
	Gestión del sistema operativo huésped por VIX API (en vSphere 5.1 y versiones posteriores)				+
	Apagar			+	+
	Encender		+	+	+

© Acronis International GmbH, 2003-2025

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
Máquina virtual > **Inventario**					
	Crear desde existente		+	+	+
	Crear nuevo		+	+	+
	Registrar				+
	Eliminar		+	+	+
	Anular el registro				+
Máquina virtual > **Aprovisionamiento**					
	Permitir acceso a disco		+	+	+
	Permitir acceso a disco de solo lectura	+		+	
	Permitir descarga de equipo virtual	+	+	+	+
Máquina virtual > **Estado** **Máquina virtual** > **Gestión de instantáneas** (vSphere 6.5 y versiones posteriores)					
	Crear instantánea	+		+	+

© Acronis International GmbH, 2003-2025

Objeto	Privilegio	Operación			
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad
	Eliminar instantánea	+		+	+
vApp					
	Agregar equipo virtual				+

* Este privilegio solo es necesario para hacer copias de seguridad de máquinas cifradas.

** Este privilegio solo es necesario para las copias de seguridad con información de aplicaciones.

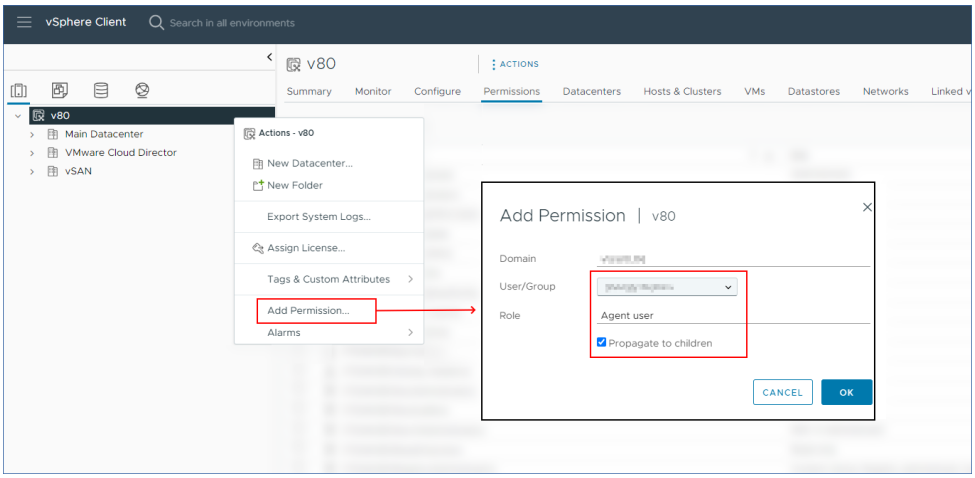
Concesión de permiso de acceso a la cuenta de usuario

La cuenta de usuario que utiliza el agente para VMware debe tener acceso a todos los niveles de la infraestructura de vSphere, como vCenter, centros de datos, clústeres, hosts ESXi, pools de recursos y máquinas virtuales.

Para conceder permiso de acceso a la cuenta de usuario

1. En vSphere Client, vaya a **Inventario**.
2. Haga clic con el botón derecho en el objeto **vCenter** al que desea conceder permiso, y luego haga clic en **Añadir permiso**.
3. En el diálogo **Añadir permiso**, seleccione una cuenta de usuario y un rol.
   El rol debe incluir los privilegios que se enumeran en "Privilegios necesarios para el agente para VMware" (p. 971).
4. Seleccione la casilla de verificación **Propagar a secundarios**.
5. Haga clic en **Aceptar**.

© Acronis International GmbH, 2003-2025



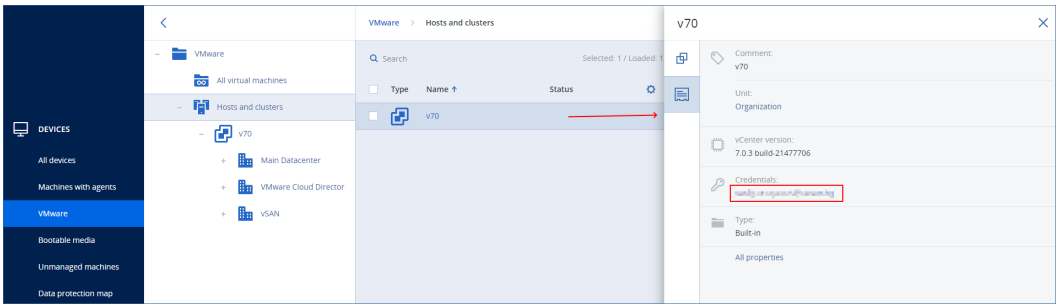
Cambio de la cuenta de usuario para agente para VMware

En la consola de Cyber Protect, puede cambiar la cuenta de usuario para un agente particular, o para todos los agentes, en vCenter o un host ESXi.

Para cambiar la cuenta de usuario para el agente para VMware

Para todos los agentes

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **VMware**.
2. Haga clic en **Servidores y clústeres**.
3. En el panel principal, haga clic en el espacio vacío junto al nombre de vCenter o el host ESXi independiente.
4. En el panel derecho, haga clic en **Detalles**.
5. Bajo **Credenciales**, haga clic en la cuenta de usuario.



6. Especifique la nueva cuenta de usuario y la contraseña para esa cuenta.
7. Haga clic en **Aceptar**.

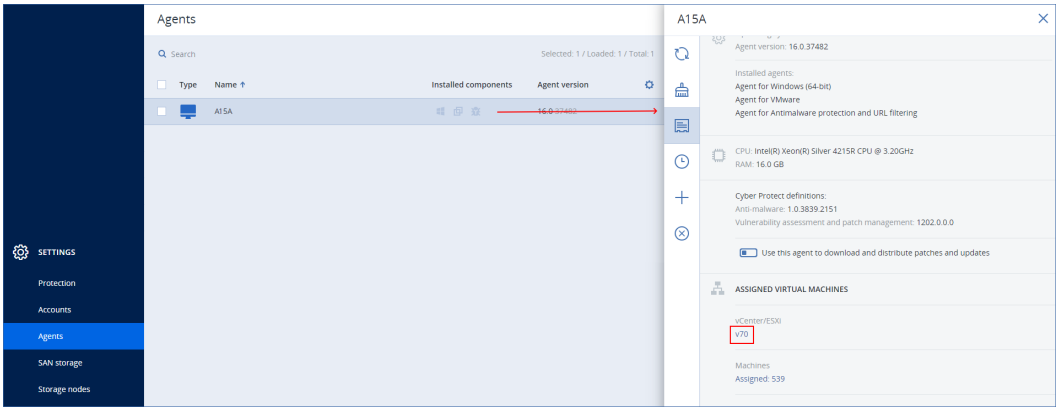
Como resultado, todos los agentes en este vCenter o host ESXi utilizarán la nueva cuenta de usuario.

Para un agente particular

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione el agente.

© Acronis International GmbH, 2003-2025

3. En el panel derecho, haga clic en **Detalles**.
4. En **Equipos virtuales asignados**, haga clic en el nombre de vCenter/ESXi.



5. En la pantalla de **Añadir VMware vCenter o host ESXi**, especifique la nueva cuenta de usuario y la contraseña para esa cuenta.
6. Haga clic en **Configurar**.

Copia de seguridad de equipos Hyper-V en clúster

En un clúster Hyper-V, los equipos virtuales pueden migrarse entre los nodos del clúster. Siga estas recomendaciones para configurar una copia de seguridad correcta de equipos Hyper-V en clúster:

1. Un equipo debe estar disponible para la copia de seguridad sin importar a qué nodo se migra. Para garantizar que el Agente para Hyper-V tenga acceso a un equipo en cualquier nodo, ejecute el servicio de agente en una cuenta de usuario del dominio que posea privilegios administrativos en cada uno de los nodos de clúster.

   Le recomendamos que especifique dicha cuenta para el servicio del agente durante la instalación de Agente para Hyper-V.
2. Instale Agente para Hyper-V en cada nodo del clúster.
3. Registre todos los agentes en el servicio Cyber Protection.

Alta disponibilidad de un equipo recuperado

Cuando recupera discos con copias de seguridad en un equipo virtual Hyper-V *existente*, la propiedad de alta disponibilidad del equipo se mantiene como está.

Cuando recupera discos con copias de seguridad en un equipo virtual Hyper-V *nuevo*, el equipo no tiene alta disponibilidad. Se considera un equipo de reserva y normalmente está apagado. Si necesita usar el equipo en el entorno de producción, puede configurarlo para que tenga alta disponibilidad desde el complemento **Administración del clúster de conmutación por error**.

© Acronis International GmbH, 2003-2025

Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo

En la opción de copia de seguridad **Programación**, puede limitar el número de máquinas virtuales por plan de protección de las que se ha hecho una copia de seguridad simultáneamente.

Cuando un agente ejecuta varios planes al mismo tiempo, el número de máquinas con copia de seguridad simultánea aumenta. Esto podría afectar al rendimiento de copia de seguridad y sobrecargar el host y el almacenamiento de la máquina virtual. Puede evitar esos problemas mediante la configuración de un límite en el nivel del agente.

Pasos para limitar el número de copias de seguridad simultáneas en el nivel del agente

Agente para VMware (Windows)

1. En el equipo con el agente, cree un nuevo documento de texto y ábralo en un editor de texto.
2. Copie y pegue las siguientes líneas en el archivo.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Reemplace `00000001` por el valor hexadecimal del límite que desee establecer.
   Por ejemplo, `00000001` es 1 y `0000000A` es 10.
4. Guarde el documento como **limit.reg**.
5. Ejecute el archivo como administrador.
6. Confirme que desea editar el registro de Windows.
7. Reinicie el agente:
   a. En el menú **Inicio**, haga clic en **Ejecutar**.
   b. Escriba **cmd** y, a continuación, haga clic en **Aceptar**.
   c. En la línea de comandos, ejecute los siguientes comandos:

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

Agente para Hyper-V

1. En el equipo con el agente, cree un nuevo documento de texto y ábralo en un editor de texto.
2. Copie y pegue las siguientes líneas en el archivo.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
```


© Acronis International GmbH, 2003-2025

```
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Reemplace `00000001` por el valor hexadecimal del límite que desee establecer.
   Por ejemplo, `00000001` es 1 y `0000000A` es 10.
4. Guarde el documento como **limit.reg**.
5. Ejecute el archivo como administrador.
6. Confirme que desea editar el registro de Windows.
7. Reinicie el agente:
   a. En el menú **Inicio**, haga clic en **Ejecutar**.
   b. Escriba **cmd** y, a continuación, haga clic en **Aceptar**.
   c. En la línea de comandos, ejecute los siguientes comandos:

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

Dispositivos virtuales

Este procedimiento se aplica a dispositivos virtuales, como Agente para VMware (dispositivo virtual), Agente para Scale Computing, Agente para Virtuozzo Hybrid Infrastructure, Agente para oVirt y Agente para Nutanix.

1. En la consola del dispositivo virtual, presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
2. Abra el archivo `/etc/Acronis/MMS.config` en un editor de texto.
3. Busque la siguiente sección:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Reemplace `10` por el número máximo de copias de seguridad simultáneas que desee establecer.
5. Guarde el archivo.
6. Reinicie el agente con el comando `reboot`.

Agentes empaquetados con Agente para Linux

Este procedimiento se aplica a agentes que están empaquetados con Agente para Linux, como Agente para Proxmox y Agente para Virtuozzo.

1. Inicie sesión como usuario raíz en el equipo con el agente.
   Utilice la contraseña que usó para acceder a la consola de Cyber Protect.
2. Abra el archivo `/etc/Acronis/MMS.config` en un editor de texto.
3. Busque la siguiente sección:

© Acronis International GmbH, 2003-2025

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Reemplace `10` por el número máximo de copias de seguridad paralelas que desee establecer.
5. Guarde el archivo.
6. Ejecute el siguiente comando para reiniciar el agente:

```
sudo service acronis_mms restart
```

Copia de seguridad basada en agente de máquinas virtuales de Microsoft Azure y Amazon EC2

Importante
Siga los procedimientos de esta sección para realizar copias de seguridad y recuperar máquinas virtuales de Azure si no utiliza el Agente para Azure.

Si utiliza el Agente para Azure, puede recuperar una copia de seguridad de **Todo el equipo** directamente como una máquina virtual. Para obtener más información, consulte "Recuperación de equipos físicos" (p. 663) y "Recuperación del equipos virtuales" (p. 678).

Copias de seguridad de equipos de Microsoft Azure y Amazon EC2

Importante
Siga este procedimiento para las máquinas virtuales de Microsoft Azure si no utiliza Agente para Azure.

Si utiliza el Agente para Azure, puede recuperar una copia de seguridad de **Todo el equipo** directamente como una máquina virtual. Para obtener más información, consulte "Recuperación de equipos físicos" (p. 663) y "Recuperación del equipos virtuales" (p. 678).

Pasos para realizar la copia de seguridad de máquinas virtuales de Microsoft Azure o Amazon EC2

1. Instale un agente de protección en el equipo del que quiera realizar una copia de seguridad.
2. Configure y ejecute un plan de protección como se describe en "Copia de seguridad" (p. 533).

Las operaciones de copia de seguridad y recuperación son las mismas que las operaciones para un equipo físico. Sin embargo, el equipo del que se ha realizado la copia de seguridad se contará como virtual cuando establezca las cuotas para el número de equipos.

A diferencia de los equipos físicos, no puede arrancar las máquinas virtuales de Microsoft Azure y Amazon EC2 desde un dispositivo de arranque.

© Acronis International GmbH, 2003-2025

Recuperación Máquinas equipos de Microsoft Azure y Amazon EC2

Importante
Siga este procedimiento para las máquinas virtuales de Microsoft Azure si no utiliza Agente para Azure.

Si utiliza el Agente para Azure, puede recuperar una copia de seguridad de **Todo el equipo** directamente como una máquina virtual. Para obtener más información, consulte "Recuperación de equipos físicos" (p. 663) y "Recuperación del equipos virtuales" (p. 678).

Pasos para recuperar un equipo como una nueva máquina virtual de Microsoft Azure o Amazon EC2

1. Cree una máquina virtual nueva desde una imagen o plantilla en Microsoft Azure o Amazon EC2.
   El equipo nuevo debe tener la misma configuración de disco que el equipo que desea recuperar.
2. En el nuevo equipo, instale el Agente para Windows o el Agente para Linux.
3. Recupere el equipo objeto de la copia de seguridad tal y como se ha descrito en "Recuperación de equipos físicos" (p. 663).
   Cuando configure la recuperación, seleccione el equipo nuevo como el equipo de destino.

Nota
Para máquinas virtuales de Microsoft Azure, este procedimiento de recuperación se aplica solo a las copias de seguridad de máquinas que contienen todos los controladores necesarios para ejecutarse en Azure de forma nativa (copias de seguridad de máquinas virtuales de Azure, equipos Hyper-V locales o equipos que ejecutan Windows Server 2016 o versiones posteriores). Para la recuperación multiplataforma, consulte este artículo de la base de conocimientos.

Creación de soportes de arranque para recuperar sistemas operativos

Los soportes de arranque son un CD, DVD, una unidad flash USB u otro dispositivo extraíble que permite ejecutar el agente de protección tanto en un entorno basado en Linux como en un entorno de preinstalación o recuperación de Windows (WinPE/WinRE) sin la ayuda de un sistema operativo. El objetivo principal del dispositivo de inicio es recuperar un sistema operativo que no se pueda iniciar.

Nota
El dispositivo de arranque no es compatible con unidades híbridas.

¿Un dispositivo de arranque personalizado o uno disponible?

Con Bootable Media Builder, puede crear su dispositivo de arranque personalizado (basado en Linux o en WinPE) para ordenadores Windows, Linux o macOS. Puede configurar ajustes

© Acronis International GmbH, 2003-2025

adicionales, como el registro automático, ajustes de red o ajustes de servidor proxy, tanto en los dispositivos de arranque personalizados basados en Linux como en WinPE/WinRE. En el dispositivo de arranque personalizado basado en WinPE/WinRE, también puede añadir controladores adicionales.

De manera alternativa, puede descargar un dispositivo de arranque disponible (solo los basados en Linux). El dispositivo de arranque disponible se usará para operaciones de recuperación y para acceder a la función Universal Restore.

¿Dispositivos de arranque basados en Linux o en WinPE/WinRE?

Basado en Linux

Los soportes de arranque basados en Linux contienen un agente de protección basado en un kernel Linux. El agente puede iniciar y realizar las operaciones en cualquier hardware compatible con PC, incluyendo desde cero y las máquinas con sistemas de archivos dañados o incompatibles.

Basados en WinPE/WinRE

El soporte de arranque basado en WinPE contiene un sistema Windows mínimo llamado entorno de preinstalación de Windows (WinPE) y un complemento de Cyber Protection para WinPE, que es una modificación del agente de protección que puede ejecutarse en el entorno de preinstalación. El dispositivo de arranque basado en WinRE utiliza el entorno de recuperación de Windows y no requiere la instalación de paquetes de Windows adicionales.

Se comprobó que WinPE es la solución de arranque más conveniente en entornos grandes con hardware heterogéneo.

Ventajas:

- El uso de Cyber Protection con el entorno de preinstalación de Windows proporciona más funcionalidad que el uso de dispositivos de arranque basados en Linux. Como se inició un hardware compatible con PC en WinPE, no solo puede utilizar el agente de protección, sino también los comandos, secuencias y otros complementos de PE que haya agregado.
- Los dispositivos de arranque basados en PE ayudan a superar los problemas de los dispositivos de arranque basados en Linux compatibles con ciertos controladores RAID de ciertos niveles de conjuntos de RAID solos. Los medios basados en WinPE 2.x y versiones posteriores permiten la carga dinámica de los controladores de dispositivos necesarios.

Limitaciones:

- Los medios de arranque basados en versiones de WinPE anteriores a la versión 4.0 no pueden iniciarse en equipos con la interfaz Unified Extensible Firmware Interface (UEFI).

Creación de un dispositivo de arranque físico

Recomendamos especialmente que cree y compruebe el dispositivo de arranque en cuanto empiece a usar copias de seguridad a nivel de discos. Además, es conveniente volver a crear el

© Acronis International GmbH, 2003-2025

dispositivo después de cada actualización importante del agente de protección.

Puede recuperar tanto Windows como Linux con el mismo dispositivo. Para recuperar macOS, cree un dispositivo independiente en un equipo que ejecute macOS.

Para crear dispositivos de arranque físicos en Windows o Linux

1. Cree un archivo ISO de dispositivo de arranque personalizado o descargue uno listo.
   Para crear un archivo ISO personalizado, utilice "Bootable Media Builder" (p. 985).
   Para descargar el archivo ISO listo, en la consola de Cyber Protect, seleccione un equipo y haga clic en **Recuperar** > **Otros métodos de recuperación...** > **Descargar la imagen ISO**.
2. [Opcional] En la consola de Cyber Protect, genere un token de registro. El token de registro se mostrará automáticamente cuando descargue un archivo ISO listo.
   Este token permite al dispositivo de arranque acceder al almacenamiento en la nube sin introducir un nombre de inicio de sesión y una contraseña.
3. Cree dispositivos de arranque físicos de las siguientes maneras:
   - Grabe el archivo ISO en un CD/DVD.
   - Cree una unidad flash USB de arranque utilizando el archivo ISO y una de las muchas herramientas gratuitas disponibles en línea.
     Para iniciar una máquina UEFI use `ISO a USB` o `RUFUS` y para una máquina BIOS, use `Win32DiskImager`. En Linux, puede usar la utilidad `dd`.

   En las máquinas virtuales, puede conectar el archivo ISO como una unidad de CD/DVD a la máquina que desea recuperar.

Para crear un dispositivo de arranque físico en macOS

1. En un equipo donde esté instalado Agente para Mac, haga clic en **Aplicaciones** > **Generador de Medios de rescate**.
2. El software muestra los dispositivos extraíbles conectados. Seleccione el que desee convertir en un dispositivo de inicio.

   Advertencia.
   Toda la información del disco se borrará.

3. Haga clic en **Crear**.
4. Espere mientras el software crea el dispositivo de inicio.

Bootable Media Builder

Bootable Media Builder es una herramienta dedicada para la creación de dispositivos de arranque. Se instala como un componente opcional en el equipo en el que está instalado el agente de protección.

© Acronis International GmbH, 2003-2025

¿Por qué se debe usar Bootable Media Builder?

El dispositivo de arranque disponible para su descarga en la consola de Cyber Protect está basado en un kernel Linux. A diferencia de Windows PE, no permite inyectar controladores personalizados sobre la marcha.

Bootable Media Builder le permite crear imágenes de dispositivo de arranque personalizadas basadas en Linux o en WinPE.

¿32 bits o 64 bits?

Bootable Media Builder crea dispositivos de arranque con componentes de 32 bits y 64 bits. En la mayoría de los casos, necesitará un medio de 64 bits para arrancar un equipo que utiliza la interfaz extensible del firmware unificada (UEFI).

Dispositivos de arranque basados en Linux

Para crear un dispositivo de arranque basado en Linux

1. Inicie **Bootable Media Builder**.
2. Seleccione **Predeterminado (dispositivo de arranque basado en Linux)** en **Tipo de dispositivo de arranque**.
3. Seleccione cómo se representarán los volúmenes y recursos de red:
   - Una representación de un dispositivo de arranque con un manejo de volúmenes estilo Linux muestra los volúmenes como, por ejemplo, hda1 y sdb2. Intenta reconstruir los dispositivos MD y los volúmenes lógicos (LVM) antes de comenzar una recuperación.
   - Una representación de un dispositivo de arranque con una gestión de volúmenes tipo Windows muestra los volúmenes, por ejemplo, como C: y D:. Proporciona acceso a los volúmenes dinámicos (LDM).
4. [Opcional] Especifique los parámetros del kernel Linux. Separe los diferentes parámetros con espacios.

   Por ejemplo, para poder seleccionar un modo de visualización para el agente de arranque cada vez que se inicia el dispositivo, escriba: **vga=ask**. Para obtener más información sobre los parámetros disponibles, consulte "Parámetros de kernel" (p. 987).
5. [Opcional] Seleccione el idioma del dispositivo de arranque.
6. [Opcional] Seleccione el modo de arranque (BIOS o UEFI) que utilizará Windows tras la recuperación.
7. Seleccione el componente que se ubicará en el dispositivo: el agente de arranque Cyber Protection.
8. [Opcional] Especifique el intervalo de tiempo de espera del menú de inicio. Si no se configura este ajuste, el cargador esperará a que seleccione si iniciar desde el sistema operativo (de estar presente) o el componente.

© Acronis International GmbH, 2003-2025

9. [Opcional] Si desea automatizar las operaciones del agente de arranque, seleccione la casilla de verificación **Utilizar el script siguiente**. A continuación, seleccione uno de los scripts y especifique los parámetros del script. Para obtener más información sobre los scripts, consulte "Scripts en dispositivo de arranque" (p. 990).
10. [Opcional] Seleccione cómo deben registrarse los dispositivos de arranque en el servicio Cyber Protection al arrancar. Para obtener más información sobre la configuración del registro, consulte "Registro del dispositivo de arranque" (p. 999).
11. Especifique la configuración de red para los adaptadores de red del equipo iniciado o conserve la configuración DHCP automática.
12. [Opcional] Si hay un servidor proxy habilitado en la red, especifique su nombre de servidor/dirección IP y puerto.
13. [Opcional] Para especificar el método de autenticación de red, haga clic en **Configuración de Wi-Fi** y seleccione uno de los siguientes:
    - Autenticación abierta
    - WEP
    - Compartido mediante WEP
    - IEEE 802.1X
    - WPA Personal
    - WPA Enterprise
    - WPA2 Personal
    - WPA2 Enterprise
14. Seleccione el tipo de archivo del dispositivo de arranque creado:
    - Imagen ISO
    - Archivo ZIP
15. Especifique un nombre de archivo para el archivo del dispositivo de arranque.
16. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.

Parámetros de kernel

Puede especificar uno o más parámetros del kernel Linux que se aplicarán automáticamente cuando se ejecute el dispositivo de arranque. Estos parámetros se utilizan comúnmente cuando tiene problemas mientras trabaja con el dispositivo de arranque. Normalmente, puede dejar este campo vacío.

También puede especificar cualquiera de estos parámetros pulsando F11 mientras está en el menú de arranque.

Parámetros

Cuando especifique varios parámetros, sepárelos con espacios.

© Acronis International GmbH, 2003-2025

- **acpi=off**

  Desactiva la interfaz de alimentación de configuración avanzada (ACPI). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.
- **noapic**

  Desactiva el Controlador de interrupciones programable avanzado (APIC). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.
- **vga=ask**

  Solicita que seleccione el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. Sin el parámetro **vga**, el modo vídeo se detecta automáticamente.
- **vga=** *mode_number*

  Especifica el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. El número de modo aparece en *mode_number* en formato hexadecimal, por ejemplo: **vga=0x318**

  La resolución de la pantalla y el número de colores correspondiente a un número de modo puede ser diferente en equipos diferentes. Le recomendamos utilizar primero el parámetro **vga=ask** para seleccionar un valor para *mode_number*.
- **quiet**

  Desactiva la muestra de mensajes de inicio cuando el kernel de Linux se está cargando y ejecuta la consola de gestión una vez que el kernel está cargado.

  Este parámetro está especificado implícitamente cuando crea el dispositivo de arranque, pero puede borrar este parámetro mientras esté en el menú de inicio.

  Si se elimina este parámetro, se mostrarán todos los mensajes de inicio, seguidos de una entrada de comandos. Para iniciar la consola de gestión desde la entrada de comandos, ejecute el comando: **/bin/product**
- **nousb**

  Desactiva la carga del subsistema del USB (bus universal en serie).
- **nousb2**

  Desactiva la compatibilidad con USB 2.0. No obstante, los dispositivos USB 1.1 trabajan con este parámetro. Este parámetro le permite utilizar algunas unidades USB en el modo USB 1.1 si no funcionan en el modo USB 2.0.
- **nodma**

  Desactiva el acceso directo a memoria (DMA) para todas las unidades del disco duro IDE. Evita que el kernel se congele en algún hardware.
- **nofw**

  Desactiva la compatibilidad con la interfaz de FireWire (IEEE1394).
- **nopcmcia**

  Desactiva la detección del hardware PCMCIA.
- **nomouse**

  Desactiva la compatibilidad con el ratón.
- *module_name* **=off**

© Acronis International GmbH, 2003-2025

Desactiva el módulo cuyo nombre aparece en *module_name*. Por ejemplo, para desactivar el uso del módulo SATA, especifique: **sata_sis=off**

- **pci=bios**

  Obliga al uso de PCI BIOS en vez de acceder directamente al dispositivo del hardware. Es conveniente que utilice este parámetro si el equipo tiene un puente PCI no estándar de host.
- **pci=nobios**

  Desactiva el uso de PCI BIOS; solo se pueden utilizar métodos de acceso directo al hardware. Es conveniente que utilice este parámetro cuando el dispositivo de arranque no puede iniciarse, lo que puede deberse a la BIOS.
- **pci=biosirq**

  Utiliza las alertas PCI BIOS para obtener la tabla de rutas de interrupción. Es conveniente que utilice este parámetro si el kernel no puede asignar solicitudes de interrupción (IRQ) o descubrir enlaces secundarios de PCI en la placa madre.

  Estas llamadas pueden no funcionar correctamente en algunos equipos. Pero puede ser la única manera de obtener la tabla de rutas de interrupción.
- **LAYOUTS=en-US, de-DE, fr-FR, ...**

  Especifica las disposiciones del teclado que se pueden utilizar en la interfaz gráfica de usuario del dispositivo de arranque.

  Sin este parámetro, solo se pueden utilizar dos disposiciones: Inglés (EE. UU.) y la disposición correspondiente al idioma seleccionado en el menú del dispositivo de arranque.

  Puede especificar cualquiera de las siguientes disposiciones:

  Belga: **be-BE**

  Checo: **cz-CZ**

  Inglés: **en-GB**

  Inglés (EE. UU.): **en-US**

  Francés: **fr-FR**

  Francés (Suiza): **fr-CH**

  Alemán: **de-DE**

  Alemán (Suiza): **de-CH**

  Italiano: **it-IT**

  Polaco **pl-PL**

  Portugués **pt-PT**

  Portugués (Brasil): **pt-BR**

  Ruso: **ru-RU**

  Serbio (cirílico): **sr-CR**

  Serbio (latino): **sr-LT**

  Español: **es-ES**

  Al trabajar con un dispositivo de arranque, utilice CTRL + MAYÚS para desplazarse por las disposiciones disponibles.

© Acronis International GmbH, 2003-2025

Scripts en dispositivo de arranque

Si desea que el dispositivo de arranque lleve a cabo un conjunto de operaciones predefinido, puede especificar un script mientras crea el dispositivo con Bootable Media Builder. Cada vez que se arranque un equipo desde el dispositivo, se ejecutará el script especificado y no se mostrará la interfaz de usuario.

Puede seleccionar uno de los scripts predefinidos o crear un script personalizado siguiendo las convenciones de scripts.

Scripts predefinidos

Bootable Media Builder proporciona los siguientes scripts predefinidos:

- Recuperación desde el almacenamiento en la nube (**entire_pc_cloud**)
- Recuperación desde un recurso compartido de red (**entire_pc_share**)

Los scripts deben estar ubicados en las carpetas siguientes del equipo en el que esté instalado Bootable Media Builder:

- En Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- En Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Recuperación desde el almacenamiento en la nube

En Bootable Media Builder, especifique los siguientes parámetros del script:

1. El nombre del archivo de la copia de seguridad.
2. [Opcional] Una contraseña que el script utilizará para acceder a copias de seguridad cifradas.

Recuperación desde un recurso compartido de red

En Bootable Media Builder, especifique los siguientes parámetros del script:

- La ruta al recurso compartido de red.
- El nombre de usuario y la contraseña de la red compartida.
- El nombre del archivo de la copia de seguridad. Pasos para descubrir el nombre del archivo de la copia de seguridad:
  a. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad** > **Ubicaciones**.
  b. Seleccione la red compartida (haga clic en **Añadir ubicación** si la red compartida no aparece en la lista).
  c. Seleccione la copia de seguridad.
  d. Haga clic en **Detalles**. El nombre del archivo se muestra en **Nombre del archivo de la copia**

© Acronis International GmbH, 2003-2025

de seguridad.

- [Opcional] Una contraseña que el script utilizará para acceder a copias de seguridad cifradas.

Scripts personalizados

Importante
Crear scripts personalizados requiere conocimientos de lenguaje de comandos Bash y JavaScript Object Notation (JSON). Si no está familiarizado con Bash, un buen lugar para aprender es http://www.tldp.org/LDP/abs/html. La especificación de JSON está disponible en http://www.json.org.

Archivos de un script

El script debe estar ubicado en los directorios siguientes del equipo en el que esté instalado Bootable Media Builder:

- En Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- En Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

El script debe constar de tres archivos como mínimo:

- **<script_file>.sh** - un archivo con su script Bash. Al crear el script, utilice únicamente un conjunto limitado de comandos shell, que podrá encontrar en https://busybox.net/downloads/BusyBox.html. Además, se pueden utilizar los comandos siguientes:
  - `acrocmd` - la utilidad de línea de comandos para copia de seguridad y recuperación
  - `product` - el comando que inicia la interfaz de usuario del dispositivo de arranque

  Este archivo y cualquier otro que incluya el script (por ejemplo, utilizando el comando dot) deben ubicarse en la subcarpeta **bin**. En el script, especifique las rutas de los archivo adicionales como **/ConfigurationFiles/bin/<some_file>**.
- **autostart** - un archivo para iniciar **<script_file>.sh**. El contenido del archivo debe ser el siguiente:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - un archivo JSON que contiene lo siguiente:
  - El nombre y la descripción del script que aparecerá en Bootable Media Builder.
  - Los nombres de las variables del script que desea configurar mediante Bootable Media Builder.
  - Los parámetros de los controles que aparecerán en Generador de dispositivos de inicio para cada variable.

© Acronis International GmbH, 2003-2025

Estructura de autostart.json

Objeto de nivel superior

Pareja		Obligatorio	Descripción
Nombre	**Tipo de valor**		
`displayName`	string	Sí	El nombre de script que aparecerá en el Generador de dispositivos de inicio.
`description`	string	No	La descripción del script que aparecerá en el Generador de dispositivos de inicio.
`timeout`	number	No	El tiempo de espera (en segundos) del menú de arranque antes de que se inicie el script. Si no se especifica la pareja, el tiempo de espera será de diez segundos.
`variables`	objeto	No	Las variables de **<script_file>.sh** que desee configurar a través del Generador de dispositivos de inicio. El valor debe ser un conjunto de las parejas siguientes: el identificador de la cadena de una variable y el objeto de la variable (consulte la tabla que aparece a continuación).

Objeto de variable

Pareja		Obligatorio	Descripción
Nombre	**Tipo de valor**		
`displayName`	string	Sí	El nombre de la variable utilizado en **<script_file>.sh**.
`type`	string	Sí	El tipo de control que aparece en el Generador de dispositivos de inicio. Este control se utiliza para configurar el valor de la variable. Para todos los tipos admitidos, consulte la tabla que aparece a continuación.
`description`	string	Sí	La etiqueta de control que aparece encima del control en el Generador de dispositivos de inicio.

© Acronis International GmbH, 2003-2025

`default`	cadena si `type` es `string`, `multiString`, `password` o `enum` número si `type` es `number`, `spinner` o `checkbox`	No	El valor predeterminado para el control. Si no se especifica la pareja, el valor predeterminado será una cadena vacía o un cero, dependiendo del tipo de control. El valor predeterminado de una casilla de verificación puede ser `0` (el estado borrado) o `1` (el estado seleccionado).
`order`	number (no negativo)	Sí	La petición de control en el Generador de dispositivos de inicio. Cuanto más alto sea el valor, más bajo será el control colocado en relación a otros controles definidos en **autostart.json**. El valor inicial debe ser `0`.
`min` (solo para `spinner`)	number	No	El valor mínimo del control de número en un cuadro de número. Si no se especifica la pareja, el valor será `0`.
`max` (solo para `spinner`)	number	No	El valor máximo del control de número en un cuadro de número. Si no se especifica la pareja, el valor será `100`.
`step` (solo para `spinner`)	number	No	El valor de paso del control de número de un cuadro de número. Si no se especifica la pareja, el valor será `1`.
`items` (solo para `enum`)	matriz de cadenas	Sí	Los valores de una lista desplegable.
`required` (para `string`, `multiString`, `password` y `enum`)	number	No	Especifica si el valor del control puede estar vacío (`0`) o no (`1`). Si no se especifica la pareja, el valor de control puede estar vacío.

Tipo de control

Nombre	Descripción
`string`	Un cuadro de texto sin límite y en una sola línea que se utiliza para introducir o modificar cadenas cortas.

© Acronis International GmbH, 2003-2025

multiString	Un cuadro de texto sin límite y en varias líneas que se utiliza para introducir o modificar cadenas largas.
password	Un cuadro de texto sin límite y en una sola línea que se utiliza para introducir contraseñas de forma segura.
number	Un cuadro de texto numérico y en una sola línea que se utiliza para introducir o modificar números.
spinner	Un cuadro de texto numérico y en una sola línea que se utiliza para introducir o modificar números con un control de números denominado cuadro de número.
enum	Una lista desplegable estándar, con un conjunto fijo de valores predeterminados.
checkbox	Una casilla de verificación con dos estados, el estado borrado o el estado seleccionado.

El ejemplo **autostart.json** que aparece a continuación contiene todos los tipos posibles de controles que se pueden utilizar para configurar variables para **<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,
```


© Acronis International GmbH, 2003-2025

```
                "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
            }
        }
}
```

Dispositivos de arranque basados en Windows

Puede crear imágenes basadas en WinRE sin ninguna preparación adicional, o crear imágenes basadas en WinPE después de instalar Windows Automated Installation Kit (AIK) o Windows Assessment and Deployment Kit (ADK).

© Acronis International GmbH, 2003-2025

Imágenes basadas en WinRE

La creación de imágenes basadas en WinRE es compatible con los siguientes sistemas operativos:

- Windows 7 (64 bits)
- Windows 8 (32 bits y 64 bits)
- Windows 8.1 (32 bits y 64 bits)
- Windows 10 (32 bits y 64 bits)
- Windows 11 (64 bits)
- Windows Server 2012 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)
- Windows Server 2022 (64 bits)
- Windows Server 2025 (64 bits)

Imágenes basadas en WinPE

Después de instalar Windows Automated Installation Kit (AIK) o Windows Assessment and Deployment Kit (ADK), Bootable Media Builder es compatible con las distribuciones de WinPE que están basadas en cualquiera de los siguientes kernels:

- Windows Vista (PE 2.0)
- Windows Vista SP1 y Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) con o sin el complemento para Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder es compatible con las distribuciones de 32 bits y 64 bits de WinPE. Las distribuciones de 32 bits de WinPE también funcionan en hardware de 64 bits. Sin embargo, necesita una distribución de 64 bits para arrancar un equipo que utiliza Unified Extensible Firmware Interface (UEFI).

Nota
Las imágenes PE basadas en WinPE 4 y versiones posteriores necesitan aproximadamente 1 GB de RAM para funcionar.

Creación de dispositivos de arranque basados en WinPE o WinRE

Bootable Media Builder ofrece dos formas de integrar Cyber Protection con WinPE y WinRE:

© Acronis International GmbH, 2003-2025

- Creación de un archivo ISO con el complemento Cyber Protection desde cero.
- Adición del complemento de Cyber Protection a un archivo WIM para cualquier propósito (creación manual de imagen ISO, adición de otras herramientas a la imagen, etc.).

Para crear dispositivos de arranque basados en WinPE o WinRE

1. Ejecute Bootable Media Builder en el equipo donde esté instalado el agente de protección.
2. Seleccione **Windows PE** o **Windows PE (64 bits)** en **Tipo de dispositivo de arranque**. Se necesita un dispositivo de 64 bits para arrancar un equipo que utiliza Unified Extensible Firmware Interface (UEFI).
3. Seleccione el subtipo del dispositivo de arranque: **WinRE** o **WinPE**.

   Para crear dispositivos de arranque basados en WinRE no es necesario instalar ningún paquete adicional.

   Para crear dispositivos basados en WinPE de 64 bits, descargue Windows Automated Installation Kit (AIK) o Windows Assessment and Deployment Kit (ADK). Para crear dispositivos basados en WinPE de 32 bits, además de descargar AIK o ADK, deberá:

   a. Haga clic en **Descargar complemento para WinPE (32 bits)**.

   b. Guardar el complemento en **%PROGRAM_ FILES%\BackupClient\BootableComponents\WinPE32**.
4. [Opcional] Seleccione el idioma del dispositivo de arranque.
5. [Opcional] Seleccione el modo de arranque (BIOS o UEFI) que utilizará Windows tras la recuperación.
6. Especifique la configuración de red para los adaptadores de red del equipo iniciado o conserve la configuración DHCP automática.
7. [Opcional] Seleccione cómo deben registrarse los dispositivos de arranque en el servicio Cyber Protection al arrancar. Para obtener más información sobre la configuración del registro, consulte "Registro del dispositivo de arranque" (p. 999).
8. [Opcional] Especifique los controladores de Windows que se deben añadir a los dispositivos de arranque.

   Cuando haya iniciado su equipo en Windows PE o Windows RE, los controladores le ayudarán a acceder al dispositivo donde esté ubicada la copia de seguridad. Añada los controladores de 32 bits si utiliza una distribución de 32 bits de WinPE o WinRE o controladores de 64 bits si utiliza una distribución de 64 bits de WinPE. o WinRE.

   Para añadir los controladores:

   - Haga clic en **Agregar** y especifique la ruta al archivo .inf necesario para el correspondiente controlador SCSI, RAID o SATA; adaptador de red, u otros dispositivos.
   - Repita este procedimiento para cada controlador que desee incluir en el medio WinPE o WinRE resultante.
9. Seleccione el tipo de archivo del dispositivo de arranque creado:
   - Imagen ISO
   - Imagen WIM

© Acronis International GmbH, 2003-2025

10. Especifique la ruta completa al archivo de imagen ISO resultante incluyendo el nombre de archivo.
11. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.

Para crear una imagen PE (archivo ISO) del archivo WIM resultante

- Reemplace el archivo boot.wim predeterminado en su carpeta de Windows PE junto al archivo WIM creado recientemente. Para el ejemplo anterior, escriba:

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Use la herramienta **Oscdimg**. Para el ejemplo anterior, escriba:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Advertencia.
No copie y pegue este ejemplo. Introduzca el comando manualmente o de lo contrario fallará.

Preparación: WinPE 2.x y 3.x

Para poder crear o modificar imágenes PE 2.x o 3.x, instale Bootable Media Builder y Windows Automated Installation Kit (AIK) en el equipo.

Pasos para preparar un equipo

1. Descargue el archivo de imagen AIK desde el sitio web de Microsoft de la siguiente manera:
   - Para Windows Vista (PE 2.0): https://www.microsoft.com/es-es/download/details.aspx?id=10333
   - Para Windows Vista SP1 y Windows Server 2008 (PE 2.1): https://www.microsoft.com/es-es/download/details.aspx?id=9085
   - Para Windows 7 (PE 3.0): https://www.microsoft.com/es-es/download/details.aspx?id=5753
     Para Windows 7 SP1 (PE 3.1), también necesita el suplemento AIK disponible en https://www.microsoft.com/es-es/download/details.aspx?id=5188
2. Grabe el archivo de imagen en un disco DVD o en una memoria USB.
3. Desde el archivo de imagen, instale lo siguiente:
   - Microsoft .NET Framework (NETFXx86 o NETFXx64, dependiendo de su hardware)
   - MSXML (Analizador XML de Microsoft)
   - Windows AIK
4. Instale Bootable Media Builder en el mismo equipo.

Preparación: WinPE 4.0 y posterior

Para poder crear o modificar imágenes PE 4 o posteriores, instale Bootable Media Builder y Windows Assessment and Deployment Kit (ADK) en el mismo equipo.

Pasos para preparar un equipo

© Acronis International GmbH, 2003-2025

1. Descargue el programa de configuración de ADK desde la página web de Microsoft.
   Las siguientes versiones de Windows son compatibles:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Instale Assessment and Deployment Kit.
3. Instale Bootable Media Builder.

Registro del dispositivo de arranque

El registro del dispositivo de arranque en el servicio Cyber Protection permite el acceso al almacenamiento en la nube para sus copias de seguridad. Puede configurar previamente el registro al crear el dispositivo de arranque. Si el registro no se configura previamente, puede registrar el dispositivo después de iniciar un equipo con él.

Para configurar previamente el registro en el servicio Cyber Protection

1. En Bootable Media Builder, vaya a **Registro de dispositivos de arranque**.
2. En **Servicio URL**, especifique la dirección del servicio Cyber Protection.
3. [Opcional] En **Nombre que se muestra**, especifique un nombre para el dispositivo de arranque.
4. Para establecer el registro automático del servicio Cyber Protection, seleccione la casilla de verificación **Registrar el dispositivo de arranque automáticamente** y seleccione el nivel del registro automático:
   - **Solicitar el token de registro en el arranque**
     Deberá proporcionar el token cada vez que se arranque un equipo desde este dispositivo de arranque.
   - **Usar el siguiente token**
     El equipo se registrará automáticamente cuando se arranque desde este dispositivo de arranque.

Para registrar el dispositivo de arranque después de arrancar un equipo con él

1. Inicie el equipo desde el dispositivo de arranque.
2. En la ventana de inicio, haga clic en **Registrar dispositivo**.
3. En **Servidor**, especifique la dirección del servicio Cyber Protection.
4. En **Token de registro**, escriba el token de registro.
5. Haga clic en **Registrar**.

© Acronis International GmbH, 2003-2025

Configuraciones de red

Al crear el dispositivo de arranque, puede preconfigurar las conexiones de red que serán usadas por el agente de inicio. Se pueden preconfigurar los siguientes parámetros:

- Dirección IP
- Máscara de subred
- Puertas de enlace
- Servidor DNS
- Servidor WINS

Una vez que se inicia el agente de arranque en un equipo, se aplica la configuración en la tarjeta de interfaz de red (NIC) del equipo. Si no se preestablece la configuración, el agente usa la configuración automática del servidor DHCP.

También puede establecer manualmente la configuración de red cuando se ejecuta el agente de inicio en el equipo.

Preconfiguración de múltiples conexiones de red

Puede preestablecer la configuración TCP/IP de hasta 10 tarjetas de interfaz de red (NIC). Para asegurar que cada NIC tendrá asignada la configuración adecuada, cree el dispositivo en el servidor en donde se personalizan los dispositivos. Cuando seleccione una NIC en el agente de Windows, se selecciona su configuración para guardarlos en el dispositivo. También se guarda la dirección MAC de cada NIC en los dispositivos.

Puede cambiar la configuración, excepto por la dirección MAC, o establecer la configuración para una NIC no existente.

Una vez que el dispositivo de inicio se ejecute en el servidor, recupera la lista de NIC disponibles. Esta lista está ordenada por las ranuras que ocupan las NIC: la más cercana al procesador está en la parte superior.

El agente de inicio asigna la configuración apropiada a cada NIC conocida y las identifica por sus direcciones MAC. Después de que se configuran las NIC con direcciones MAC conocidas, se asigna la configuración que realizó para NIC no existentes a las NIC restantes, comenzando por la NIC no asignada superior.

Puede personalizar los dispositivos de arranque para cualquier equipo, y no solo para el equipo en donde se crea el dispositivo. Para hacerlo, configure las NIC de acuerdo con el orden de ranuras del equipo. NIC1 ocupa la ranura más cercana al procesador, NIC2 es la siguiente ranura. Cuando el agente de inicio se ejecute en el equipo, no encontrará las NIC con direcciones MAC conocidas y configurará las NIC en el mismo orden que usted.

Ejemplo

© Acronis International GmbH, 2003-2025

El agente de arranque puede usar uno de los adaptadores de red para la comunicación con la consola de administración por medio de la red de producción. Se puede establecer la configuración automática para esta conexión. Se pueden transferir los datos que se pueden dividir para su recuperación por la segunda NIC, incluida en la red de copia de seguridad por medio de la configuración TCP/IP.

Conexión a un equipo que se inició desde un dispositivo de arranque

Conexión local

Para realizar la operación directamente en el equipo iniciado desde el dispositivo de arranque, haga clic en **Gestionar este equipo localmente** en la ventana de inicio.

Cuando un equipo se inicia desde un dispositivo de arranque, la terminal del equipo muestra una ventana de inicio con las direcciones IP que el servidor DHCP proporcionó o las establecidas de acuerdo con los valores preconfigurados.

Configurar los ajustes de red

Para cambiar los ajustes de red de la sesión actual, haga clic en **Configurar red** en la ventana de inicio. La ventana **Configuraciones de red** que aparece le permite configurar los ajustes de red para cada tarjeta de interfaz de red (NIC) del equipo.

Los cambios realizados durante una sesión se perderán cuando se reinicie el equipo.

Añadir VLAN

En la ventana **Configuraciones de red** puede añadir redes de área local virtual (VLAN). Utilice esta función si precisa acceder a la ubicación de una copia de seguridad incluida en una VLAN específica.

Las VLAN se utilizan principalmente para dividir una red de área local en segmentos. Las NIC conectadas a un puerto de *acceso* del conmutador pueden acceder a la VLAN especificada en la configuración del puerto. Las NIC conectadas a un puerto *troncal* del conmutador pueden acceder a las VLAN incluidas en la configuración del puerto únicamente si especifica la VLAN en las configuraciones de red.

Para habilitar el acceso a una VLAN mediante un puerto troncal

1. Haga clic en **Añadir VLAN**.
2. Seleccione la NIC que proporciona el acceso a la red de área local en la que se incluye la VLAN necesaria.
3. Especifique el identificador de la VLAN.

Después de hacer clic en **Aceptar**, aparecerá una entrada nueva en la lista de adaptadores de red.

Si desea eliminar una VLAN, seleccione la entrada de la VLAN correspondiente y, a continuación, en **Eliminar la VLAN**.

© Acronis International GmbH, 2003-2025

Operaciones locales con dispositivos de arranque

Las operaciones con dispositivos de arranque son similares a las operaciones de recuperación que se llevan a cabo en un sistema operativo actualmente en ejecución. Las diferencias son las siguientes:

1. En dispositivos de arranque con una representación del volumen de tipo Windows, un volumen tiene la misma letra de unidad que en Windows. A los volúmenes que no tienen letras de unidad en Windows (tal como el volumen Reservado del sistema) se les asignan letras según el orden de su secuencia en el disco.

   Si el dispositivo de arranque no puede detectar Windows en el equipo o detecta más de uno, se asigna una letra a todos los volúmenes, incluidos aquellos que no tienen letra de unidad de disco, según el orden de su secuencia en el disco. Por eso, es posible que las letras de los volúmenes no coincidan con las de Windows. Por ejemplo, la unidad D: del dispositivo de arranque podría corresponder a la unidad E: de Windows.

   Nota
   Es aconsejable asignar nombres únicos a los volúmenes.

2. Los dispositivos de arranque con una representación del volumen de estilo Linux muestran tanto los discos y volúmenes locales como desmontados (sda1, sda2...).
3. No se pueden planificar las tareas. Si necesita repetir una operación, configúrela desde cero.
4. La vida útil del registro se limita a la sesión actual. Puede guardar todo el registro o las entradas del registro filtradas a en un archivo.

Configuración del modo de visualización

Cuando inicia un equipo desde un dispositivo de arranque basado en Linux, se detecta automáticamente un modo de vídeo de visualización basado en la configuración del hardware (especificaciones de la tarjeta del monitor y de los gráficos). Si el modo vídeo se detecta de manera incorrecta, realice lo siguiente:

1. Pulse F11 en el menú de inicio.
2. En la línea de comando, introduzca **vga=ask** y prosiga con el arranque.
3. En la lista de modos de vídeo compatibles, escoja el correcto al escribir su número (por ejemplo, **318**) y pulse **Intro**.

Si no desea seguir este procedimiento cada vez que inicie una configuración de hardware en concreto, cree de nuevo el dispositivo de arranque con el número de modo apropiado (en el ejemplo anterior, **vga=0x318**) especificado en el campo **Parámetros del kernel**.

© Acronis International GmbH, 2003-2025

Recuperación con soporte de arranque in situ

1. Inicie su equipo desde el dispositivo de arranque.
2. Haga clic en **Gestionar este equipo localmente**.
3. Haga clic en **Recuperar**.
4. En **Qué recuperar**, haga clic en **Seleccionar datos**.
5. Seleccione el archivo de la copia de seguridad que desea recuperar.
6. En el panel inferior izquierdo, seleccione las unidades o volúmenes, o archivos y carpetas, que desee recuperar y haga clic en **Aceptar**.
7. Configure las reglas de sobrescritura.
8. Configure las exclusiones de recuperación.
9. Configure las opciones de recuperación.
10. Compruebe que su configuración sea correcta y haga clic en **Aceptar**.

Operaciones remotas con soportes de arranque

Nota
Esta función está disponible con el paquete Advanced Backup.

Para ver el soporte de arranque en la consola de Cyber Protect, primero debe registrarlo como se describe en "Registro del dispositivo de arranque" (p. 999).

Después de registrar el medio en la consola de Cyber Protect, aparecerá en la pestaña **Dispositivos** > **Dispositivos de arranque**. Un dispositivo de arranque desaparece de esta pestaña cuando lleva offline más de 30 días.

Puede gestionar el dispositivo de arranque de forma remota en la consola de Cyber Protect. Por ejemplo, puede recuperar datos, reiniciar o apagar el equipo arrancado con el dispositivo o ver información, actividades y alertas sobre este.

Importante

- La operación remota con dispositivos de arranque no es compatible con volúmenes LVM/LDM.
- No puede actualizar el dispositivo de arranque de forma remota en la pestaña **Configuración** > **Agentes** de la consola de Cyber Protect.

  Para actualizar el dispositivo de arranque, cree uno nuevo tal y como se describe en la sección "Bootable Media Builder" (p. 985). También puede descargar el dispositivo listo haciendo clic en el icono de su cuenta > **Descargas** > **Dispositivos de arranque** en la consola de Cyber Protect.

Pasos para recuperar archivos o carpetas con el soporte de arranque de forma remota

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Dispositivo de arranque**.
1. Seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Recuperación**.
3. Seleccione la ubicación y, a continuación, seleccione la copia de seguridad que necesite. Tenga en cuenta que las copias de seguridad se filtran por ubicación.
4. Seleccione el punto de recuperación y haga clic en **Recuperar archivos o carpetas**.
5. Vaya hasta la carpeta requerida o utilice la barra de búsqueda para obtener la lista de los archivos y carpetas deseados.

   La búsqueda es independiente del idioma.

   Puede utilizar uno o más caracteres comodín (* y ?). Para obtener más información sobre el uso de los caracteres comodín, consulte la sección "Filtros de archivo (inclusiones y exclusiones)" (p. 607).
6. Haga clic para seleccionar los archivos que desea recuperar y, a continuación, haga clic en **Recuperar**.
7. En **Ruta**, seleccione el destino de la recuperación.
8. [Opcional] Para la configuración de recuperación avanzada, haga clic en **Opciones de recuperación**. Para obtener más información, consulte "Opciones de recuperación" (p. 710).
9. Haga clic en **Iniciar recuperación**.
10. Seleccione una de las opciones de sobreescritura de archivos:
    - **Sobrescribir archivos existentes**
    - **Sobrescribir un archivo existente si es más antiguo**
    - **No sobrescribir archivos existentes**

    Elija si desea reiniciar el equipo automáticamente.
11. Haga clic en **Continuar** para iniciar la recuperación. Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Pasos para recuperar discos, volúmenes o equipos completos con el soporte de arranque de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Dispositivo de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Recuperación**.
3. Seleccione la ubicación y, a continuación, seleccione la copia de seguridad que necesite. Tenga en cuenta que las copias de seguridad se filtran por ubicación.
4. Seleccione el punto de recuperación y haga clic en **Recuperar** > **Todo el equipo**.

   Si fuese necesario, configure el equipo de destino y la asignación de volúmenes como se describe en "Recuperación de equipos físicos" (p. 663).
5. Para la configuración de recuperación avanzada, haga clic en **Opciones de recuperación**. Para obtener más información, consulte "Opciones de recuperación" (p. 710).
6. Haga clic en **Iniciar recuperación**.

© Acronis International GmbH, 2003-2025

7. Confirme si desea sobrescribir los discos con sus respectivas copias de seguridad. Elija si desea reiniciar el equipo automáticamente.
8. Puede comprobar el progreso de la recuperación en de Cyber Protect en la pestaña **Actividades**.

Pasos para reiniciar el equipo arrancado de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Dispositivo de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Reiniciar**.
3. Confirme que quiere reiniciar el equipo arrancado con el medio.

Pasos para apagar el equipo arrancado de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Dispositivo de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Apagar**.
3. Confirme que quiere apagar el equipo arrancado con el medio.

Pasos para ver información sobre el soporte de arranque

1. En la pestaña, **Dispositivos**, vaya al grupo **Dispositivo de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Detalles**, **Actividades** o **Alertas** para ver la información correspondiente.

Pasos para eliminar el soporte de arranque de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Dispositivo de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Eliminar** para eliminar el soporte de arranque de la consola de Cyber Protect.
3. Confirme que desea eliminar el soporte de arranque.

Soporte para agrupación de tarjetas NIC

La agrupación (bonding) de tarjetas de interfaz de red (NIC) se conserva tanto durante la recuperación de una carga de trabajo con tarjetas NIC agrupadas, como después de la recuperación.

Puede desactivar la agrupación de tarjetas NIC durante la recuperación si recupera una carga de trabajo de cualquiera de las siguientes maneras:

- Con dispositivo de arranque descargado
- Con dispositivo de arranque basado en Linux creado en Bootable Media Builder
- Mediante Acronis Startup Recovery Manager
- Mediante recuperación con un clic
- Mediante la recuperación con reinicio, utilizando el entorno de recuperación de Linux

© Acronis International GmbH, 2003-2025

Pasos para desactivar la agrupación de tarjetas NIC durante la recuperación

1. En el equipo respaldado, abra el siguiente archivo de configuración para editarlo:
   - Windows:
     ```
     C:\Program Files\Common Files\Acronis\BackupAndRecoveryAgent\bootagent_
     msp64.config
     ```
   - Linux:
     ```
     /usr/lib/Acronis/BackupAndRecoveryAgent/bootagent_msp64.config
     ```
2. En el archivo de configuración, busque la siguiente línea:
   - Windows:
     ```
     <kernel64 name="kernel64.dat" value="product=bootagent media_for_windows"
     target="abr64ker.dat"/>
     ```
   - Linux:
     ```
     <kernel64 name="kernel64.dat" value="product=bootagent media_for_linux"
     target="abr64ker.dat"/>
     ```
3. Edite la línea de esta manera:
   - Windows
     ```
     <kernel64 name="kernel64.dat" value="product=bootagent DONT_CREATE_BONDING=1
     media_for_windows" target="abr64ker.dat"/>
     ```
   - Linux
     ```
     <kernel64 name="kernel64.dat" value="product=bootagent DONT_CREATE_BONDING=1
     media_for_linux" target="abr64ker.dat"/>
     ```
4. Guarde el archivo de configuración.
5. Recupere la carga de trabajo utilizando cualquiera de los métodos soportados.

Como resultado, el agrupamiento de tarjetas NIC no se utilizará durante la recuperación.

Nota
La carga de trabajo recuperada retiene el agrupamiento de tarjetas NIC. Para deshabilitar el agrupamiento de tarjetas NIC después de la recuperación, reconfigure la configuración de la red de la carga de trabajo.

© Acronis International GmbH, 2003-2025

Startup Recovery Manager

Startup Recovery Manager es un componente de arranque que reside en la unidad de disco duro. Con Startup Recovery Manager, puede iniciar la utilidad de rescate de inicio sin usar un soporte de arranque distinto.

Si ocurre un fallo, reinicie el equipo, espere a que aparezca el mensaje **Pulse F11 para Acronis Startup Recovery Manager** y luego pulse F11 o seleccione Startup Recovery Manager en el menú de inicio (si usa el cargador de arranque GRUB). Se inicia Startup Recovery Manager y puede realizar una recuperación.

Startup Recovery Manager es compatible con equipos Windows y Linux.

Importante
La activación de Startup Recovery Manager en un equipo con volumen de sistema cifrado requiere al menos un volumen no cifrado en el mismo equipo.

Requisitos de espacio en disco

Startup Recovery Manager requiere espacio en disco para archivos temporales. Los requisitos varían según el equipo en el que se activa Startup Recovery Manager.

La tabla siguiente resume las opciones disponibles.

Modo de arranque	Equipo sin Secure Zone		Equipo con Secure Zone
	Con volumen del sistema no cifrado	Con volumen del sistema cifrado	Con volumen del sistema cifrado o no cifrado
BIOS	200 MB en el volumen del sistema	400 MB en un volumen sin cifrar	400 MB en Secure Zone
UEFI	200 MB en la partición del sistema EFI (ESP)	Uno de los siguientes: • 400 MB en la partición del sistema EFI (ESP) • 200 MB en la partición del sistema EFI (ESP) y 200 MB en una partición no cifrada que es accesible durante el proceso de arranque	400 MB en Secure Zone

© Acronis International GmbH, 2003-2025

Nota
La recuperación con reinicio requiere espacio adicional en el disco. Para comprobar cuánto espacio adicional se necesita, consulte "Requisitos de espacio en disco" (p. 705).

Limitaciones

- [No aplicable a GRUB que está instalado en el registro de inicio maestro] Activar Startup Recovery Manager sobrescribe el registro de inicio maestro (MBR) con su propio código de inicio. Como resultado, es posible que necesite reactivar cualquier cargador de inicio de terceros después de la activación.
- [No aplicable a GRUB] Antes de activar Startup Recovery Manager en Linux, recomendamos que instale el cargador de inicio en el registro de inicio de la partición raíz o en el registro de inicio de las particiones /boot en lugar de instalarlo en el registro de inicio maestro. De lo contrario, debe reconfigurar manualmente el cargador de inicio después de la activación.

Activación de Startup Recovery Manager

Para habilitar el mensaje de tiempo de inicio **Pulse F11 para Acronis Startup Recovery Manager** (o añada el elemento **Startup Recovery Manager** al menú GRUB), se debe activar Startup Recovery Manager.

Nota
Las operaciones de copia de seguridad que crean copias de seguridad de recuperación con un clic no funcionarán si Startup Recovery Manager no está activado.

Para activar Startup Recovery Manager

En una máquina con un agente

1. En la consola de Cyber Protect, seleccione el equipo en el que quiera activar Startup Recovery Manager.
2. Haga clic en **Detalles**.
3. Habilite el conmutador de **Startup Recovery Manager**.

En un equipo sin un agente

1. Arranque el equipo utilizando un soporte de arranque.
2. En la interfaz gráfica del soporte de arranque, haga clic en **Herramientas** > **Activar Startup Recovery Manager**.
3. Seleccione **Activar**.
4. Haga clic en **Aceptar**.
5. En la pestaña **Detalles**, revise la fila **Resultado** para verificar que la activación se ha realizado correctamente.
6. Haga clic en **Cerrar**.

© Acronis International GmbH, 2003-2025

Desactivación de Startup Recovery Manager

La inhabilitación desactiva el mensaje de tiempo de inicio **Pulse F11 para Acronis Startup Recovery Manager** (o elimine el elemento **Startup Recovery Manager** del menú GRUB).

Si Startup Recovery Manager no está activado, aún puede recuperar un equipo que no logra arrancar utilizando un soporte de arranque separado.

Nota
Las operaciones de copia de seguridad que crean copias de seguridad de recuperación con un clic no funcionarán si Startup Recovery Manager no está activado.

Para desactivar Startup Recovery Manager

En una máquina con un agente

1. En la consola de Cyber Protect, seleccione el equipo en el que quiera desactivar Startup Recovery Manager.
2. Haga clic en **Detalles**.
3. Deshabilite el conmutador **Startup Recovery Manager**.

En un equipo sin un agente

1. Arranque el equipo utilizando un soporte de arranque.
2. En la interfaz gráfica del soporte de arranque, haga clic en **Herramientas** > **Desactivar Startup Recovery Manager**.
3. Seleccione **Desactivar**.
4. Haga clic en **Aceptar**.
5. En la pestaña **Detalles**, revise la fila **Resultado** para confirmar que la desactivación se ha completado.
6. Haga clic en **Cerrar**.

© Acronis International GmbH, 2003-2025

Implementación de la recuperación ante desastres

Acerca de Acronis Disaster Recovery

Acronis Disaster Recovery forma parte de Cyber Protection, que ofrece recuperación ante desastres como servicio (DRaaS). Disaster Recovery es una solución rápida y estable que, en caso de desastre natural o provocado por el hombre, activa servidores de recuperación (copias exactas de sus servidores locales) en el sitio de recuperación ante desastres (DR).

El sitio de DR es una ubicación secundaria que garantiza que las operaciones de TI se restauren y continúen si el sitio principal falla. En tal caso, DR cambia las cargas de trabajo de los equipos originales dañados a los servidores de recuperación en el sitio de DR. El sitio de DR incluye los servidores en la nube y la conexión a la nube (redes en la nube).

La ubicación del sitio de DR puede estar en Acronis Cyber Protect Cloud o en Microsoft Azure. La disponibilidad de las ubicaciones del sitio de DR depende de los elementos de la oferta que estén habilitados para su inquilino.

Nota
Solo se admite una ubicación por inquilino de cliente. Si desea cambiar la ubicación de su sitio de DR, primero debe eliminar la configuración existente y, a continuación, crear una nueva con la nueva ubicación.

Para obtener más información sobre Disaster Recovery en Acronis Cyber Protect Cloud, consulte "Disaster Recovery para Cyber Protect Cloud" (p. 1010).

Para obtener más información sobre Disaster Recovery en Microsoft Azure, consulte "Disaster Recovery para Microsoft Azure" (p. 1106).

Disaster Recovery para Cyber Protect Cloud

Disaster Recovery para Cyber Protect Cloud tiene las siguientes características:

- La ubicación del sitio de DR es Cyber Protect Cloud.
- Las copias de seguridad (puntos de recuperación) de los servidores protegidos se almacenan en Cyber Protect Cloud.

La funcionalidad clave

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

© Acronis International GmbH, 2003-2025

- Gestionar el servicio Disaster Recovery desde una única consola
- Ampliar hasta 23 redes locales a la nube mediante un túnel VPN seguro
- Establecer la conexión al sitio en la nube sin necesidad de implementar dispositivos VPN[1] (el modo solo en la nube)
- Establecer la conexión de punto a sitio en sus sitios locales[2] y en la nube
- Proteger su equipo con el uso de servidores de recuperación[3] en la nube
- Proteger aplicaciones y dispositivos con el uso de servidores principales[4] en la nube
- Realizar operaciones de recuperación ante desastres automáticas para copias de seguridad cifradas
- Realizar una prueba de conmutación por error en la red aislada
- Utilice runbooks para automatizar el despliegue en el entorno de producción en la nube

Requisitos de software para Disaster Recovery para Cyber Protect Cloud

Sistemas operativos compatibles

La protección con un servidor de recuperación se ha probado para los siguientes sistemas operativos:

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 18.04, 20.x, 21.x, 22.04, 22.10
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

---

[1][Disaster Recovery] Un equipo virtual especial que permite la conexión entre la red local y el sitio en la nube mediante un túnel de VPN seguro. El dispositivo VPN se implementa en el sitio local.
[2][Disaster Recovery] La infraestructura local implementada en las instalaciones de su empresa.
[3][Disaster Recovery] Una réplica en equipo virtual del equipo original basada en las copias de seguridad del servidor protegido almacenadas en la nube. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.
[4][Disaster Recovery] Un equipo virtual que no tiene un equipo enlazado en el sitio local (como un servidor de recuperación). Los servidores principales se utilizan para proteger una aplicación o para ejecutar varios servicios auxiliares (como un servidor web).

© Acronis International GmbH, 2003-2025

- AlmaLinux 8.x, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5
- Rocky Linux 9.x, 8.x

Es posible que este software funcione con otros sistemas operativos de Windows y distribuciones Linux, pero no se lo podemos asegurar.

Nota
La protección con un servidor de recuperación se ha probado para máquinas virtuales de Microsoft Azure con los siguientes sistemas operativos:

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- Servidor Ubuntu 20.04 LTS - 2.ª generación (canónico). Para obtener más información sobre el acceso a la consola del servidor de recuperación, consulte este artículo de la base de conocimientos.

Plataformas de virtualización compatibles

La protección de equipos virtuales con un servidor de recuperación se ha probado para las siguientes plataformas de virtualización:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Máquinas virtuales basadas en Kernel (KVM): solo invitados completamente virtualizados (HVM). No se admiten invitados paravirtualizados (PV).
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Nutanix Acropolis Hypervisor (AHV) con Sistema Operativo Nutanix Acropolis (AOS): 6.5, 6.6, 6.7, 6.8, 6.10

El dispositivo VPN se ha probado para las siguientes plataformas de virtualización:

© Acronis International GmbH, 2003-2025

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Se admite las cargas de trabajo de Linux que tienen copias de seguridad sin agente desde un SO invitado y tienen volúmenes con las configuraciones de Logical Volume Manager (LVM).

Se admite las cargas de trabajo de Windows que tienen copias de seguridad sin agente desde un SO invitado y tienen configuraciones de discos dinámicos (LDM).

Puede que este software funcione con otras plataformas de virtualización y versiones, pero no se lo podemos asegurar.

Limitaciones

Las siguientes plataformas y configuraciones no son compatibles con Disaster Recovery:

1. Plataformas no compatibles:
   - Agentes para Virtuozzo.
   - macOS
   - Los sistemas operativos de los equipos de escritorio Windows no son compatibles con las condiciones de los productos de Microsoft.
   - Windows Server Azure Edition

     Azure Edition es una versión especial de Windows Server que fue creada específicamente para ejecutarse ya sea como una máquina virtual (MV) de Azure IaaS en Azure o como una máquina virtual en un clúster de Azure Stack HCI. A diferencia de las ediciones Standard y Datacenter, Azure Edition no tiene licencia para ejecutarse en hardware sin sistema operativo, Hyper-V de cliente de Windows, Hyper-V de Windows Server, hipervisores de terceros o nubes de terceros.
2. Configuraciones no compatibles:

   Microsoft Windows
   - Los sistemas operativos de los equipos de escritorio Windows no son compatibles (debido a las condiciones de los productos de Microsoft).
   - El servicio de Active Directory no es compatible con la replicación FRS.
   - Los dispositivos extraíbles sin formateo GPT o MBR (también llamado "superfloppy") no son compatibles.

   Linux

© Acronis International GmbH, 2003-2025

- Sistemas de archivos sin tabla de partición.
- Cargas de trabajo de Linux de las que se realiza una copia de seguridad con un agente de desde un SO invitado y que tienen volúmenes con las siguientes configuraciones avanzadas de Logical Volume Manager (LVM): Volúmenes segmentados, volúmenes replicados o volúmenes RAID 0, RAID 4, RAID 5, RAID 6 o RAID 10.

Nota
Las cargas de trabajo con varios sistemas operativos instalados no son compatibles.

3. Modos de inquilino no compatibles:
   - La recuperación ante desastres no está disponible cuando el modo de cumplimiento está habilitado para el inquilino.
4. Tipos de copias de seguridad no compatibles:
   - Los puntos de recuperación de Protección continua de datos (CDP) no son compatibles.

     Importante
     Si crea un servidor de recuperación a partir de una copia de seguridad que tenga un punto de recuperación CDP, perderá los datos incluidos en este punto de recuperación durante la conmutación por recuperación o al crear una copia de seguridad de un servidor de recuperación.

   - Las copias de seguridad de datos forenses no se pueden usar para crear servidores de recuperación.

Un servidor de recuperación tiene una interfaz de red. Si el equipo original tiene varias interfaces de red, solo se emula una.

Los servidores en la cloud no se cifran.

Producto de prueba de Disaster Recovery

Puede utilizar una versión de prueba de Acronis Disaster Recovery durante un período de 30 días. En este caso, Disaster Recovery tiene las siguientes limitaciones para los inquilinos de los partners:

- Sin acceso a Internet público para la recuperación y los servidores principales. No puede asignar direcciones IP públicas a los servidores.
- La VPN multisitio IPsec no está disponible.

Operaciones con máquinas virtuales de Microsoft Azure

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

© Acronis International GmbH, 2003-2025

Puede ejecutar la conmutación por error de las máquinas virtuales de Microsoft Azure para Acronis Cyber Protect Cloud. Para obtener más información, consulte "Realización de una conmutación por error" (p. 1083).

Después, puede realizar la conmutación tras recuperación desde Acronis Cyber Protect Cloud de vuelta a las máquinas virtuales de Azure. Para obtener más información, consulte Conmutación tras recuperación desde Cyber Protect Cloud a una máquina virtual de Azure.

Puede configurar una conectividad VPN multisitio IPsec entre Acronis Cyber Protect Cloud y la puerta de enlace VPN de Azure. Para obtener más información, consulte "Configuración de VPN de IPsec de varios sitios" (p. 1036).

Limitaciones al usar el almacenamiento en la nube con redundancia geográfica

El almacenamiento en la nube con redundancia geográfica proporciona una ubicación secundaria para los datos de copias de seguridad. La ubicación secundaria es una región geográficamente distinta a la ubicación de almacenamiento primaria. La separación geográfica de las regiones garantiza que, en caso de que se produzca un desastre que afecte a una de las regiones e impida que se recuperen los datos de copias de seguridad, la otra región no se verá afectada y no se interrumpirán las operaciones.

Importante
El servicio de Disaster Recovery no se puede utilizar si se cambia la ubicación primaria de almacenamiento de copia de seguridad por una secundaria con redundancia geográfica.

Eliminación automática de entornos de clientes que no se usan en el sitio en la nube

El servicio de Disaster Recovery realiza el seguimiento del uso de entornos de cliente creados para la recuperación ante desastres y los elimina automáticamente si no se utilizan.

Los siguientes criterios se utilizan para definir si un inquilino cliente está activo:

- Actualmente, hay al menos un servidor en la nube o ha habido algún servidor en la nube en los últimos siete días.

  O

- La opción **Acceso mediante VPN al sitio local** está habilitada y, o bien se ha establecido el túnel OpenVPN de sitio a sitio, o bien se han reportado datos desde el dispositivo VPN en los últimos 7 días.

El resto de inquilinos se considera inquilinos inactivos. El sistema realiza lo siguiente para estos inquilinos:

- Se elimina la puerta de enlace de VPN, así como todos los recursos en la nube relacionados con el inquilino.

© Acronis International GmbH, 2003-2025

- Se elimina el registro del dispositivo VPN.

Los inquilinos inactivos se restauran al estado en el que no se había configurado la conectividad.

Trabajo con Disaster Recovery a Cyber Protect Cloud

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

El flujo de trabajo básico para utilizar la recuperación ante desastres es el siguiente:

1. Cree un servidor de recuperación de la carga de trabajo que desee proteger de una de las siguientes maneras:
   - a. Cree un plan de protección que incluya el módulo de **recuperación ante desastres** y el módulo de **copia de seguridad** con la configuración **Qué copiar** establecida en **Todo el equipo** o **Sistema y volúmenes de arranque**.
     b. Aplique el plan a sus dispositivos. Esto configurará automáticamente la infraestructura de recuperación ante desastres predeterminada. Para obtener más información, consulte Crear un plan de protección de recuperación ante desastres.

     Nota
     Los administradores de unidades no pueden crear, modificar ni aplicar planes de protección de recuperación ante desastres.
   - Configure la infraestructura en la nube de recuperación ante desastres manualmente y controle cada paso. Consulte "Creación de un servidor de recuperación" (p. 1062).
2. Configure la conectividad con el sitio en la nube.
   - Modo solo en la nube
   - Conexión OpenVPN de sitio a sitio
   - Conexión VPN de IPsec de varios sitios
   - Conexión de punto a sitio
3. Configure la conmutación por error de prueba automatizada.
4. Ejecute una prueba de conmutación por error.
5. [Si ocurre un desastre] Realice una conmutación por error de producción.
6. [Después del desastre] Realice una conmutación tras recuperación al sitio local.
7. [Opcional] Configurar runbooks.

Creación de un plan de protección de recuperación ante desastres

El plan de protección de recuperación ante desastres es un plan de protección en el que el módulo **Recuperación ante desastres** está habilitado.

© Acronis International GmbH, 2003-2025

Al habilitar la función de recuperación ante desastres y aplicar el plan a sus dispositivos, automáticamente se crea la infraestructura de red en la nube (sitio en la nube). Para obtener más información, consulte "Infraestructura de red en la nube predeterminada" (p. 1019).

Nota

- Al aplicar un plan de protección de recuperación ante desastres, se crea la infraestructura de red en la nube de recuperación únicamente en el caso de que no exista. Las redes existentes en la nube no se cambian ni se vuelven a crear.
- Después de configurar la recuperación ante desastres podrá realizar una prueba o la conmutación por error de producción desde cualquier punto de recuperación generado después de la creación del servidor de recuperación del dispositivo. Los puntos de recuperación (copias de seguridad) que se generaron antes de que el dispositivo estuviese protegido con la recuperación ante desastres (antes de crear el servidor de recuperación) no se pueden usar para la conmutación por error.
- No se puede habilitar un plan de protección para la recuperación ante desastres si no se puede detectar la dirección IP de un dispositivo. Por ejemplo, cuando se realizan copias de seguridad sin agente de máquinas virtuales y no se les asigna una dirección IP.
- Cuando aplica un plan de protección, se asignan las mismas redes y direcciones IP al sitio en la nube. La conectividad VPN de IPsec requiere que los segmentos de red en la nube y los sitios locales no se superpongan. Si se configura una conectividad VPN de IPsec de varios sitios y, a continuación, aplica un plan de protección a uno o varios dispositivos, debe actualizar de forma adicional las redes en la nube y reasignar las direcciones IP de los servidores en la nube. Para obtener más información, consulte "Reasignación de direcciones IP" (p. 1055).

Para crear un plan de protección de recuperación ante desastres

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione los equipos que quiera proteger.
3. Haga clic en **Proteger** y, a continuación, en **Crear plan**.
   Se abre la configuración predeterminada del plan de protección.
4. Configure las opciones de copia de seguridad.
   Para usar la funcionalidad de recuperación ante desastres, el plan debe realizar copias de seguridad de todo el equipo o solo de los discos. Estas son necesarias para arrancar y proporcionar los servicios necesarios a un almacenamiento en la nube.
5. Active el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Recuperación ante desastres**.
6. En el campo **Ubicación**, seleccione dónde crear la infraestructura de recuperación ante desastres.
7. Haga clic en **Crear**.
   El plan se crea y se aplica a los equipos seleccionados. Se crea la infraestructura de red predeterminada y los servidores de recuperación con parámetros predeterminados. Para obtener más información, consulte "Edición de la configuración predeterminada de un servidor de recuperación" (p. 1018) y "Infraestructura de red en la nube predeterminada" (p. 1019).

© Acronis International GmbH, 2003-2025

Qué hacer a continuación

- Puede editar la configuración predeterminada del servidor de recuperación. Para obtener más información, consulte "Edición de la configuración predeterminada de un servidor de recuperación" (p. 1018).
- Puede editar la configuración predeterminada del servidor de red. Para obtener más información, consulte "Conectividad y redes" (p. 1020).

Edición de la configuración predeterminada de un servidor de recuperación

Cuando cree y aplique un plan de protección de recuperación ante desastres, se creará un servidor de recuperación con la configuración predeterminada. Puede editar esta configuración predeterminada cuando sea necesario.

El siguiente procedimiento se aplica a los servidores de recuperación que se encuentran en Cyber Protect Cloud. Si desea configurar los ajustes de un servidor de recuperación que está ubicado en Microsoft Azure, siga los pasos que se describen en "Creación de servidores de recuperación en Microsoft Azure" (p. 1122).

Nota
Se crea un servidor de recuperación únicamente en caso de que no exista. Los servidores de recuperación que ya existan no se cambian ni se vuelven a crear.

Pasos para editar la configuración predeterminada del servidor de recuperación

1. Vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un dispositivo y haga clic en **Recuperación ante desastres**.
3. Pasos para editar la configuración predeterminada del servidor de recuperación.
   La configuración del servidor de recuperación se describe en la siguiente tabla.

Configuración	Valor predeterminado	Descripción
CPU y RAM	automático	El número de CPU virtuales y la cantidad de RAM del servidor de recuperación. La configuración predeterminada se determinará automáticamente según la configuración de la CPU y la RAM del dispositivo original.
Red en la nube	automático	Red en la nube a la que se conectará el servidor. Para obtener datos sobre cómo se configuran las redes en la nube, consulte Infraestructura de red en la nube.
Dirección IP en la red de producción	automático	Dirección IP que tendrá el servidor en la red productiva. La dirección IP del equipo original se establece de forma predeterminada.

© Acronis International GmbH, 2003-2025

Dirección IP de prueba	inválido	La dirección IP de prueba le permitirá probar una conmutación por error en la red de prueba aislada y conectarse al servidor de recuperación mediante escritorio remoto o SSH durante una prueba de conmutación por error. En el modo de prueba de conmutación por error, la puerta de enlace de VPN sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT. La dirección IP de prueba no aparece especificada. La consola será la única forma de acceder al servidor durante una conmutación por error de prueba.
Acceso a Internet	habilitado	Habilite el servidor de recuperación para acceder a Internet durante una conmutación por error de prueba o real. De forma predeterminada, el puerto TCP 25 está denegado para las conexiones de salida.
Usar dirección pública	inválido	El hecho de que el servidor de recuperación cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet durante una conmutación por error de prueba o real. Si no usa una dirección IP pública, el servidor solo estará disponible en su red productiva. Para usar una dirección IP pública, debe habilitar el acceso a Internet. La dirección IP pública se mostrara cuando finalice la configuración. De forma predeterminada, el puerto TCP 443 está abierto para las conexiones de entrada.
Establecer el umbral de RPO	inválido	El umbral de RPO determina el intervalo temporal máximo permitido entre el último punto de recuperación y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.

Infraestructura de red en la nube predeterminada

La infraestructura de red en la nube que se crea automáticamente cuando aplica un plan de protección de recuperación ante desastres a recursos informáticos consta de los siguientes componentes:

- Un servidor de recuperación para cada dispositivo protegido.

  El servidor de recuperación es una máquina virtual en la nube que constituye una copia del dispositivo seleccionado.

  Para cada uno de los dispositivos seleccionados se crea un servidor de recuperación con la configuración predeterminada en el estado **En espera** (máquina virtual que no está en

© Acronis International GmbH, 2003-2025

ejecución). El tamaño del servidor de recuperación se ajusta automáticamente según la CPU y la RAM del dispositivo protegido.
- Puerta de enlace VPN en el sitio de la nube.
- Redes en la nube a las que están conectados los servidores de recuperación.

El sistema comprueba la dirección IP de cada dispositivo y crea automáticamente redes en la nube adecuadas si no hay redes en la nube a las que se pueda adaptar una dirección IP. Si ya ha tiene redes en la nube existentes a las que se puedan adaptar las direcciones IP de los servidores de recuperación, las redes en la nube existentes no cambiarán ni se volverán a crear.

- Si no tiene ninguna red en la nube o ha configurado los ajustes de la recuperación ante desastres por primera vez, la entidad IANA configurará las redes en la nube con rangos máximos recomendados para uso privado (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) según el rango de direcciones IP de su dispositivo. Puede editar la máscara de red para reducir su red.
- Si tiene dispositivos en varias redes locales, la red del sitio en la nube puede convertirse en un superconjunto de redes locales. Puede volver a configurar las redes en la sección **Conectividad**. Consulte "Gestión de redes para OpenVPN de sitio a sitio" (p. 1029).
- Si tiene que configurar la conectividad OpenVPN de sitio a sitio, descargue el dispositivo VPN y configúrelo. Consulte "Requisitos del sistema" (p. 1026). Asegúrese de que los rangos de las redes en la nube coinciden con los de sus redes locales conectadas al dispositivo VPN.
- Para cambiar la configuración de red predeterminada, vaya a **Disaster Recovery** > **Conectividad**, o en el módulo **Recuperación ante desastres** del plan de protección, haga clic en **Ir a conectividad**.

Si revoca, elimina o desconecta el módulo **Recuperación ante desastres** de un plan de protección, los servidores de recuperación y las redes en la nube no se eliminarán automáticamente. Puede eliminar la infraestructura de recuperación ante desastres manualmente, en caso necesario.

Conectividad y redes

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Disaster Recovery le permite definir los siguientes tipos de conectividad al sitio en la nube:

- **Modo solo en la nube**

  Este tipo de conexión no requiere la implementación de un dispositivo VPN en el sitio local.

  Las redes locales y en el cloud son independientes. Este tipo de conexión implica la conmutación por error de todos los servidores protegidos del sitio local o bien la conmutación por error parcial de los servidores independientes que no necesitan comunicarse con el sitio local.

  Los servidores en el cloud en el sitio en el cloud son accesibles a través de VPN de punto a sitio y de direcciones IP públicas (si están asignadas).
- **Conexión OpenVPN de sitio a sitio**

© Acronis International GmbH, 2003-2025

Este tipo de conexión requiere la implementación de un dispositivo VPN en el sitio local.

La conexión de OpenVPN de sitio a sitio le permite extender sus redes a la nube y conservar las direcciones IP.

Su sitio local se conecta al sitio en el cloud por medio de un túnel VPN seguro. Este tipo de conexión es adecuado en caso de que sus servidores dependan en gran medida del sitio local, como puede suceder con un servidor web o un servidor de bases de datos. En caso de una conmutación por error parcial, al recrear uno de estos servidores en el sitio en el cloud mientras el otro se queda en el sitio local, podrán seguir comunicándose mediante un túnel VPN.

Los servidores en el cloud en el sitio en el cloud son accesibles a través de la red local, de VPN de punto a sitio y de direcciones IP públicas (si están asignadas).

- **Conexión VPN de IPsec de varios sitios**

  Este tipo de conexión requiere un dispositivo VPN local compatible con IPsec IKE v2.

  Cuando inicie la configuración de la conexión VPN de IPsec de varios sitios, Disaster Recovery creará automáticamente una puerta de enlace de Cloud VPN con una dirección IP pública.

  Con la VPN de IPsec de varios sitios, sus sitios locales se conectan al sitio en la nube por medio de un túnel VPN de IPsec seguro.

  Este tipo de conexión es adecuada para los escenarios de Disaster Recovery cuando tiene uno o varios sitios locales que alojan cargas de trabajo críticas o servicios estrechamente dependientes.

  En caso de una conmutación por error parcial de uno de los servidores, se recreará dicho servidor en el sitio en la nube mientras que el resto se mantendrán en el sitio local, por lo que podrán seguir comunicándose mediante un túnel VPN de IPsec.

  En caso de una conmutación por error parcial de uno de los sitios locales, el resto seguirá operativo, por lo que podrán seguir comunicándose mediante un túnel VPN de IPsec.

- **Acceso de VPN remoto de punto a sitio**

  Un acceso remoto y seguro de la VPN de punto a sitio a sus cargas de trabajo de sitio local y en la nube desde fuera mediante su dispositivo de punto final.

  Para el acceso en un sitio local, este tipo de conexión requiere la implementación de un dispositivo VPN en el sitio local.

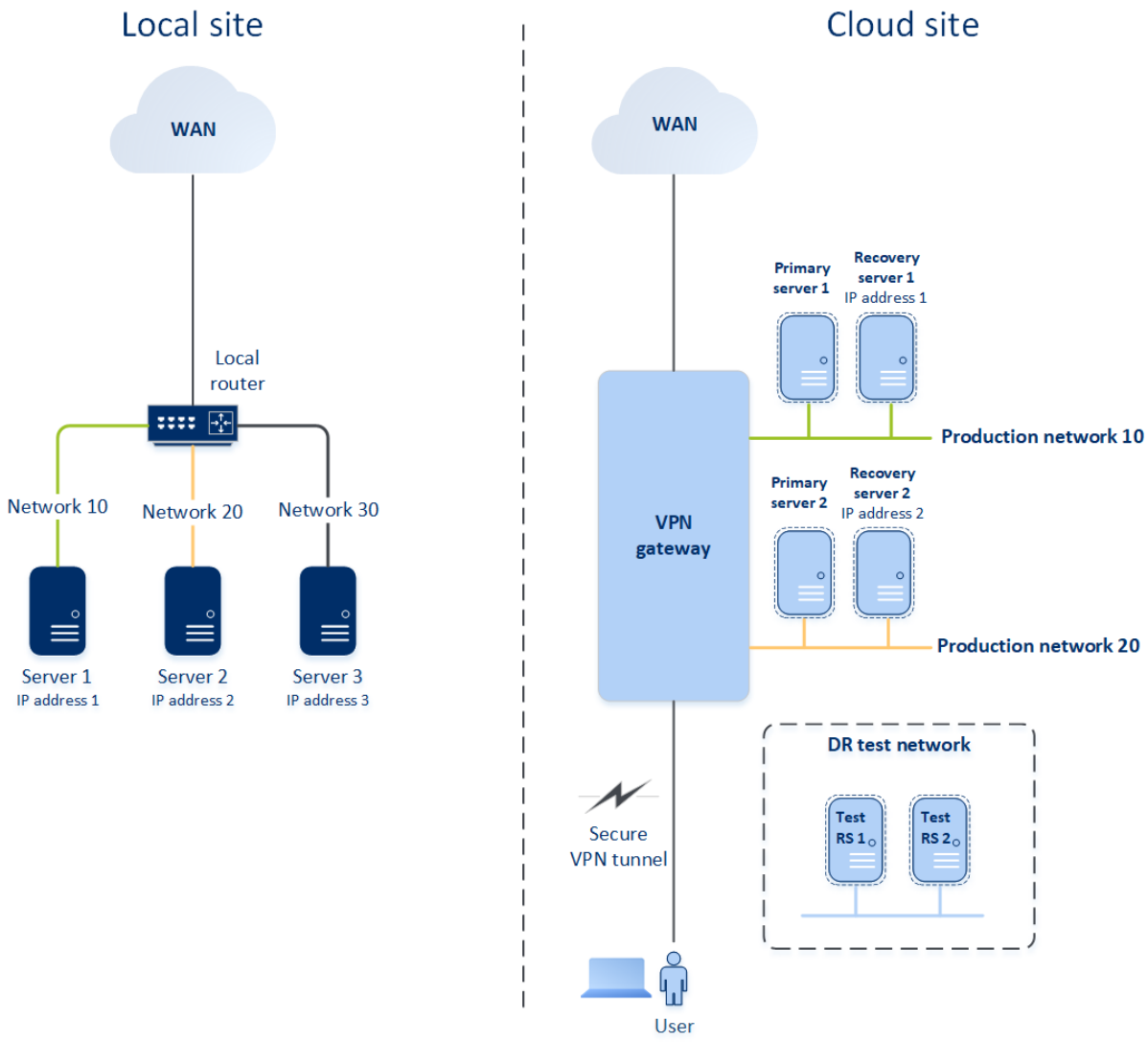
Modo solo en la nube

El modo solo en el cloud no requiere la implementación de un dispositivo VPN en el sitio local. Implica que tiene dos redes independientes: una en el sitio local y otra en el sitio en el cloud. La enrutación se realiza con el enrutador en el sitio de la nube.

Cómo funciona el enrutamiento

Si se establece el modo solo en la nube, el enrutamiento se realiza con el enrutador en el sitio de la nube, de forma que los servidores de diferentes redes en la nube puedan comunicarse entre ellos.

© Acronis International GmbH, 2003-2025



Configuración del modo solo en la nube

El modo "Solo en la nube" es el tipo de conectividad predeterminado que se crea automáticamente cuando aplica un plan de recuperación ante desastres a un recurso informático.

Para configurar una conexión en el modo "Solo en la nube"

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Seleccione **Solo en la nube** y haga clic en **Configurar**.
   Como resultado, la puerta de enlace de VPN y la red de la nube con la dirección y la máscara definidas se despliegan en el sitio en la nube.

Gestión de redes en el modo Solo en la nube

Puede añadir y gestionar hasta 23 redes en la nube.

Añadir red

Para agregar una nueva red al cloud:

© Acronis International GmbH, 2003-2025

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. En el **Sitio en la nube**, pulse **Añadir red en la nube**.
3. Defina los parámetros de red en la nube: la máscara y dirección de red, y haga clic en **Listo**.

Como resultado, la red en la nube adicional se creará en el sitio de la nube con la máscara y la dirección definidas.

Eliminar red

Requisitos previos

Se eliminarán todos los servidores de nube de la red que desea eliminar.

Para eliminar una red en la nube

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. En **Sitio en el cloud**, haga clic en la dirección de red que desea eliminar.
3. Haga clic en **Eliminar** y confirme la operación.

Cambiar parámetros

Para cambiar los parámetros de la red en el cloud:

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. En **Sitio en el cloud**, haga clic en la dirección de red que desea editar.
3. Haga clic en **Editar**.
4. Defina la máscara y dirección de red y haga clic en **Listo**.

Conexión OpenVPN de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

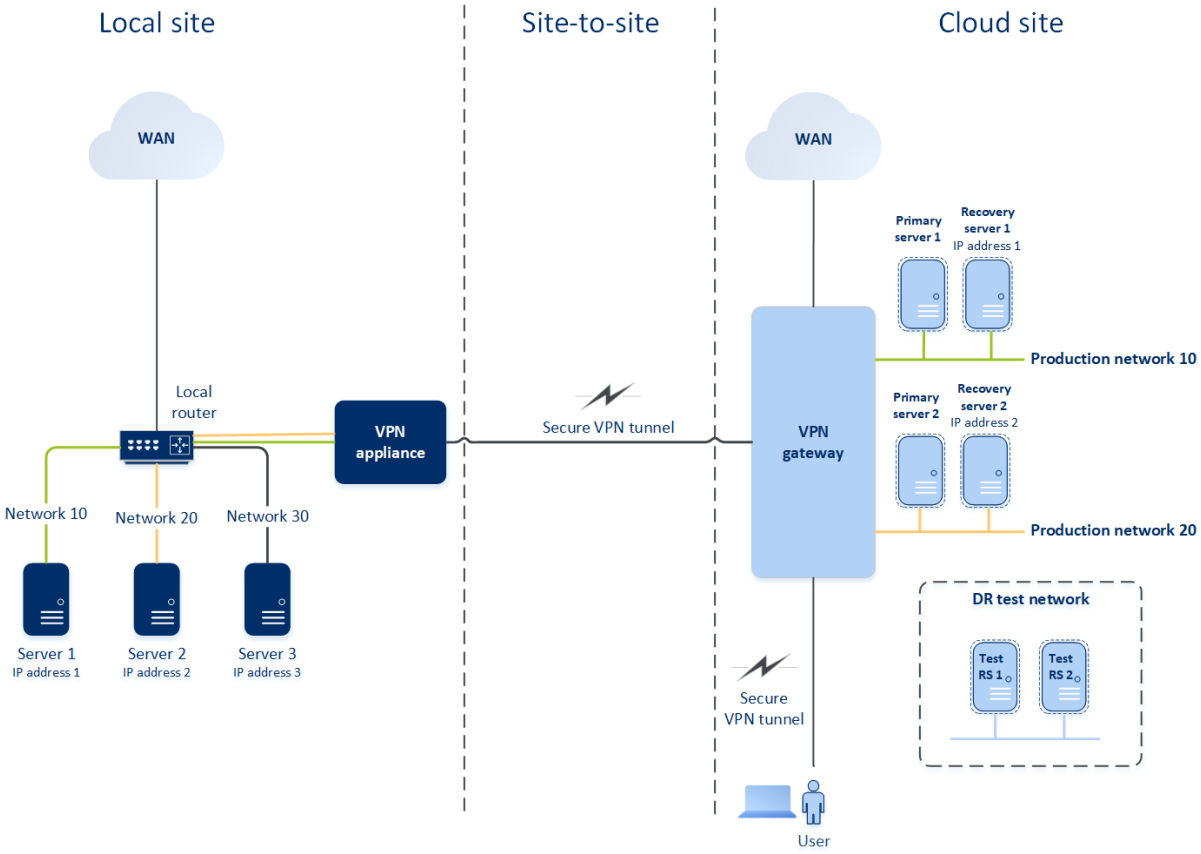
Para entender cómo funcionan las redes en Disaster Recovery, pensaremos en un caso en el que tiene tres redes, cada una con un equipo en el sitio local. Va a configurar la protección frente a desastres para dos redes, Red 10 y Red 20.

En el siguiente diagrama, puede ver el sitio local donde se alojan sus equipos y el sitio en la nube donde se inician los servidores en la nube en caso de desastre.

La solución Disaster Recovery le permite realizar una conmutación por error de toda la carga de trabajo de los equipos dañados en el sitio local a los servidores de nube que se encuentran en la nube.

Puede añadir y gestionar hasta 23 redes en la nube.

© Acronis International GmbH, 2003-2025



Para establecer una conectividad OpenVPN de sitio a sitio entre el sitio local y el sitio en la nube, se usa un **dispositivo VPN** y una **puerta de enlace de VPN**.

Cuando comience a configurar la conexión OpenVPN de sitio a sitio en la consola de Cyber Protect, se desplegará automáticamente la puerta de enlace de VPN en el sitio de la nube.

Después del despliegue de la puerta de enlace de VPN, debe hacer lo siguiente:

- Despliegue el dispositivo VPN en su sitio local.
- Añada las redes que desee proteger.
- Registre el dispositivo VPN en la nube.

Disaster Recovery creará una réplica de su red local en la nube. Se establecerá un túnel VPN seguro entre el dispositivo VPN y la puerta de enlace VPN. Este túnel VPN proporcionará la extensión de su red local a la nube. Las redes de producción en la nube se conectarán con sus redes locales. Los servidores locales y de nube se comunicarán a través de este túnel VPN como si estuvieran en el mismo segmento de Ethernet. El enrutamiento se realizará a través de su router local.

Para que cada equipo de origen quede protegido, debe crear un servidor de recuperación en el sitio en la nube. Se queda en estado **En espera** hasta que ocurre un evento de conmutación por error. Si sucede un desastre e inicia un proceso de conmutación por error (en el **modo de producción**), el servidor de recuperación que representa la copia exacta de su equipo protegido se inicia en la nube. Puede tener la misma dirección IP asignada que el equipo de origen e iniciarse en el mismo

© Acronis International GmbH, 2003-2025

segmento de Ethernet. Sus clientes pueden seguir trabajando con el servidor sin notar ningún cambio en segundo plano.

También puede iniciar un proceso de conmutación por error en el **modo de prueba**. Esto quiere decir que el equipo de origen continúa funcionando y, al mismo tiempo, se inicia en la nube el servidor de recuperación correspondiente con la misma dirección IP. Para evitar conflictos debido a la dirección IP, se crea una red virtual especial en la nube, la **red de prueba**. La red de prueba se aísla para evitar que se duplique la dirección IP del equipo de origen en un segmento de Ethernet. Para acceder al servidor de recuperación en el modo de prueba de conmutación por error, debe asignar la **Dirección IP de prueba** al servidor de recuperación al crearlo. Se pueden especificar otros parámetros para el servidor de recuperación que también puede configurar.

Cómo funciona el enrutamiento

Cuando se establece una conexión de sitio a sitio, el enrutamiento entre redes en la nube se realiza con su enrutador local. El servidor VPN no lleva a cabo enrutamientos entre los servidores en la nube localizados en diferentes redes. Si un servidor de nube de una red quiere comunicarse con un servidor de otra red en la nube, el tráfico pasará a través del túnel VPN del enrutador local del sitio local. Después, el enrutador local lo enruta hacia otra red y vuelve a través del túnel al servidor de destino del sitio en la nube.

Puerta de enlace de VPN

Un componente importante que permite la comunicación entre los sitios locales y en la nube es la puerta de enlace del VPN. Es una máquina virtual en la nube en el que está instalado software especial y la red se configura de forma específica. La puerta de enlace del VPN realiza las siguientes funciones:

- Conecta los segmentos de Ethernet de su red local y de producción en la nube en el modo L2.
- Proporciona reglas de tablas de IP y EB.
- Funciona como enrutador y NAT predeterminados para los equipos en las redes de prueba y producción.
- Funciona como servidor DHCP. Todos los equipos en las redes de producción y prueba obtienen la configuración de red (direcciones IP, configuración del DNS) por medio de DHCP. Un servidor en la nube obtendrá cada vez la misma dirección IP del servidor DHCP. Si necesita establecer la configuración de DNS personalizada, póngase en contacto con el equipo de soporte técnico.
- Funciona como DNS para almacenar archivos en la memoria caché.

Configuración de red de la puerta de enlace de VPN

La puerta de enlace de VPN tiene varias interfaces de red:

- Interfaz externa, conectada a Internet.
- Interfaces de producción, conectadas a las redes de producción.
- Interfaz de prueba, conectada a la red de prueba.

© Acronis International GmbH, 2003-2025

Además, se añaden dos interfaces virtuales para las conexiones de punto a sitio y de sitio a sitio.

Cuando se implementa e inicializa la puerta de enlace de VPN, se crean los puentes: uno para la interfaz externa y otro para las interfaces de cliente y producción. Aunque el puente entre cliente y producción y la interfaz de prueba usen las mismas direcciones IP, la puerta de enlace de VPN puede enrutar paquetes correctamente mediante una técnica específica.

Dispositivo VPN

El **dispositivo VPN** es una máquina virtual en el sitio local en el que se instala Linux, software especial y una configuración de red especial. Permite la comunicación entre los sitios local y en la nube.

Habilitación de la conectividad de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede habilitar la conectividad de sitio a sitio en los siguientes casos:

- Si necesita que los servidores en el cloud en el sitio en el cloud se comuniquen con los servidores en el sitio local.
- Si, después de una conmutación por error al cloud, la infraestructura local se recupera y quiere realizar una conmutación por recuperación de sus servidores al sitio local.

Para habilitar la conectividad de sitio a sitio

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades** y luego habilite la opción **Conexión de sitio a sitio**.

Como resultado, se habilita la conexión de sitio a sitio VPN entre los sitios local y en la nube. El servicio Disaster Recovery obtiene la configuración de red del dispositivo VPN y extiende las redes locales al sitio en la nube.

Configuración de OpenVPN de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Requisitos del dispositivo VPN

Requisitos del sistema

- 1 CPU
- 1 GB DE RAM

© Acronis International GmbH, 2003-2025

- 8 GB de espacio de disco

Puertos

- TCP 443 (salida): para conexión VPN
- TCP 80 (salida): para actualizar el dispositivo automáticamente

Asegúrese de que sus cortafuegos y otros componentes del sistema de seguridad de la red permiten las conexiones a través de estos puertos a cualquier dirección IP.

Configuración de una conexión OpenVPN de sitio a sitio

El dispositivo VPN amplía su red local a la nube mediante un túnel de VPN seguro. Este tipo de conexión se suele llamar conexión "de sitio a sitio" (S2S). Puede seguir el procedimiento siguiente o ver el tutorial en vídeo.

Para configurar una conexión mediante el dispositivo VPN

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Seleccione **Conexión OpenVPN de sitio a sitio** y haga clic en **Configurar**.
   El sistema empieza a implementar la puerta de enlace de VPN en la nube. Este procedimiento tardará un tiempo. mientras tanto, puede continuar con el siguiente paso.

   Nota
   La puerta de enlace de VPN se proporciona sin ningún cargo adicional. Se eliminará si la funcionalidad de Disaster Recovery no se usa, es decir, si no hay ningún servidor principal ni de recuperación en la nube durante siete días.

3. En el bloque **Dispositivo VPN**, pulse en **Descargar e implementar**. En función de la plataforma de virtualización que use, descargue el dispositivo VPN de VMware vSphere o Microsoft Hyper-V.
4. Implemente el dispositivo y conéctelo a las redes de producción.
   En vSphere, asegúrese de que esté activado el **modo Promiscuous** y **Transmisiones falsificadas** y establezca en **Aceptar** todos los conmutadores virtuales que conecten el dispositivo VPN a las redes de producción. Para acceder a esta configuración, en vSphere Client, seleccione el host > **Resumen** > **Red** y, a continuación, seleccione el conmutador > **Editar configuración...** > **Seguridad**.
   En Hyper-V, cree un equipo virtual de **1.ª generación** con 1024 MB de memoria. Asimismo, le recomendamos que habilite la **Memoria dinámica** para el equipo. Cuando haya creado el equipo, vaya a **Configuración** > **Hardware** > **Adaptador de red** > **Funciones avanzadas** y marque la casilla de verificación **Habilitar el redireccionamiento de direcciones MAC**.
5. Encienda el dispositivo.
6. Abra la consola del dispositivo e inicie sesión con el nombre de usuario y la contraseña "admin"/"admin".
7. [Opcional] Cambie la contraseña.

© Acronis International GmbH, 2003-2025

8. [Opcional] Cambie la configuración de red si así lo precisa. Defina la interfaz que se usará como WAN para la conexión a Internet.
9. Use las credenciales del administrador de la empresa para registrar el dispositivo en el servicio Cyber Protection.

   Estas credenciales solo se usan una vez para recuperar el certificado. La URL del centro de datos viene predefinida.

   Nota
   Si se ha configurado la autenticación de doble factor para su cuenta, también se le solicitará el código TOTP. Si se ha habilitado, pero no se ha configurado la autenticación de doble factor para su cuenta, no puede registrar el dispositivo VPN. Primero, debe ir a la página de inicio de sesión de la consola de Cyber Protect y completar la configuración de la autenticación de doble factor para su cuenta. Para obtener más información acerca de la autenticación de doble factor, vaya a la Guía del administrador del portal de gestión.

Cuando haya completado la configuración, el dispositivo mostrará el estado **En línea**. El dispositivo se conecta a la puerta de enlace de VPN y comienza a transmitir información sobre las redes de todas las interfaces activas al servicio Disaster Recovery. La consola de Cyber Protect muestra las interfaces basándose en la información del dispositivo VPN.

Gestión de la configuración del dispositivo VPN

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

En la pestaña **Disaster Recovery** > **Conectividad**, puede:

- Descargar archivos de registro.
- Cancelar el registro del dispositivo (si necesita restablecer la configuración del dispositivo VPN o cambiar al modo Solo en la nube).

Para acceder a esta configuración, haga clic en el icono **i** del bloque **Dispositivo VPN**.

En la consola del dispositivo VPN, puede hacer lo siguiente:

- Cambiar la contraseña del dispositivo.
- Ver o cambiar la configuración de red y definir la interfaz que utilizará como WAN para la conexión a Internet.
- Registrar la cuenta o cambiar su registro (repitiéndolo).
- Reiniciar el servicio VPN.
- Reiniciar el dispositivo VPN.
- Ejecutar el comando del shell de Linux (solo en casos avanzados de resolución de problemas).

© Acronis International GmbH, 2003-2025

Gestión de redes para OpenVPN de sitio a sitio

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

Puede añadir y gestionar hasta 23 redes en la nube.

Adición de redes

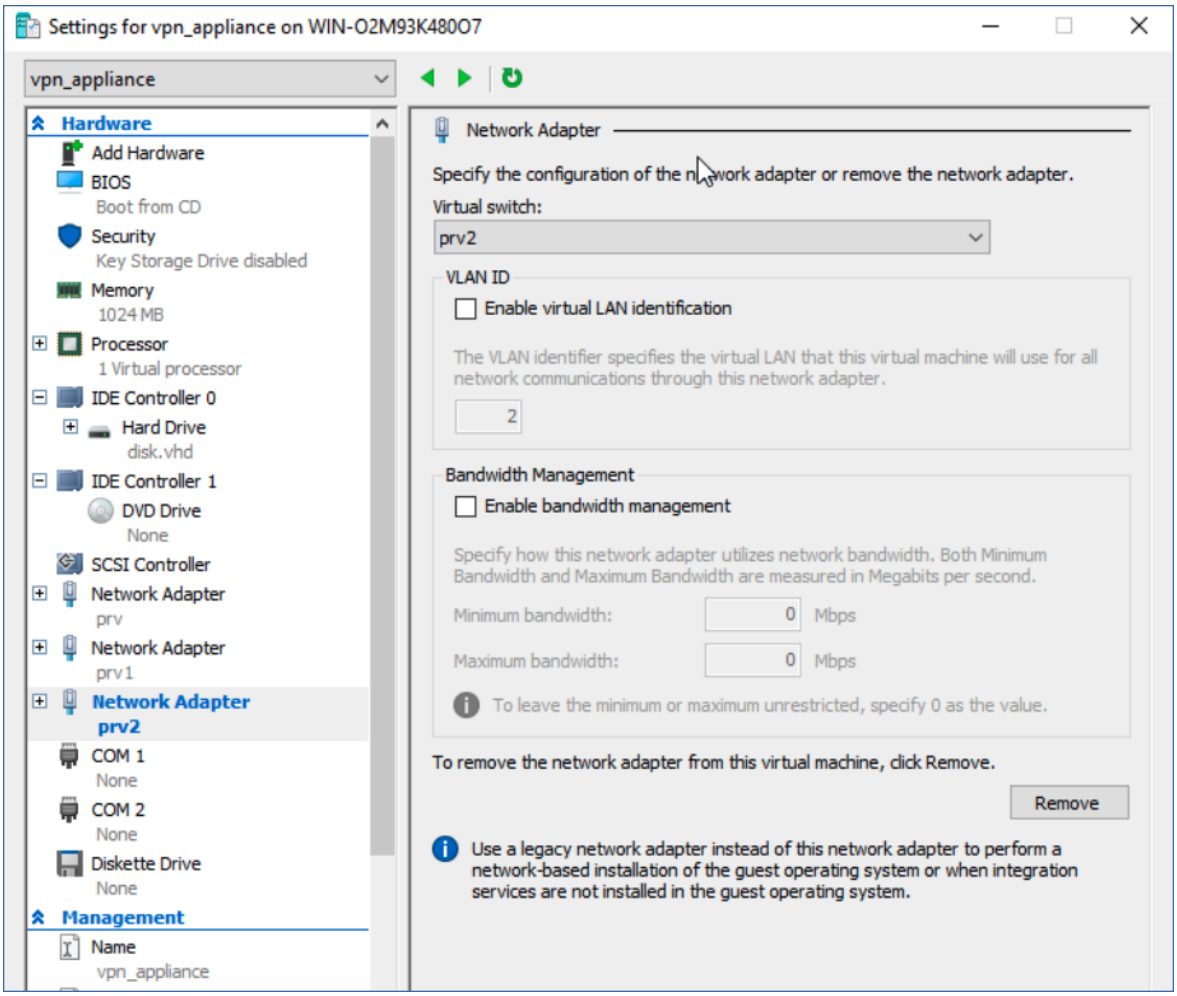
Requisitos previos

La conectividad Open VPN de sitio a sitio está configurada, según se indica en "Requisitos del sistema" (p. 1026).

Pasos para añadir una red en el sitio local y extenderla a la nube

1. En el dispositivo VPN, configure la nueva interfaz de red con la red local que desea extender al cloud.
2. [Opcional] Si desea añadir una o más redes, por cada red adicional, añada una interfaz de red virtual (adaptador de red) a la máquina virtual en la que se está ejecutando el dispositivo virtual.
   El siguiente ejemplo muestra cómo hacerlo en el caso de una máquina virtual que se está ejecutando en un hipervisor de Hyper-V.

© Acronis International GmbH, 2003-2025



Nota

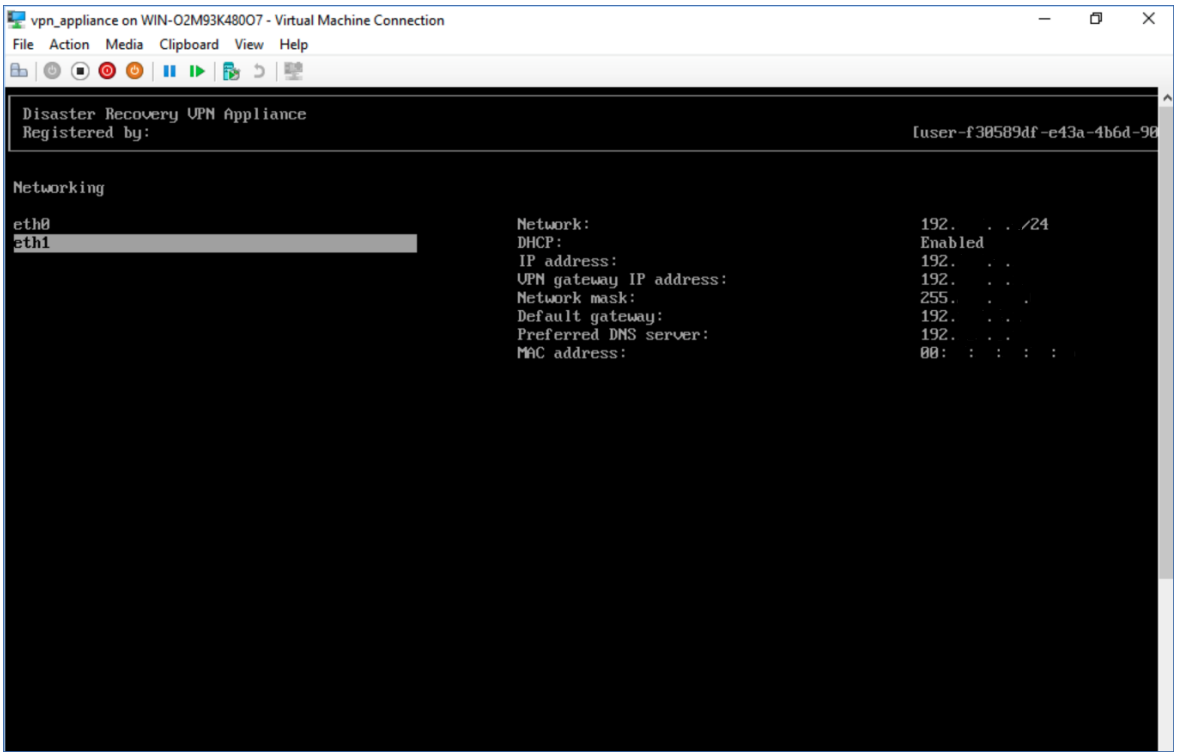
Los nuevos adaptadores de red virtuales deben configurarse con la red virtual local que desea extender a la nube.

3. Inicie sesión en la consola del dispositivo VPN y, a continuación, en la sección **Conexión a redes virtuales**, configure los ajuste de red para una de las interfaces (adaptadores).

Nota

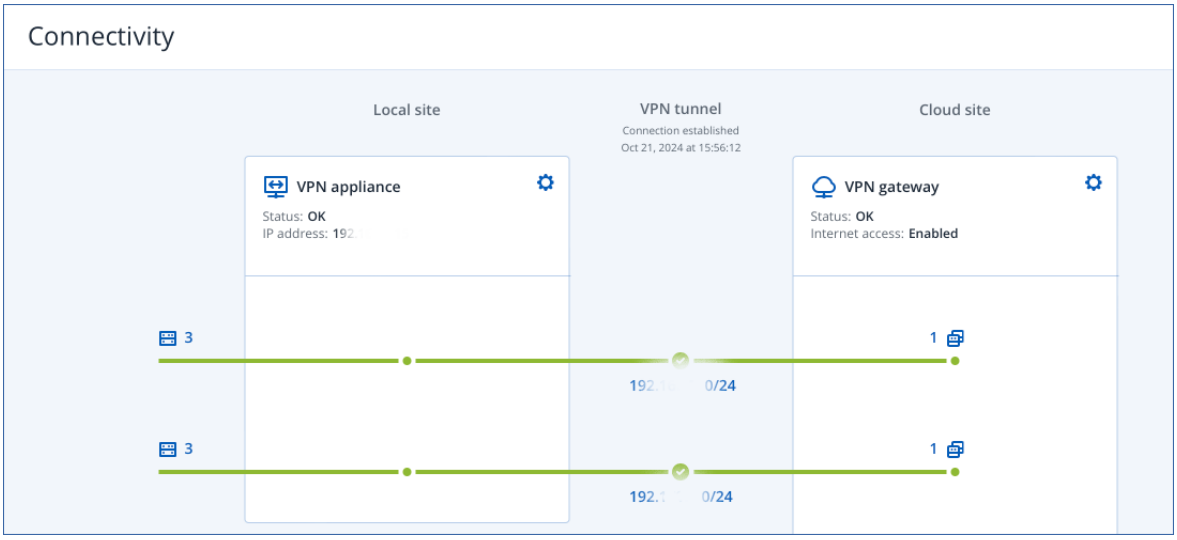
- La configuración de la dirección IP es obligatoria únicamente para una de las interfaces de red virtuales para habilitar el acceso a Internet. Puede omitir la configuración de la dirección IP para las otras interfaces de red.
- El modo promiscuo y las transmisiones falsificadas o suplantación de direcciones MAC deben estar habilitados para cada adaptador. Para obtener más información, consulte este artículo de la base de conocimientos.

© Acronis International GmbH, 2003-2025



El dispositivo VPN comienza automáticamente a transmitir información sobre las redes de todas las interfaces activas a Disaster Recovery.

4. Inicie sesión en la consola de Cyber Protect y vaya a **Recuperación ante desastres** > **Conectividad**.



Todas las redes locales se extienden automáticamente al sitio en la nube.

Eliminar red

Para eliminar una red extendida al cloud:

1. Inicie sesión en la consola del dispositivo VPN.
2. En la sección **Redes**, seleccione la interfaz que desea eliminar y haga clic en **Borrar**

© Acronis International GmbH, 2003-2025

configuración de red.

3. Confirme la operación.

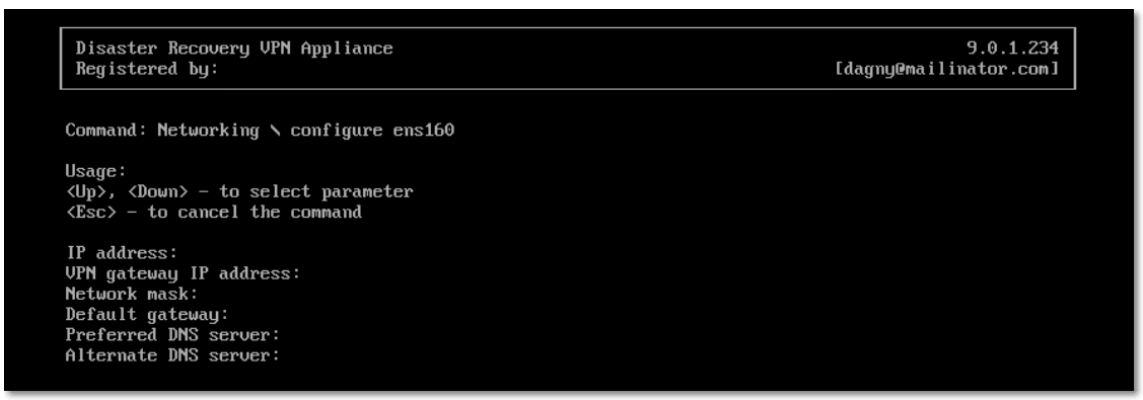
Como resultado, se detendrá la extensión de red local al la nube mediante un túnel de VPN seguro. Esta red funcionará como un segmento independiente de la nube. Si esta interfaz se usa para pasar el tráfico hacia o desde el sitio en el la nube, todas sus conexiones de red hacia o desde el sitio en la nube se desconectarán.

Cambiar parámetros

Para cambiar los parámetros de red:

1. Inicie sesión en la consola del dispositivo VPN.
2. En la sección **Redes**, seleccione la interfaz que desea editar.
3. Haga clic en **Editar configuración de red**.
4. Seleccione una de las opciones:
   - Para la configuración automática de la red mediante DHCP, haga clic en **Usar DHCP** y confirme la operación.
   - Para configurar la red manualmente, haga clic en **Establecer dirección IP estática**, establezca la configuración y, a continuación, haga clic en **Introducir**.

Configuración	Descripción
Dirección IP	Dirección IP de la interfaz en la red local.
Dirección IP de la puerta de enlace de VPN	Dirección IP especial que se reserva para el segmento en la nube de la red con el fin de que el servicio de Disaster Recovery funcione correctamente.
Máscara de red	Máscara de red de la red local.
Puerta de enlace predeterminada	Entrada predeterminada en el sitio local.
Servidor DNS preferido	Servidor DNS principal del sitio local.
Servidor DNS alternativo	Servidor DNS secundario del sitio local.



© Acronis International GmbH, 2003-2025

Permitir tráfico DHCP a través de VPN L2

Si los dispositivos de su sitio local obtienen su dirección IP de un servidor DHCP, puede proteger dicho servidor con Disaster Recovery, conmutarlo por error a la nube y, a continuación, permitir que el tráfico DHCP circule por una VPN L2. De este modo, su servidor DHCP se ejecutará en la nube, pero continuará asignando direcciones IP a sus dispositivos locales.

Requisitos previos

Se debe establecer un tipo de conectividad VPN L2 de sitio a sitio para el sitio en la nube.

Para permitir el tráfico DHCP a través de la conexión VPN L2

1. Vaya a **Disaster Recovery** > pestaña **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Habilite el conmutador **Permitir tráfico DHCP a través de VPN L2**.

Cambio de VPN de sitio a sitio OpenVPN a VPN IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede cambiar fácilmente de una conexión OpenVPN de sitio a sitio a una conexión VPN de IPsec de varios sitios y al contrario.

Cuando cambia el tipo de conectividad, las conexiones VPN activas se eliminan, pero la configuración de la red y de los servidores en la nube se conservan. Sin embargo, puede que necesite reasignar las direcciones IP de las redes y los servidores en la nube.

La siguiente tabla compara las características básicas de la conexión OpenVPN de sitio a sitio y la conexión VPN de IPsec de varios sitios.

	OpenVPN de sitio a sitio	**VPN de IPsec de varios sitios**
Soporte técnico del sitio local	Único	Único, múltiple
Modo de puerta de enlace de VPN	L2 Open VPN	L3 IPsec VPN
Segmentos de red	Amplía la red local a la red en la nube	Las redes locales y los segmentos de las redes en la nube no deben superponerse
Compatible con el acceso de punto a sitio al sitio local	Sí	No

© Acronis International GmbH, 2003-2025

	OpenVPN de sitio a sitio	VPN de IPsec de varios sitios
Compatible con el acceso de punto a sitio al sitio en la nube	Sí	Sí
Requiere un elemento de oferta de IP pública	No	Sí

Para cambiar de una conexión OpenVPN de sitio a sitio a una conexión VPN de IPsec de varios sitios

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Cambiar a VPN de IPsec de varios sitios**.
4. Haga clic en **Reconfigurar**.
5. Reasigne las direcciones IP de la red y los servidores en la nube.
6. Configurar los ajustes de conexión de IPsec de varios sitios.

Deshabilitación de la conexión de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Si no necesita que los servidores de nube del sitio en la nube se comuniquen con los servidores del sitio local, puede deshabilitar la conexión de sitio a sitio.

Pasos para deshabilitar la conectividad de sitio a sitio

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades** y luego deshabilite la opción **Conexión de sitio a sitio**.

El sitio local se desconectará del sitio en el cloud.

Solucionar problemas en la conectividad Open VPN de sitio a sitio

Cuando experimente problemas de conectividad con su sitio Open VPN de sitio a sitio, puede solucionar problemas y, a continuación, corregir los errores informados o enviar la información al equipo de soporte para su análisis y asistencia.

Para solucionar problemas de conectividad Open VPN de sitio a sitio

1. Abra la interfaz gráfica del dispositivo VPN.
2. En **Comandos**, seleccione **Resolución de problemas** y, a continuación, pulse **Intro**.

© Acronis International GmbH, 2003-2025

3. En la interfaz de línea de comandos, en la línea **¿Desea ejecutar el diagnóstico para la conexión de sitio a sitio [S/N]**, escriba **S** y, a continuación, pulse **Intro**.
   Se inicia la herramienta de diagnóstico. Si se detecta un problema, verá un error correspondiente y una descripción detallada. Puede copiar el texto que aparece o tomar una captura de pantalla y enviarla al equipo de soporte para obtener asistencia.

Conexión VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede utilizar la conectividad VPN de IPsec de varios sitios para conectar un solo sitio local o varios sitios locales a Disaster Recovery mediante una conexión VPN de IPsec L3 segura.

Este tipo de conectividad es útil para escenarios de Disaster Recovery si tiene uno de los siguientes casos:

- Tiene un sitio local con cargas de trabajo críticas.
- tiene varios sitios locales con cargas de trabajo críticas. Por ejemplo, oficinas en diferentes ubicaciones.
- utiliza sitios de software de terceros o sitios de proveedor de servicios gestionados y se conecta a ellos mediante un túnel VPN IPsec.

Para establecer una comunicación VPN de IPsec de varios sitios entre el sitio local y el sitio en la nube, se usa una **puerta de enlace de VPN**. Cuando comience a configurar la conexión VPN de IPsec de varios sitios en la consola de Cyber Protect, se implementará la puerta de enlace de VPN automáticamente en el sitio de la nube. Debe configurar los segmentos de red en la nube y asegurarse de que no se superpongan con los segmentos de la red local. Se establece un túnel VPN seguro entre los sitios locales y el sitio en la nube. Los servidores locales y en la nube pueden comunicarse mediante este túnel VPN si se encuentran todos en el mismo segmento de Ethernet.

Nota
Cuando se utiliza una conexión VPN de IPsec de varios sitios, la puerta de enlace VPN se asigna automáticamente una dirección IP pública.

Para que cada equipo de origen quede protegido, debe crear un servidor de recuperación en el sitio en la nube. Se queda en estado **En espera** hasta que sucede un evento de conmutación por error. Si sucede un desastre e inicia un proceso de conmutación por error (en el **modo de producción**), el servidor de recuperación que representa la copia exacta de su equipo protegido se inicia en la nube. Sus clientes pueden seguir trabajando con el servidor sin notar ningún cambio en segundo plano.

También puede iniciar un proceso de conmutación por error en el **modo de prueba**. Esto quiere decir que el equipo de origen continúa funcionando y, al mismo tiempo, se inicia en la nube el servidor de recuperación correspondiente en una red virtual especial que se crea en la nube, la **red**

© Acronis International GmbH, 2003-2025

de prueba. La red de prueba se aísla para evitar que se dupliquen las direcciones IP en el resto de los segmentos de red en la nube.

Puerta de enlace de VPN

El principal componente que permite la comunicación entre los sitios locales y el sitio en la nube es la **puerta de enlace de VPN**. Es un equipo virtual en el cloud en el que se instala software especial, y la red se configura de forma específica. La puerta de enlace de VPN realiza las siguientes funciones:

- Conecta los segmentos de Ethernet de su red local y de producción en la nube en el modo IPsec L3.
- Funciona como enrutador y NAT predeterminados para los equipos en las redes de prueba y producción.
- Funciona como servidor DHCP. Todos los equipos en las redes de producción y prueba obtienen la configuración de red (direcciones IP, configuración del DNS) por medio de DHCP. Un servidor en la nube obtendrá cada vez la misma dirección IP del servidor DHCP.

  Si lo prefiere, puede establecer una configuración de DNS personalizada. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 1056).
- Funciona como DNS para almacenar archivos en la memoria caché.

Cómo funciona el enrutamiento

El enrutamiento entre las redes en la nube se realiza con el enrutador en el sitio en la nube, de forma que los servidores de diferentes redes en esta puedan comunicarse entre ellos.

Configuración de VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede configurar la conexión VPN de IPsec de varios sitios de dos formas:

- Desde la pestaña **Disaster Recovery** > **Conectividad**.
- Aplicar un plan de protección en uno o varios dispositivos y luego cambiar de forma manual de la conexión OpenVPN de sitio a sitio creada de forma automática a una conexión VPN de IPsec de varios sitios, configurando los ajustes de VPN de IPsec de varios sitios y reasignando las direcciones IP.

Pestaña Conectividad

Pasos para configurar una conexión VPN de IPsec de varios sitios desde la pestaña Conectividad

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En la sección **Conexión VPN de varios sitios**, haga clic en **Configurar**.

© Acronis International GmbH, 2003-2025

Una puerta de enlace de VPN se implementa en el sitio en la nube.

3. Configure los ajustes de VPN de IPsec de varios sitios.

Plan de protección

Pasos para configurar una conexión VPN de IPsec de varios sitios desde un plan de protección

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Aplique un plan de protección a uno o varios dispositivos de la lista.
   El servidor de recuperación y los ajustes de infraestructura en la nube se configuran de manera automática para la conectividad OpenVPN de sitio a sitio.
3. Vaya a **Disaster Recovery** > **Conectividad**.
4. Haga clic en **Mostrar propiedades**.
5. Haga clic en **Cambiar a VPN de IPsec de varios sitios**.
6. Configure los ajustes de VPN de IPsec de varios sitios.
7. Reasigne las direcciones IP de la red y los servidores en la nube.

Configuración de los ajustes de VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Después de configurar una VPN de IPsec de varios sitios, debe configurar los ajustes del sitio en la nube y los sitios locales en la pestaña **Disaster Recovery** > **Conectividad**.

Requisitos previos

- Se ha configurado la conectividad VPN de IPsec de varios sitios. Para obtener más información sobre la configuración de la conectividad VPN de IPsec de varios sitios, consulte "Configuración de VPN de IPsec de varios sitios" (p. 1036).
- Cada puerta de enlace de VPN de IPsec local tiene una dirección IP pública.
- Su red en la nube tiene suficientes direcciones IP para los servidores en la nube que son copias de sus equipos protegidos (en la red de producción) y para los servidores de recuperación (con una o dos direcciones IP, según sus necesidades).
- [Si usa un cortafuegos entre los sitios locales y el sitio en la nube] Los siguientes protocolos IP y puertos UDP se admiten en los sitios locales: Protocolo IP ID 50 (ESP), Puerto UDP 500 (IKE) y Puerto UDP 4500.
- Se ha deshabilitado la configuración de NAT-T en el sitio local.

Para configurar una conexión VPN de IPsec de varios sitios

© Acronis International GmbH, 2003-2025

1. Añada una o más redes al sitio en la nube.
   a. Haga clic en **Añadir red**.

      Nota
      Cuando añada una red en la nube, se añadirá automáticamente la red de prueba correspondiente con la misma dirección y máscara de red para realizar conmutaciones por error de prueba. Los servidores en la nube de la red de prueba tendrán las mismas direcciones IP que en la red productiva en la nube. Si necesita acceder a un servidor en la nube desde la red productiva durante una conmutación por error de prueba, asigne una segunda dirección IP de prueba cuando cree un servidor de recuperación.

   b. En el campo **Dirección de red**, escriba la dirección IP de la red.

      Nota
      Asegúrese de que las redes de la nube no se solapen con ninguna red local en su entorno. De lo contrario, no se podrá establecer un túnel.

   c. En el campo **Máscara de red**, escriba la máscara de la red.
   d. Haga clic en **Agregar**.
2. Configure los ajustes de cada sitio local que quiera conectar al sitio en la nube, de acuerdo con las recomendaciones de los sitios locales. Para obtener más información sobre estas recomendaciones, consulte "Recomendaciones generales para sitios locales" (p. 1039).
   a. Haga clic en **Añadir conexión**.
   b. Introduzca un nombre para la puerta de enlace de VPN local.
   c. Introduzca la dirección IP pública de la puerta de enlace de VPN local.
   d. [Opcional] Introduzca una descripción de la puerta de enlace de VPN local.
   e. Haga clic en **Siguiente**.
   f. En el campo **Clave compartida previamente**, escríbala o haga clic en **Generar nueva clave compartida previamente** para utilizar un valor generado automáticamente.

      Nota
      Utilice la misma clave compartida previamente para las puertas de enlace de VPN locales y en la nube.

   g. Haga clic en **Configuración de seguridad de IPsec o IKE** para configurar los ajustes. Para obtener más información acerca de los ajustes que puede configurar, consulte "Configuración de seguridad de IPsec o IKE" (p. 1040).

© Acronis International GmbH, 2003-2025

Nota
Puede utilizar los ajustes predeterminados, que se completan automáticamente, o valores personalizados. Solo se admiten las conexiones del protocolo IKEv2. La **acción de inicio** predeterminada cuando se establece la VPN es **Agregar** (su puerta de enlace de VPN local iniciará la conexión). Sin embargo, puede cambiarla a **Iniciar** (la puerta de enlace de la VPN en la nube iniciará la conexión) o **Dirigir** (adecuada para cortafuegos compatibles con la opción dirigir).

h. Configurar las **directivas de red**.
   Las directivas de red especifican las redes a las que se conecta la VPN IPsec. Escriba la dirección IP y la máscara de la red con el formato CIDR. Los segmentos de las redes locales y en la nube no deben superponerse.
i. Haga clic en **Guardar**.

Recomendaciones generales para sitios locales

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando configure los sitios locales para la conectividad VPN de IPsec de varios sitios, tenga en cuenta las siguientes recomendaciones:

- En cada fase de IKE, establezca al menos uno de los valores que están configurados en el sitio en la nube para los siguientes parámetros: Algoritmo de cifrado, algoritmo de hash y números de grupo Diffie-Hellman.
- Habilite el secreto perfecto hacia adelante con al menos uno de los valores para los números de grupo Diffie-Hellman configurados en el sitio en la nube para la fase 2 de IKE.
- Configure los mismos valores para la **vida útil** de las fases 1 y 2 de IKE que los del sitio en la nube.
- No se admiten las configuraciones con NAT traversal (NAT-T). Deshabilite la configuración de NAT-T en el sitio local. Si no, no se podrá negociar la encapsulación de UDP adicional.
- La configuración **Acción de inicio** define qué lado inicia la conexión. El valor predeterminado **Agregar** significa que la conexión se inicia en el sitio local y que el sitio en la nube está esperando que se inicie la conexión. Cambie el valor a **Iniciar** si desea que la conexión se inicie en el sitio en la nube, o a **Dirigir** si desea que ambos lados puedan iniciar la conexión (adecuado para cortafuegos que son compatibles con la opción dirigir).

Para obtener más información y ejemplos de configuración para distintas soluciones, consulte:

- Esta serie de artículos de la base de conocimientos:
- Este vídeo de ejemplo:

© Acronis International GmbH, 2003-2025

Configuración de seguridad de IPsec o IKE

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La siguiente tabla proporciona más información sobre los parámetros de seguridad Psec/IKE.

Parámetro	Descripción
Algoritmo de cifrado	El algoritmo de cifrado que se utilizará para asegurarse de que los datos no se puedan ver mientras estén en tránsito. De manera predeterminada, se seleccionarán todos los algoritmos. Al menos uno de los algoritmos seleccionados debe estar configurado en su puerta de enlace local para cada fase de IKE.
Algoritmo de hash	El algoritmo de hash que se utilizará para verificar la integridad y la autenticidad de los datos. De manera predeterminada, se seleccionarán todos los algoritmos. Al menos uno de los algoritmos seleccionados debe estar configurado en su puerta de enlace local para cada fase de IKE.
Números de grupo Diffie-Hellman	Los números de grupo Diffie-Hellman definen la fuerza de la clave utilizada en el proceso de Internet Key Exchange (IKE). Los números de grupo más altos son más seguros, pero requieren más tiempo para que la clave se calcule. De manera predeterminada, se seleccionarán todos los grupos. Al menos uno de los grupos seleccionados debe estar configurado en su puerta de enlace local para cada fase de IKE.
Vida útil (segundos)	El valor de la vida útil determina la duración de una instancia de conexión con un conjunto de claves de cifrado o autenticación para paquetes de usuario, desde la compleción de la negociación hasta el vencimiento. Intervalo de la fase 1:De 900 a 28 800 segundos, con 28 800 como valor predeterminado. Intervalo de la fase 2: De 900 a 3600 segundos, con 3600 como valor predeterminado.

© Acronis International GmbH, 2003-2025

Parámetro	Descripción
	La vida útil de la fase 2 debe ser inferior a la de la fase 1. La conexión se renegocia a través del canal de codificación antes de que venza. Consulte **Tiempo de margen para cambiar la clave**. Si el lado local y el remoto no tienen la misma vida útil, las conexiones remplazadas estarán desordenadas en el lado con la vida útil más larga. Consulte también **Tiempo de margen para cambiar la clave** y **Difusión de cambio de clave**.
Tiempo de margen para cambiar la clave (segundos)	Tiempo de margen antes de la expiración de la conexión o la expiración del canal de claves durante el cual el lado local de la conexión VPN intenta negociar un reemplazo. El tiempo exacto para cambiar la clave se selecciona de manera aleatoria según el valor de la **Difusión de cambio de clave**. Es relevante solo a nivel local; el lado remoto no necesita estar de acuerdo. Intervalo: 900-3600 segundos. El valor predeterminado es 3600.
Tamaño del período de reproducción (paquete)	Tamaño del período de reproducción de IPsec para esta conexión. El valor predeterminado -1 utiliza el valor configurado con charon.replay_window en el archivo strongswan.conf. Los valores superiores a 32 solo son compatibles cuando se utiliza el backend Netlink. Un valor igual a 0 deshabilita la protección de reproducción de IPsec.
Difusión de cambio de clave (%)	Porcentaje máximo que los valores de marginbytes, marginpackets y margintime aumentan aleatoriamente para distribuir al azar los intervalos de cambio de clave (importante para servidores con muchas conexiones). El valor de difusión de cambio de clave puede exceder el 100 %. Después del aumento aleatorio, el valor de marginTYPE no debe exceder lifeTYPE, donde TYPE es bytes, paquetes o tiempo. El valor 0 % deshabilita la distribución aleatoria. Es relevante solo a nivel local; el lado remoto no

© Acronis International GmbH, 2003-2025

Parámetro	Descripción
	necesita estar de acuerdo.
Tiempo de espera de DPD (segundos)	Tiempo tras el que tiene lugar la acción del tiempo de espera de la detección de pares inactivos (DPD). Puede especificar un valor igual o mayor que 30. El valor predeterminado es 30.
Acción del tiempo de espera de la detección de pares inactivos (DPD)	Acción que debe realizarse después de que se agote el tiempo de espera de la detección de pares inactivos (DPD). **Reiniciar**: Reinicia la sesión cuando se agota el tiempo de espera de DPD. **Borrar**: Finaliza la sesión cuando se agote el tiempo de espera de DPD. **Ninguna**: No realiza ninguna acción cuando se agota el tiempo de espera de DPD.
Acción de inicio	Determina qué lado inicia la conexión y establece el túnel para la conexión VPN. **Agregar**: La puerta de enlace de su VPN local iniciará la conexión. **Iniciar**: La puerta de enlace de la VPN en la nube iniciará la conexión. **Dirigir**: Adecuado para puertas de enlace de VPN compatibles con la opción dirigir. el túnel estará activo solo cuando haya tráfico iniciado desde la puerta de enlace de VPN local o la puerta de enlace de Cloud VPN.

Cambio de VPN IPsec de varios sitios a OpenVPN de sitio a sitio

Puede cambiar fácilmente de una conexión VPN de IPsec de varios sitios a una conexión OpenVPN de sitio a sitio.

Cuando cambia el tipo de conectividad, las conexiones VPN activas se eliminan, pero la configuración de la red y de los servidores en la nube se conservan. Sin embargo, puede que necesite reasignar las direcciones IP de las redes y los servidores en la nube.

La siguiente tabla compara las características básicas de la conexión OpenVPN de sitio a sitio y la conexión VPN de IPsec de varios sitios.

© Acronis International GmbH, 2003-2025

	OpenVPN de sitio a sitio	VPN de IPsec de varios sitios
Soporte técnico del sitio local	Único	Único, múltiple
Modo de puerta de enlace de VPN	L2 Open VPN	L3 IPsec VPN
Segmentos de red	Amplía la red local a la red en la nube	Las redes locales y los segmentos de las redes en la nube no deben superponerse
Compatible con el acceso de punto a sitio al sitio local	Sí	No
Compatible con el acceso de punto a sitio al sitio en la nube	Sí	Sí
Requiere un elemento de oferta de IP pública	No	Sí

Para cambiar de una conexión VPN de IPsec de varios sitios a una conexión OpenVPN de sitio a sitio

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Cambiar a OpenVPN de sitio a sitio**.
4. Haga clic en **Reconfigurar**.
5. Reasigne las direcciones IP de la red y los servidores en la nube.
6. Configure los ajustes de la conexión de sitio a sitio.

Solución de problemas de configuración de VPN de IPsec

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando configure o use la conexión VPN de IPsec, puede experimentar problemas.

Puede obtener más información sobre los problemas que puede encontrar en los archivos de registro de IPsec y comprobar el tema Solución de problemas de configuración de VPN IPsec para conocer las posibles soluciones a algunos de los problemas comunes que pueden ocurrir.

© Acronis International GmbH, 2003-2025

Solución de problemas de configuración de VPN de IPsec

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La siguiente tabla describe los problemas de configuración de VPN de IPsec más frecuentes y explica cómo resolverlos.

Problema	Posible solución
Aparece el siguiente mensaje de error: **Error de negociación de la fase 1 de IKE. Compruebe la configuración de IPsec IKE en los sitios locales y en la nube.**	Haga clic en **Reintentar** y compruebe si aparece algún mensaje de error más específico. Por ejemplo, un mensaje de error más específico podría ser uno sobre una discrepancia de algoritmos o una clave compartida previamente incorrecta. **Nota** Por motivos de seguridad, las siguientes restricciones se aplican a la conectividad VPN de IPsec: • IKEv1 está obsoleto en RFC8247 y no se admite debido a que supone riesgos de seguridad. Solo se admiten las conexiones del protocolo IKEv2. • Los siguientes algoritmos de cifrado no se consideran seguros y no son compatibles: DES y 3DES. • Los siguientes algoritmos de hash no se consideran seguros y no son compatibles: SHA1 y MD5. • El número 2 de grupo de Diffie-Hellman no se considera seguro y no es compatible.
El estado de la conexión entre mi sitio local y en la nube sigue siendo **Conectando**.	Compruebe: • Si el puerto UDP 500 está abierto (cuando use un cortafuegos). • La conectividad entre el sitio local y el sitio en la nube. • Si la dirección IP del sitio local es correcta.
El estado de la conexión entre mi sitio local y en la nube sigue siendo **Esperando una conexión**.	Este estado aparece cuando se establece **Agregar** como **Acción de inicio** para el sitio en la nube, lo que significa que el sitio en la nube está esperando que se inicie la conexión desde el sitio local.

© Acronis International GmbH, 2003-2025

Problema	Posible solución
	Inicie la conexión desde el sitio local.
El estado de la conexión entre mi sitio local y en la nube sigue siendo **Esperando el tráfico**.	Verá este estado cuando la **acción de inicio** para el sitio local sea **Dirigir**. Si está esperando una conexión desde el sitio local, haga lo siguiente: • Desde el sitio local, intente hacer ping en la máquina virtual del sitio en la nube. Se trata de un comportamiento estándar necesario para establecer un túnel para algunos dispositivos, por ejemplo, Cisco ASA. (Modo Dirigir) • Asegúrese de que el sitio local haya establecido un túnel al configurar **Iniciar** como **Acción de inicio** del sitio local.
El estado de la conexión entre mi sitio local y en la nube se ha establecido, pero una o más directivas de red no funcionan.	Esto puede deberse a las siguientes razones: • La asignación de red en el sitio IPsec en la nube es distinta de la asignación de red del sitio local. Asegúrese de que las asignaciones de red y la secuencia de las directivas de red de los sitios local y en la nube coinciden exactamente. • Este estado es correcto cuando se establece **Dirigir** como **Acción de inicio** del sitio local o en la nube (por ejemplo, en dispositivos Cisco ASA), y no hay tráfico en ese momento. Puede intentar hacer ping para asegurarse de que se ha establecido el túnel. Si el ping no funciona, compruebe la asignación de red del sitio local y en la nube.
Quiero reiniciar una conexión IPsec específica.	Para reiniciar una conexión IPsec específica: 1. En la pantalla **Recuperación ante desastres** > **Conectividad**, haga clic en la conexión IPsec. 2. Haga clic en **Deshabilitar conexión**. 3. Haga clic en la conexión de IPsec de nuevo. 4. Haga clic en **Habilitar conexión**.

Descarga de archivos de registro de VPN de IPsec

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

© Acronis International GmbH, 2003-2025

Puede obtener más información sobre la conectividad IPsec en los archivos de registro del servidor VPN. Los archivos de registro están comprimidos en un archivo .zip que puede descargar y extraer.

Requisitos previos

Se ha configurado la conectividad VPN de IPsec de varios sitios.

Para descargar el archivo .zip con los archivos de registro

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en el icono de engranaje que se encuentra junto a la puerta de enlace de VPN del sitio en la nube.
3. Haga clic en **Descargar registro**.
4. Haga clic en **Listo**.
5. Cuando el archivo .zip esté listo para descargarse, haga clic en **Descargar registro** y guárdelo de forma local.

Archivos de registro de VPN de IPsec de varios sitios

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La siguiente lista describe los archivos de registro de VPN de IPsec que son parte del archivo .zip y sobre la información que contienen.

- `ip.txt`: El archivo contiene los registros de la configuración de las interfaces de red. Deben aparecer dos direcciones IP: una pública y una local. Si no ve estas direcciones IP en el registro, hay un problema. Comuníquese con el equipo de soporte.

  Nota
  El valor de la máscara de la dirección IP pública debe ser 32.

- `swanctl-list-loaded-config.txt`: El archivo contiene información sobre todos los sitios de IPsec. Si no ve algún sitio en el archivo, no se habrá aplicado la configuración de IPsec. Intente actualizar la configuración y guardarla o comuníquese con el equipo de soporte.
- `swanctl-list-active-sas.txt`: El archivo contiene conexiones y políticas en estado activo o conectado.

Acceso de VPN remoto de punto a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

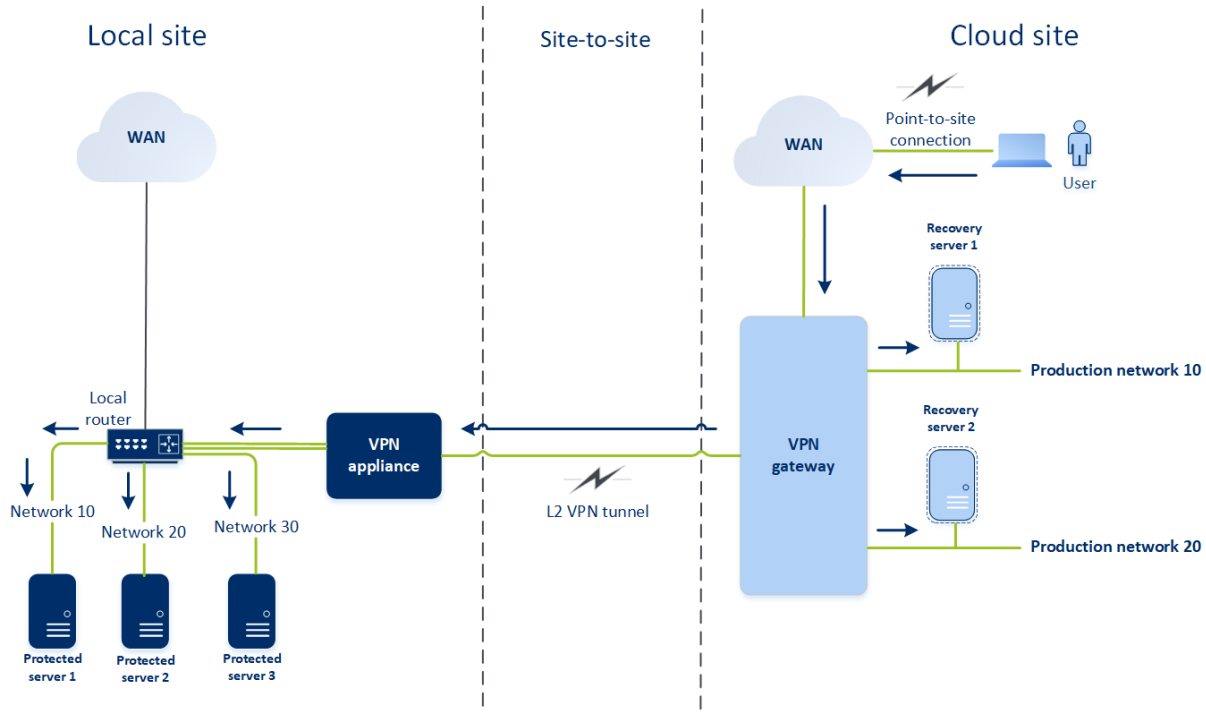
© Acronis International GmbH, 2003-2025

La conexión de punto a sitio es una conexión VPN segura desde el exterior que usa sus dispositivos de endpoint (como un ordenador o portátil) a los sitios en la nube y locales mediante un VPN. Está disponible después de establecer una conexión OpenVPN de sitio a sitio al sitio de recuperación de desastres. Este tipo de conexión es útil en los casos siguientes:

- En muchas empresas, los servicios corporativos y los recursos web solo están disponibles desde la red de la empresa. Puede utilizar la conexión de punto a sitio para conectarse al sitio local de forma segura.
- En caso de desastre, al trasladar una carga de trabajo al sitio en la nube mientras la red local está desactivada, puede necesitar acceder directamente a sus servidores en el cloud. Esto es posible gracias a la conexión de punto a sitio al sitio en la nube.

Para la conexión de punto a sitio en el sitio local, debe instalar el dispositivo VPN en el sitio local, configurar la conexión de sitio a sitio y después la conexión de punto a sitio del sitio local. Así, sus empleados remotos tendrán acceso a la red corporativa mediante L2 VPN.

El siguiente esquema muestra el sitio local, el sitio del cloud y las comunicaciones entre servidores están marcadas en verde. El túnel L2 VPN conecta el sitio local con el de la nube. Cuando un usuario establece una conexión de punto a sitio, las comunicaciones al sitio local se realizan a través del sitio en la nube.



La configuración de punto a sitio usa certificados para autenticar el cliente de VPN. También se usan las credenciales de usuario para la autenticación. Tenga en cuenta lo siguiente acerca de la conexión de punto a sitio al sitio local:

- Los usuarios deben usar sus credenciales de Cyber Protect Cloud para autenticarse en el cliente VPN. Deben tener los roles de usuario "Administrador de la empresa" o "Ciberprotección".

© Acronis International GmbH, 2003-2025

- Si ha vuelto a generar la configuración OpenVPN, debe proporcionar la configuración actualizada a todos los usuarios que estén utilizando la conexión de punto a sitio para acceder al sitio en la nube.

Configuración de acceso de VPN remoto de punto a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Si necesita conectar su sitio local de forma remota, puede configurar la conexión de punto a sitio del sitio local. Puede seguir el procedimiento siguiente o ver el tutorial en vídeo.

Requisitos previos

- La conectividad OpenVPN de sitio a sitio está configurada.
- El dispositivo VPN está instalado en el sitio local.

Para configurar la conexión de punto a sitio al sitio local

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Habilite la opción **Acceso mediante VPN al sitio local**.
4. Asegúrese de que el usuario que debe establecer la conexión de punto a sitio en el sitio local tiene:
   - Una cuenta de usuario en Cyber Protect Cloud. Eestas credenciales se usan para la autenticación en el cliente VPN. De lo contrario, cree una cuenta de usuario en Cyber Protect Cloud.
   - Un rol de usuario de "Administrador de la empresa" o "Ciberprotección".
5. Configurar el cliente OpenVPN:
   a. Descargue el cliente OpenVPN versión 2.4.0 o posterior de la siguiente ubicación https://openvpn.net/community-downloads/.

      Nota
      El cliente OpenVPN Connect no es compatible.

   b. Instale el cliente OpenVPN en el equipo desde el que quiera conectarse al sitio local.
   c. Haga clic en **Descargar configuración para OpenVPN**. El archivo de configuración es válido para los usuarios de su organización con el rol de usuario "Administrador de la empresa" o "Ciberprotección".
   d. Importe la configuración descargada al cliente OpenVPN.
   e. Inicie sesión en el cliente OpenVPN con sus credenciales de usuario de Cyber Protect Cloud (vea el paso 4 anterior).

© Acronis International GmbH, 2003-2025

f. [Opcional] Si la autenticación de doble factor está habilitada en su organización, debe proporcional el código TOTP de generación única.

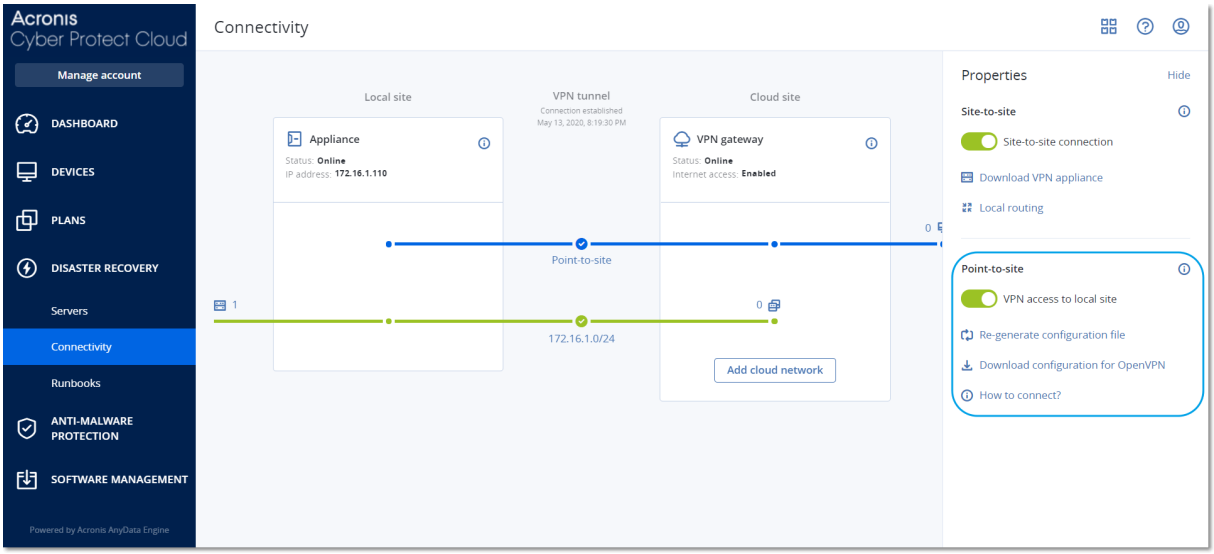
Importante
Si ha habilitado la autenticación de doble factor para su cuenta, tiene que volver a generar el archivo de configuración y renovarlo para sus clientes OpenVPN existentes. Los usuarios deben volver a iniciar sesión en Cyber Protect Cloud para configurar la configurar la autenticación de doble factor en sus cuentas.

Como resultado, podrá conectarse a las máquinas en el sitio local.

Gestión de la configuración de la conexión de punto a sitio:

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad** y pulse en **Mostrar propiedades** en la esquina superior derecha.



Acceso mediante VPN al sitio local

Esta opción se utiliza para administrar el acceso VPN al sitio local. Está habilitada por defecto. Si está deshabilitada, entonces no se permitirá el acceso de punto a sitio al sitio local.

Descargar configuración para OpenVPN

Así se descargará el archivo de configuración del cliente OpenVPN, El archivo es necesario para establecer una conexión de punto a sitio al sitio en la nube.

Volver a generar la configuración

Puede volver a generar el archivo de configuración del cliente OpenVPN.

© Acronis International GmbH, 2003-2025

Esta acción es obligatoria en los siguientes casos:

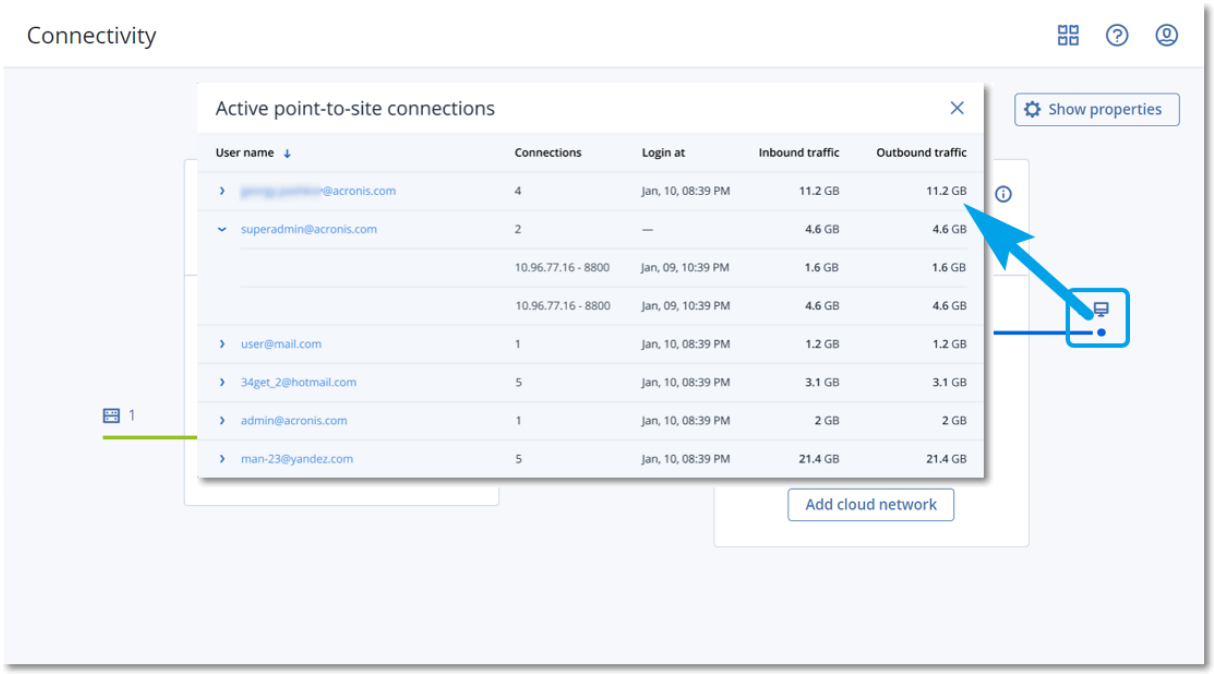
- Si cree que el archivo de configuración está en riesgo.
- Si la autenticación de doble factor estaba habilitada en su cuenta.

En cuanto se actualice el archivo de configuración, no se podrá llevar a cabo la conexión a través del archivo de configuración anterior. Asegúrese de distribuir el nuevo archivo entre los usuarios a los que se les permita usar la conexión de punto a sitio.

Conexiones activas de punto a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ver todas las conexiones de punto a sitio activas en **Recuperación ante desastres** > **Conectividad**. Pulse en el icono del equipo en la línea azul de **De punto a sitio** y verá información detallada sobre las conexiones de punto a sitio activas agrupadas por su nombre de usuario.



Recomendaciones para la disponibilidad de servicios de dominio de Active Directory

Si tiene que autenticar sus cargas de trabajo protegidas en un controlador de dominio, le recomendamos que disponga de una instancia de controlador de dominio de Active Directory (AD DC) en el sitio de Disaster Recovery.

© Acronis International GmbH, 2003-2025

Controladores de dominio de Active Directory para conectividad OpenVPN L2

Con la conectividad OpenVPN L2, las direcciones IP de las cargas de trabajo protegidas se conservan en el sitio en la nube durante una conmutación por error de prueba o de producción. Por ello, la instancia de AD DC tiene la misma dirección IP que en el sitio local durante una conmutación por error de prueba o de producción.

Con DNS personalizados podrá establecer su propio servidor DNS personalizado para todos los servidores en la nube. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 1056).

Controladores de dominio de Active Directory para conectividad VPN de IPsec L3

Con la conectividad VPN de IPsec L3, las direcciones IP de las cargas de trabajo protegidas no se conservan en el sitio en la nube. Por ello, recomendamos tener una instancia de AD DC dedicada adicional como un servidor principal en el sitio en la nube antes de llevar a cabo la conmutación por error de producción.

Estas son las recomendaciones para una instancia de AD DC dedicada que esté configurada como un servidor principal en el sitio en la nube:

- Apague el cortafuegos de Windows.
- Una el servidor principal al servicio de Active Directory.
- Asegúrese de que el servidor principal tenga acceso a Internet.
- Añada la función de Active Directory.

Con DNS personalizados podrá establecer su propio servidor DNS personalizado para todos los servidores en la nube. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 1056).

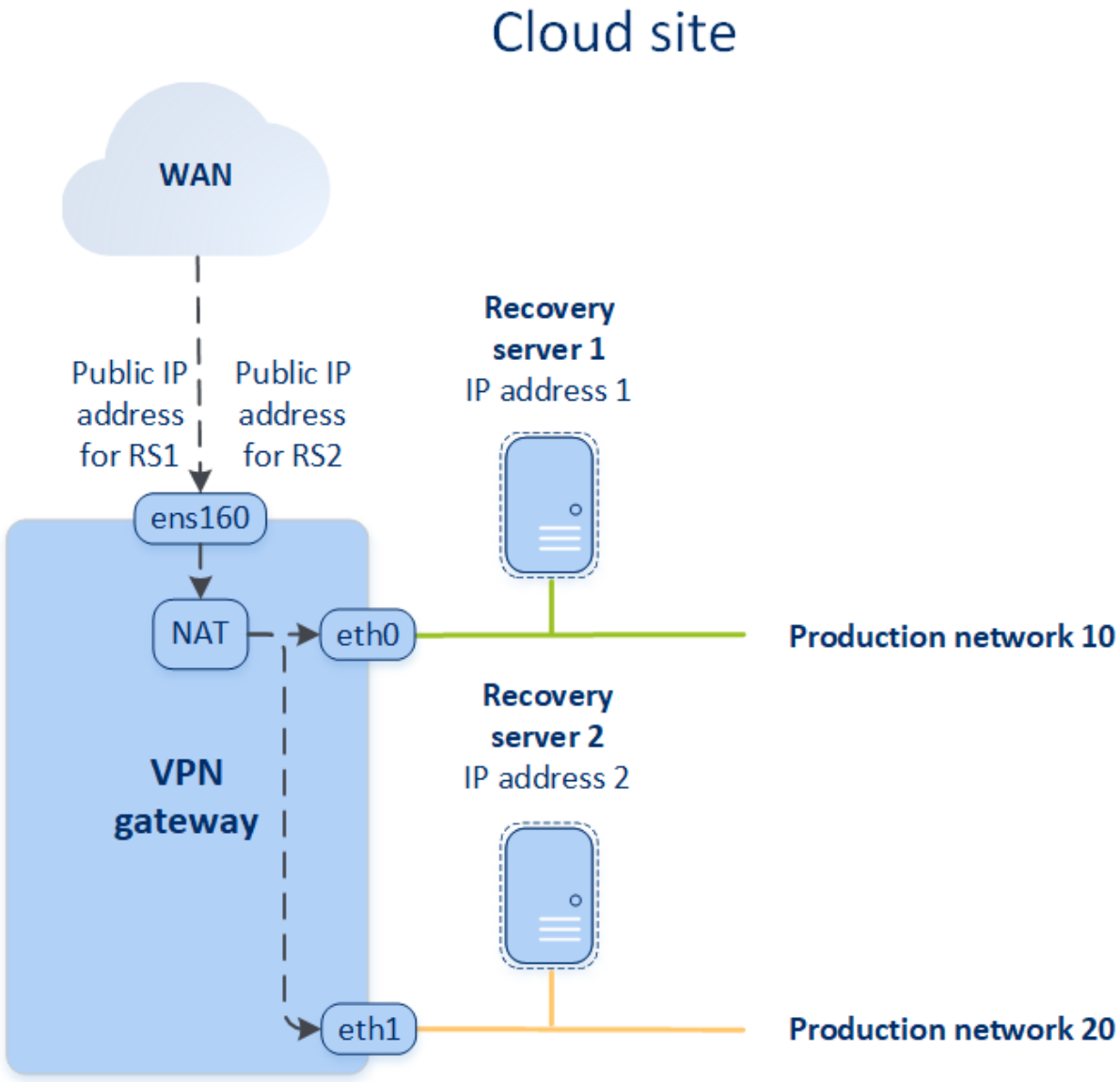
Gestión de redes

Esta sección describe escenarios de gestión de redes.

Direcciones IP de prueba y públicas

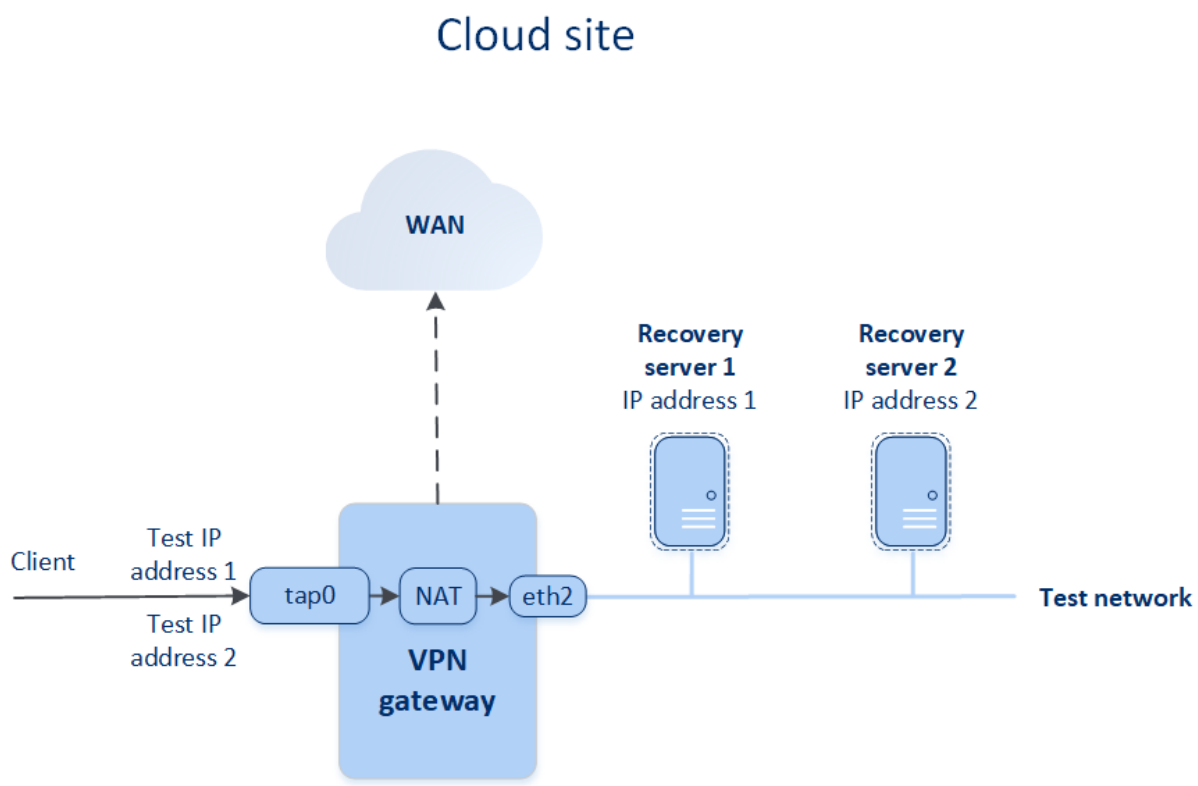
Si asigna la dirección IP pública al crear un servidor de recuperación, este pasará a estar disponible desde Internet a través de dicha dirección IP. Cuando llega un paquete de Internet con la dirección IP pública de destino, la puerta de enlace de VPN la vuelve a asignar a la dirección IP de producción correspondiente mediante NAT y la envía al servidor de recuperación correspondiente.

© Acronis International GmbH, 2003-2025



Si asigna la dirección IP de prueba al crear un servidor de recuperación, este pasará a estar disponible desde la red de prueba a través de dicha dirección IP. Al realizar la prueba de conmutación por error, el equipo de origen continuará funcionando mientras el servidor de recuperación con la misma dirección IP se inicia en la red de prueba en la nube. No se produce ningún conflicto de dirección IP, ya que la red de prueba está aislada. Se puede acceder a los servidores de recuperación en la red de prueba con sus direcciones IP de prueba que se vuelven a asignar a las direcciones IP de producción mediante NAT.

© Acronis International GmbH, 2003-2025



Para obtener más información sobre OpenVPN de sitio a sitio, consulte "OpenVPN de sitio a sitio: información adicional" (p. 1578).

Volver a configurar la dirección IP

Para garantizar el rendimiento adecuado de la recuperación ante desastres, las direcciones IP asignadas a los servidores local y en el cloud deben ser coherentes. Si hay alguna incoherencia en las direcciones IP o estas no coinciden, verá un signo de exclamación junto a la red correspondiente en **Disaster Recovery** > **Conectividad**.

A continuación, se enumeran algunas de las razones más conocidas de la incoherencia de direcciones IP:

1. Se ha migrado un servidor de recuperación de una red a otra o se ha cambiado la máscara de red de la red en la nube. Como resultado, los servidores de nube tienen las direcciones IP de redes a las que no están conectados.
2. El tipo de conectividad se cambió de sin conexión de sitio a sitio a conexión de sitio a sitio. Como resultado, un servidor local se encuentra en una red distinta de aquella que se creó para el servidor de recuperación en el sitio en el cloud.
3. El tipo de conectividad se cambió de OpenVPN de sitio a sitio a VPN de IPsec de varios sitios, o de VPN de IPsec de varios sitios a OpenVPN de sitio a sitio. Para obtener más información sobre estos escenarios, consulte Cambio de conexiones, "Cambio de VPN IPsec de varios sitios a OpenVPN de sitio a sitio" (p. 1042) y Reasignación de direcciones IP.
4. Editar los siguientes parámetros de red en el sitio del dispositivo VPN:

© Acronis International GmbH, 2003-2025

- Agregar una interfaz mediante la configuración de red.
- Editar manualmente la máscara de red mediante la configuración de interfaz.
- Editar la máscara de red mediante DHCP.
- Editar manualmente la máscara y dirección de red mediante la configuración de interfaz.
- Editar la máscara y dirección de red mediante DHCP.

El resultado de las anteriores acciones es que la red en el sitio en el cloud puede convertirse en un subconjunto o un superconjunto de la red local, o bien la interfaz del dispositivo VPN puede informar de que distintas interfaces tienen la misma configuración de red.

Para resolver el problema con la configuración de red:

1. Haga clic en la red cuya dirección IP debe volver a configurar.
   Verá una lista de servidores en la red seleccionada, sus estados y sus direcciones IP. Los servidores cuyas configuraciones de red sean incoherentes se marcan con un signo de exclamación.
2. Para cambiar la configuración de red de un servidor, haga clic en **Ir al servidor**. Para cambiar la configuración de red de todos los servidores a la vez, haga clic en **Modificar**, en el bloque de notificaciones.
3. Cambie las direcciones IP según sea necesario definiéndolas en los campos **IP nueva** y **Nueva IP de prueba**.
4. Haga clic en **Confirmar** cuando tenga todo a punto.

Mover servidores a una red adecuada

Al crear un plan de protección con recuperación ante desastres y aplicarlo a los dispositivos seleccionados, el sistema comprueba la dirección IP de cada dispositivo y crea automáticamente redes en la nube si no hay redes en la nube que existentes a las que se pueda adaptar la dirección IP. De forma predeterminada, la entidad IANA configura las redes con rangos máximos recomendados en la nube para uso privado (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Puede editar la máscara de red para reducir su red.

En el caso de que los dispositivos seleccionados estén en varias redes locales, la red del sitio en la nube puede convertirse en un superconjunto de redes locales. En este caso, siga estos pasos para volver a configurar redes en la nube:

1. Haga clic en la red en la nube cuyo tamaño tenga que volver a configurar y luego en **Editar**.
2. Vuelva a configurar el tamaño de la red con los ajustes correctos.
3. Cree otras redes requeridas.
4. Haga clic en el icono de notificación que se encuentra junto al número de dispositivos conectados a la red.
5. Haga clic en **Mover a una red adecuada**.
6. Seleccione los servidores que desea mover a las redes adecuadas y, a continuación, haga clic en **Mover**.

© Acronis International GmbH, 2003-2025

Reasignación de direcciones IP

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Debe reasignar las direcciones IP de las redes y los servidores en la nube para completar la configuración en los siguientes casos:

- Tras cambiar de OpenVPN de sitio a sitio a VPN de IPsec de varios sitios, o al contrario.
- Tras aplicar un plan de protección (si se ha configurado la conectividad VPN de IPsec de varios sitios).

Red en el cloud

Para reasignar la dirección IP de una red en la nube

1. En la pestaña **Conectividad**, haga clic en la dirección IP de la red en la nube.
2. En la ventana emergente **Red**, haga clic en **Editar**.
3. Escriba la dirección y la máscara de red nuevas.
4. Haga clic en **Listo**.

Después de reasignar la dirección IP de una red en la nube, deberá reasignar los servidores en la nube que pertenecen a la red en la nube reasignada.

Servidor en la nube

Para reasignar la dirección IP de un servidor

1. En la pestaña **Conectividad**, haga clic en la dirección IP del servidor de la red en la nube.
2. En la ventana emergente **Servidores**, haga clic en **Cambiar la dirección IP**.
3. En la ventana emergente **Cambiar la dirección IP**, escriba la nueva dirección IP del servidor o utilice la dirección IP generada automáticamente que forma parte de la red en la nube reasignada.

   Nota
   Disaster Recovery asigna automáticamente direcciones IP de la red en la nube a todos los servidores en la nube que son parte de esta antes de reasignar la dirección IP de la red. Puede utilizar las direcciones IP sugeridas para reasignar las direcciones IP de todos los servidores en la nube a la vez.

4. Haga clic en **Confirmar**.

© Acronis International GmbH, 2003-2025

Reinstalación de la puerta de enlace de VPN

Si ocurre un problema con la puerta de enlace de VPN que no puede resolver, puede que quiera volver a instalarla. Los posibles problemas incluyen los siguientes:

- El estado de la puerta de enlace de la VPN es **Error**.
- El estado de la puerta de enlace de la VPN aparece como **Pendiente** durante un periodo prolongado.
- El estado de la puerta de enlace de la VPN no se ha determinado durante un periodo prolongado.

El proceso de reinstalación de la puerta de enlace de VPN incluye las siguientes acciones automáticas: eliminación por completo de la máquina virtual de la puerta de enlace de VPN, instalación de una nueva máquina virtual a partir de la plantilla y aplicación de la configuración de la puerta de enlace de VPN anterior a la nueva máquina virtual.

Requisitos previos

Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para volver a instalar la puerta de enlace de VPN

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en el icono de engranaje de la puerta de enlace de VPN y seleccione **Reinstalar la puerta de enlace de la VPN**.
3. En el cuadro de diálogo **Reinstalar la puerta de enlace de la VPN**, ingrese sus credenciales de inicio de sesión.
4. Haga clic en **Reinstalar**.

Configuración de servidores DNS personalizados

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando configura una conectividad, Disaster Recovery crea su infraestructura de red en la nube. El servidor DHCP en la nube asigna de forma automática los servidores DNS predeterminados a los servidores de recuperación y servidores principales. Sin embargo, puede cambiar los ajustes predeterminados y configurar los servidores DNS personalizados. La nueva configuración de DNS se aplicará en el momento de la próxima solicitud al servidor DHCP.

Requisitos previos

Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Para configurar un servidor DNS personalizado

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Predeterminado (proporcionado por Cloud Site)**.
4. Seleccione **Servidores personalizados**.
5. Escriba la dirección IP del servidor DNS.
6. [Opcional] Si desea agregar otro servidor DNS, haga clic en **Agregar** y escriba la dirección IP del servidor DNS.

   Nota
   Cuando haya añadido los servidores DNS personalizados, también podrá añadir los servidores DNS predeterminados. De ese modo, si los servidores DNS personalizados no están disponibles, Disaster Recovery utilizará los servidores DNS predeterminados.

7. Haga clic en **Listo**.

Eliminación de servidores DNS personalizados

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede eliminar servidores DNS desde la lista de DNS personalizados.

Requisitos previos

Se han configurado los servidores DNS personalizados.

Para eliminar un servidor DNS personalizado

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Servidores personalizados**.
4. Haga clic en el icono de eliminar que hay junto al servidor DNS.

   Nota
   La operación de eliminación está deshabilitada cuando solo hay disponible un servidor DNS personalizado. Si desea eliminar todos los servidores DNS personalizados, seleccione **Predeterminado (proporcionado por Cloud Site)**.

5. Haga clic en **Listo**.

Configuración de enrutación local

Además de sus redes locales que se extienden a la nube mediante el dispositivo VPN, puede tener otras redes locales que no estén registradas en dicho dispositivo y cuyos servidores deban

© Acronis International GmbH, 2003-2025

comunicarse con servidores en la nube. Para establecer la conectividad entre estos servidores locales y los servidores en el cloud, debe configurar los ajustes de enrutación local.

Para configurar la enrutación local:

1. Vaya a **Disaster Recovery** > **Conectividad**.
2. Pulse en **Mostrar propiedades** y luego pulse en **Enrutamiento local**.
3. Especifique las redes locales en la notación del CIDR.
4. Haga clic en **Guardar**.

Como resultado, los servidores de las redes locales especificadas podrán comunicarse con los servidores en la nube.

Descarga de direcciones MAC

Puede descargar una lista de direcciones MAC para extraerlas e importarlas en la configuración de su servidor DHCP personalizado.

Requisitos previos

- Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.
- Se debe configurar al menos un servidor de recuperación o principal con una dirección MAC.

Cómo descargar la lista de direcciones MAC

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Descargar la lista de direcciones MAC** y guarde el archivo CSV.

Trabajar con registros

Disaster Recovery recopila registros para el dispositivo VPN y la puerta de enlace VPN. Los registros se guardan como archivos .txt, que se comprimen en un archivo .zip. Puede descargar y extraer el archivo comprimido y utilizar la información para resolver problemas o supervisar objetivos.

La siguiente lista describe los archivos de registro que son parte del archivo .zip y la información que contienen.

`dnsmasq.config.txt`: El archivo contiene información sobre la configuración del servicio que proporciona direcciones DNS y DHCP.

`dnsmasq.leases.txt`: El archivo contiene información sobre los alquileres actuales de direcciones DHCP.

`dnsmasq_log.txt`: El archivo contiene registros del servicio dnsmasq.

`ebtables.txt`: El archivo contiene información sobre las tablas del cortafuegos.

`free.txt`: El archivo contiene información sobre la memoria disponible.

© Acronis International GmbH, 2003-2025

`ip.txt`: El archivo contiene los registros de la configuración de las interfaces de red, incluidos los nombres que pueden utilizarse en la configuración de **Capturar paquetes de red**.

`NetworkManager_log.txt`: El archivo contiene registros del servicio NetworkManager.

`NetworkManager_status.txt`: El archivo contiene información sobre el estado del servicio NetworkManager.

`openvpn@p2s_log.txt`: El archivo contiene los registros del servicio OpenVPN.

`openvpn@p2s_status.txt`: El archivo contiene información sobre el estado de los túneles de VPN.

`ps.txt`: El archivo contiene información sobre los procesos que se ejecutan actualmente en la puerta de enlace VPN o en el dispositivo VPN.

`resolf.conf.txt`: El archivo contiene información sobre la configuración de los servidores DNS.

`routes.txt`: El archivo contiene información sobre las rutas de conexión a redes virtuales.

`uname.txt`: El archivo contiene información sobre la versión actual del kernel del sistema operativo.

`uptime.txt`: El archivo contiene información sobre la longitud del periodo para el que el sistema operativo no se ha reiniciado.

`vpnserver_log.txt`: El archivo contiene los registros del servicio VPN.

`vpnserver_status.txt`: El archivo contiene información sobre el estado del servidor VPN.

Para obtener más información sobre los archivos de registro que son específicos de la conectividad VPN de IPsec, consulte "Archivos de registro de VPN de IPsec de varios sitios" (p. 1046).

Descarga de registros del dispositivo VPN

Puede descargar y extraer el archivo comprimido que contiene los registros del dispositivo VPN y utilizar la información para resolver problemas o supervisar objetivos.

Pasos para descargar los registros del dispositivo VPN

1. En la página **Conectividad**, haga clic en el icono de engranaje junto al dispositivo VPN.
2. Haga clic en **Descargar registro**.
3. [Opcional] Seleccione **Capturar paquetes de red** y configure los ajustes. Para obtener más información, consulte "Capturar paquetes de red" (p. 1060).
4. Haga clic en **Listo**.
5. Cuando el archivo .zip esté listo para descargarse, haga clic en **Descargar registro** y guárdelo de forma local.

Descarga de registros de la puerta de enlace VPN

Puede descargar y extraer el archivo comprimido que contiene los registros de la puerta de enlace VPN y utilizar la información para resolver problemas o supervisar objetivos.

Pasos para descargar los registros de la puerta de enlace VPN

© Acronis International GmbH, 2003-2025

1. En la página **Conectividad**, haga clic en el icono de engranaje junto a la puerta de enlace VPN.
2. Haga clic en **Descargar registro**.
3. [Opcional] Seleccione **Capturar paquetes de red** y luego configure los ajustes. Para obtener más información, consulte "Capturar paquetes de red" (p. 1060).
4. Haga clic en **Listo**.
5. Cuando el archivo .zip esté listo para descargarse, haga clic en **Descargar registro** y guárdelo de forma local.

Capturar paquetes de red

Para solucionar problemas y analizar la comunicación entre el sitio de producción local y un servidor principal o de recuperación, puede elegir recopilar paquetes de red en la puerta de enlace VPN o en el dispositivo VPN.

Cuando se recopilan 32 000 paquetes de red o se llega al límite de tiempo, la captura de paquetes de red se detiene y los resultados se escriben en un archivo .libpcap que se añade al archivo ZIP de registros.

La siguiente tabla proporciona más información sobre los ajustes de **Capturar paquetes de red** que puede configurar.

Configuración	Descripción
Nombre de la interfaz de red	Interfaz de red en la que capturar paquetes de red. Si desea capturar paquetes de red en todas las interfaces de red, seleccione **Cualquiera**.
Límite temporal (segundos)	El límite temporal para capturar paquetes de red. El valor máximo que puede establecer es 1800.
Filtrado	Un filtro extra para aplicar a los paquetes de red capturados. Puede introducir una cadena con protocolos, puertos, direcciones, y sus combinaciones, separada por un espacio, como "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp", y "esp". Si desea utilizar paréntesis, ponga espacios antes y después. También puede introducir direcciones IP y de red, por ejemplo: "icmp o arp" y "puerto 67 o 68". Para obtener más información acerca de los valores que puede introducir, consulte la ayuda tpcdump de Linux.

Servidores de nube

Con Disaster Recovery a Cyber Protect Cloud, puede utilizar dos tipos de servidores de nube: principal y de recuperación.

© Acronis International GmbH, 2003-2025

Un servidor principal es una máquina virtual que no está vinculada a un equipo en el sitio local. Puede utilizar servidores principales para proteger una aplicación específica o ejecutar varios servicios auxiliares (como un servidor web).

Un servidor de recuperación es una máquina virtual réplica del equipo original (servidor protegido). El servidor de recuperación se basa en las copias de seguridad del servidor protegido que se almacenan en la nube. En caso de un desastre, los servidores de recuperación se utilizan para cambiar los recursos informáticos de los servidores originales.

Configuración de servidores de recuperación

Servidor de recuperación: réplica del equipo original basada en las copias de seguridad del servidor protegido almacenadas en el cloud. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.

Al crear un servidor de recuperación, debe especificar los siguientes parámetros de red:

Parámetro	Descripción
Red en la nube	(Obligatorio) La red en la nube a la que se conectará un servidor de recuperación.
Dirección IP en la red de producción	(Obligatorio) La dirección IP con la que se inicia una máquina virtual para un servidor de recuperación. Esta dirección se usa tanto para la red de producción como para la de prueba. Antes de iniciar la máquina virtual, esta se configura para obtener la dirección IP mediante DHCP.
Dirección IP de prueba	(Opcional) La dirección IP para acceder a un servidor de recuperación desde la red de cliente-producción durante la prueba de conmutación por error, para evitar que la dirección IP de producción se duplique en la misma red. Esta dirección IP es distinta de la de la red de producción. Los servidores en el sitio local pueden alcanzar el servidor de recuperación durante la prueba de conmutación por error a través de la dirección IP, pero el acceso en la dirección contraria no está disponible. El servidor de recuperación en la red de prueba dispone de acceso a Internet si se seleccionó la opción **Acceso a Internet** durante la creación de dicho servidor.
Dirección IP pública	(Opcional) La dirección IP para acceder a un servidor de recuperación desde Internet. Si un servidor no tiene dirección IP pública, solo es alcanzable desde la red local.
Acceso a Internet	(Opcional) Permite que un servidor de recuperación acceda a Internet (tanto en el caso de producción como en el de la prueba de conmutación por error).

© Acronis International GmbH, 2003-2025

Creación de un servidor de recuperación

Para crear un servidor de recuperación que será una copia de su carga de trabajo, siga el procedimiento que aparece a continuación. También puede ver el vídeo tutorial que muestra el proceso.

Importante
Cuando realice una conmutación por error, puede seleccionar solo los puntos de recuperación que se crearon después de crear el servidor de recuperación.

Requisitos previos

- Se debe aplicar un plan de protección al equipo original que quiera proteger. Este plan debe realizar copias de seguridad de todo el equipo o solo de los discos. Estas son necesarias para arrancar y proporcionar los servicios necesarios a un almacenamiento en la nube.
- Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para crear un servidor de recuperación

1. En la pestaña **Todos los dispositivos**, seleccione la máquina que desea proteger.
2. Haga clic en **Recuperación ante desastres** y, luego, en **Crear servidor de recuperación**.
3. En el asistente **Crear servidor de recuperación**, en la pestaña **Configuración del servidor**, haga lo siguiente:
   a. Seleccione el número de núcleos virtuales y el tamaño de la RAM.

      Nota
      Puede ver los puntos de cálculo para cada opción. El número de puntos de cálculo indican el coste de funcionamiento del servidor de recuperación por hora. Para obtener más información, consulte "Puntos de cálculo" (p. 1076).

   b. [Opcional] Cambie el nombre predeterminado del servidor de recuperación.
   c. [Opcional] Agregue una descripción.
4. En la pestaña **Red**, haga lo siguiente:
   a. Especifique la red en el cloud a la que se conectará el servidor.
   b. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	Esta es la configuración predeterminada. Un servidor DHCP en la nube configurado automáticamente proporcionará la dirección IP del servidor.
Personalizado	Su propio servidor DHCP en la nube proporcionará la dirección IP del servidor.

© Acronis International GmbH, 2003-2025

c. Especifique la **dirección MAC**.

La dirección MAC es un identificador único asignado al adaptador de red del servidor. Si usa un DHCP personalizado, puede configurarlo para que siempre asigne una dirección IP específica a una dirección MAC concreta. Así, se garantiza que el servidor de recuperación siempre tenga la misma dirección IP. Puede ejecutar aplicaciones con licencias registradas con la dirección MAC.

d. Especifique la dirección IP que tendrá el servidor en la red de producción. La dirección IP del equipo original se establece de forma predeterminada.

Nota

Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.

Si usa un servidor DHCP personalizado, deberá especificar la misma dirección IP en la **Dirección IP en la red de producción** que la configurada en el servidor DHCP. De lo contrario, la conmutación por error de prueba no funcionará correctamente y no será posible alcanzar el servidor mediante una dirección IP pública.

e. [Opcional] Marque la casilla de verificación de **Dirección IP de prueba** y, a continuación, especifique la dirección IP.

Si selecciona esta configuración, podrá probar una conmutación por error en la red de prueba aislada y conectarse al servidor de recuperación mediante escritorio remoto o SSH durante una conmutación por error de prueba. Durante una conmutación por error de prueba, la puerta de enlace de VPN sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT.

Si no selecciona la configuración, la consola será la única forma de acceder al servidor durante una conmutación por error de prueba.

Nota

Si utiliza un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.

Puede seleccionar una de las direcciones IP propuestas o introducir otra.

f. [Opcional] Marque la casilla de verificación de **acceso a Internet**.

Si selecciona esta configuración, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o de producción. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.

g. [Opcional] Marque la casilla de verificación **Usar dirección IP pública**.

Con una dirección IP pública, el servidor de recuperación se vuelve accesible desde Internet durante una conmutación por error o una conmutación por error de prueba. Si no selecciona esta configuración, el servidor solo estará disponible en su red de producción.

La opción **Usar dirección IP pública** requiere que esté seleccionada la opción **Acceso a Internet**.

© Acronis International GmbH, 2003-2025

La dirección IP pública se mostrara cuando finalice la configuración. De forma predeterminada, el puerto TCP 443 está abierto para las conexiones de entrada a direcciones IP públicas.

Nota
Si borra la casilla de verificación **Usar dirección IP pública** o elimina el servidor de recuperación, su dirección IP pública no se reservará.

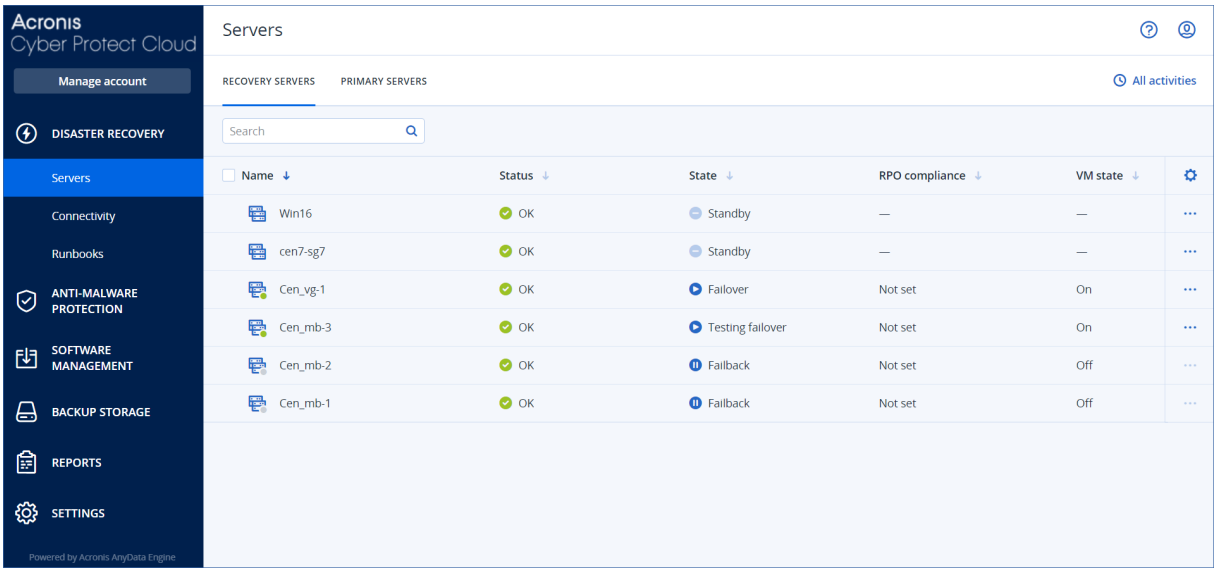
5. En la pestaña **Configuración**, seleccione **Establecer el umbral de RPO** y, a continuación, establezca el valor.
   El umbral de RPO define el intervalo temporal máximo entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
6. [Opcional] [Si las copias de seguridad del equipo seleccionado están cifradas utilizando el cifrado como una propiedad del equipo], especifique la contraseña que se utilizará automáticamente al crear una máquina virtual para el servidor de recuperación a partir de la copia de seguridad cifrada.
   a. Haga clic en **Introducir contraseña**, introduzca la contraseña de la copia de seguridad cifrada y defina un nombre para las credenciales.
      De forma predeterminada, verá la copia de seguridad más reciente en la lista.
   b. Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.
   c. Haga clic en **Guardar**.

Nota
Tenga en cuenta que, aunque la contraseña que especifique se guardará en un almacén de credenciales seguro, es posible que incumpla sus obligaciones legales si la guarda.

7. En la pestaña **Reglas del cortafuegos de la nube**, edite las reglas de firewall predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 1073).
8. Haga clic en **Crear**.

En la consola de Cyber Protect, el servidor de recuperación aparece en la pestaña **Disaster Recovery** > **Servidores** > **Servidores de recuperación**.

© Acronis International GmbH, 2003-2025



Operaciones con servidores de recuperación

En la consola de Cyber Protect, los servidores principales se muestran en la pestaña **Disaster Recovery** > **Servidores** > **Servidores de recuperación**.

Encender

Para encender un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Encender**.

Apagar

Para apagar un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, haga clic en **Apagar**.

Apagado forzoso

Para forzar el apagado de un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, seleccione **Forzar apagado del servidor** y, a continuación, haga clic en **Apagar**.

Detener

Pasos para parar un servidor de recuperación

© Acronis International GmbH, 2003-2025

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Detener**.

Editar configuración

Para editar la configuración de un servidor de recuperación

1. En la pestaña **Servidores de recuperación**, haga clic en el servidor de recuperación.
2. Haga clic en **Detener**.
3. Haga clic en **Editar** y, a continuación, edite la configuración.

Aplicar plan de protección

Pasos para aplicar un plan a un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. En la pestaña **Plan**, haga clic en **Crear**.
   Verá un plan de protección predefinido en el que solo puede cambiar las reglas de programación y retención. Para obtener más información, consulte "Copia de seguridad de los servidores de nube".

Configuración de servidores principales

Un **servidor principal** es una máquina virtual que no tiene un equipo enlazado en el sitio local, en comparación con un servidor de recuperación. Los servidores principales se utilizan para proteger una aplicación por replicación o para ejecutar varios servicios auxiliares (como un servidor web).

Normalmente, se usa un servidor principal para la replicación de datos en tiempo real en servidores que ejecuten aplicaciones fundamentales. La replicación la configura usted mismo con herramientas nativas de la aplicación. Por ejemplo, la replicación de Active Directory o de SQL se puede configurar entre los servidores locales y el principal.

Como alternativa, un servidor principal se puede incluir en un grupo de disponibilidad AlwaysOn (AGG) o un grupo de disponibilidad de base de datos (DAG).

Ambos métodos requieren un profundo conocimiento de la aplicación y los derechos del administrador. Un servidor principal consume constantemente recursos informáticos y espacio del almacenamiento rápido de recuperación ante desastres. Necesita mantenimiento por su parte, como el control de la replicación, la instalación de actualizaciones de software y la realización de copias de seguridad. Las ventajas son los RPO y RTO mínimos con una carga mínima del entorno de producción (en comparación con la realización de copias de seguridad de servidores completos en la cloud).

Los servidores principales solo se inician en la red de producción y tienen los siguientes parámetros de red:

© Acronis International GmbH, 2003-2025

Parámetro	Descripción
Red en la nube	(Obligatorio) La red en la nube a la que se conectará un servidor principal.
Dirección IP en la red de producción	(Obligatorio) La dirección IP que tendrá el servidor principal en la red de producción. La primera dirección IP libre de su red de producción se establece de forma predeterminada.
Dirección IP pública	(Opcional) La dirección IP para acceder a un servidor principal desde Internet. Si un servidor no tiene dirección IP pública, solo se podrá acceder a él desde la red local y no desde Internet.
Acceso a Internet	(Opcional) Permite que un servidor principal tenga acceso a Internet.

Creación de un servidor principal

Requisitos previos

Se debe establecer uno de los tipos de conectividad en el sitio en el cloud.

Pasos para crear un servidor principal

1. Vaya a la pestaña **Disaster Recovery** > **Servidores** > **Servidores principales**.
2. Haga clic en **Crear**.
3. En el asistente **Crear servidor principal**, en la pestaña **Configuración del servidor**, haga lo siguiente:
   a. Seleccione una plantilla para el nuevo equipo virtual.
   b. Seleccione la variante de la configuración (el número de núcleos virtuales y el tamaño de la RAM).
   La siguiente tabla muestra la cantidad total máxima de espacio en el disco (GB) para cada variante.

Tipo	vCPU	RAM (GB)	Cantidad total máxima de espacio en el disco (GB)
F1	1	2	500
F2	1	4	1,000
F3	2	8	2,000
F4	4	16	4,000
F5	8	32	8,000
F6	16	64	16,000
F7	16	128	32,000
F8	16	256	64,000

© Acronis International GmbH, 2003-2025

c. [Opcional] Cambie el tamaño de los discos virtuales. Si necesita más de un disco duro, haga clic en **Agregar disco** y, a continuación, especifique el nuevo tamaño de disco. Puede añadir hasta 10 discos en un servidor principal.

d. Cambie el nombre predeterminado del servidor de recuperación.

e. Agregue una descripción.

4. En la pestaña **Red**, haga lo siguiente:

a. Especifique la red de cloud en la que se incluirá el servidor principal.

b. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	Esta es la configuración predeterminada. Un servidor DHCP en la nube configurado automáticamente proporcionará la dirección IP del servidor.
Personalizado	Su propio servidor DHCP en la nube proporcionará la dirección IP del servidor.

c. Especifique la **dirección MAC**.

La dirección MAC es un identificador único que se asigna al adaptador de red del servidor. Si usa un DHCP personalizado, puede configurarlo para que siempre asigne una dirección IP específica a una dirección MAC concreta. Así se garantiza que el servidor principal siempre tenga la misma dirección IP. Puede ejecutar aplicaciones con licencias que se registran en la dirección MAC.

d. Especifique la dirección IP que tendrá el servidor en la red de producción.

La primera dirección IP libre de su red de producción se establece de forma predeterminada.

Nota

Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.

Si usa un servidor DHCP personalizado, deberá especificar la misma dirección IP en la **Dirección IP en la red de producción** que la configurada en el servidor DHCP. De lo contrario, la conmutación por error de prueba no funcionará correctamente y no será posible alcanzar el servidor mediante una dirección IP pública.

e. [Opcional] Marque la casilla de verificación de **acceso a Internet**.

Si selecciona esta opción, el servidor principal tendrá acceso a Internet. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.

f. [Opcional] Marque la casilla de verificación **Usar dirección IP pública**.

Con una dirección IP pública, el servidor principal se vuelve accesible desde Internet. Si no selecciona esta configuración, el servidor solo estará disponible en su red de producción.

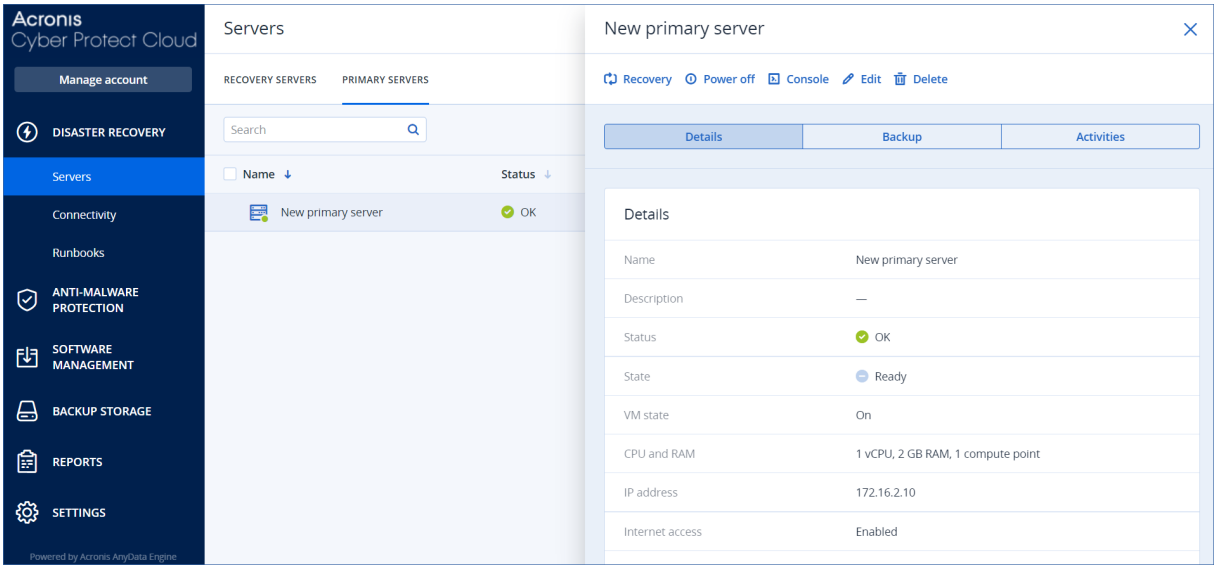
© Acronis International GmbH, 2003-2025

La dirección IP pública se mostrara cuando finalice la configuración. De forma predeterminada, el puerto TCP 443 está abierto para las conexiones de entrada a direcciones IP públicas.

Nota
Si borra la casilla de verificación **Usar dirección IP pública** o elimina el servidor de recuperación, su dirección IP pública no se reservará.

5. [Opcional] En la pestaña **Configuración**, seleccione **Establecer el umbral de RPO** y, a continuación, establezca el valor.
   El umbral de RPO determina el intervalo temporal máximo entre el último punto de recuperación y el momento presente. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
6. [Opcional] En la pestaña **Reglas de cortafuegos de la nube**, edite las reglas de firewall predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 1073).
7. Haga clic en **Crear**.

El servidor principal estará disponible en la red de producción. Puede gestionar el servidor mediante su consola, el escritorio remoto, SSH o TeamViewer.



Operaciones con servidores principales

En la consola de Cyber Protect, los servidores principales se muestran en la pestaña **Disaster Recovery** > **Servidores** > **Servidores principales**.

Encender

Pasos para encender un servidor principal

© Acronis International GmbH, 2003-2025

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Encender**.

Apagar

Pasos para apagar un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, haga clic en **Apagar**.

Apagado forzoso

Pasos para forzar el apagado de un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Apagar**.
3. En la pantalla **Apagar servidor**, seleccione **Forzar apagado del servidor** y, a continuación, haga clic en **Apagar**.

Detener

Pasos para parar un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Detener**.

Editar configuración

Pasos para editar la configuración de un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. Haga clic en **Detener**.
3. Haga clic en **Editar** y, a continuación, edite la configuración.

Aplicar plan de protección

Pasos para aplicar un plan a un servidor principal

1. En la pestaña **Servidores principales**, haga clic en el servidor principal.
2. En la pestaña **Plan**, haga clic en **Crear**.
   Verá un plan de protección predefinido en el que solo puede cambiar las reglas de programación y retención. Para obtener más información, consulte "Copia de seguridad de los servidores de nube".

Vista de detalles sobre servidores e la nube

Para ver los detalles de los servidores de nube, vaya a **Disaster Recovery** > **Servidores**. Allí encontrará dos pestañas: **Servidores de recuperación** y **Servidores principales**. Para mostrar

© Acronis International GmbH, 2003-2025

todas las columnas opcionales de la tabla, haga clic en el icono de engranaje.

Puede encontrar la siguiente información acerca de cada servidor si lo selecciona.

Nombre de la columna	Descripción
Nombre	Un nombre de servidor de cloud que ha definido usted
Rango	El rango que refleja el problema más grave con un servidor de cloud (en función de las alertas activas)
Estado	Estado de un servidor en la nube
Estado del equipo virtual	El estado de energía de un equipo virtual asociado con un servidor de cloud.
Ubicación activa	Ubicación en la que se aloja un servidor en la nube. Por ejemplo, **Nube**.
Umbral de RPO	El intervalo temporal máximo permitido entre el último punto de recuperación viable para una conmutación por error y el momento presente. El valor puede establecerse entre 15-60 minutos, 1-24 horas y 1-14 días.
Cumplimiento de RPO	El Cumplimiento de RPO es la proporción entre los RPO reales y el Umbral de RPO. El Cumplimiento de RPO se muestra si se ha definido el Umbral de RPO. Se calcula de la siguiente forma: **Cumplimiento de RPO = RPO reales / Umbral de RPO** donde **RPO reales = hora actual – último tiempo de punto de recuperación** **Rangos de cumplimiento de RPO** Dependiendo del valor de la proporción entre los RPO reales y el Umbral de RPO, se usan los siguientes rangos: • **Dentro del umbral**. El Cumplimiento de RPO es < 1x. Un servidor cumple el Umbral de RPO. • **Superado**. El Cumplimiento de RPO es <= 2x. Un servidor infringe el Umbral de RPO. • **Superado en gran medida**. El Cumplimiento de RPO es <= 4x. Un servidor infringe el Umbral de RPO más de 2 veces. • **Superado severamente**. El Cumplimiento de RPO es > 4x. Un servidor infringe el Umbral de RPO más de 4 veces. • **Pendiente (no hay copias de seguridad)**. El servidor está protegido con el plan de protección, pero la copia de seguridad está en proceso de creación y no se ha completado aún.
RPO reales	Tiempo transcurrido desde la creación del último punto de recuperación

© Acronis International GmbH, 2003-2025

Último punto de recuperación	La fecha y la hora en las que se creó el último punto de recuperación

Copias de seguridad de servidores de nube

Se realiza una copia de seguridad sin agente de la nube de los servidores principales y de recuperación. Estas copias de seguridad tienen las siguientes restricciones.

- La única ubicación de copia de seguridad posible es el almacenamiento en la nube. Las copias de seguridad de los servidores principales se realizan en el almacenamiento de **copias de seguridad de los servidores principales**.

  Nota
  No se admiten ubicaciones de copia de seguridad de Microsoft Azure.

- No se puede aplicar un plan de copias de seguridad a varios servidores. Cada servidor debe tener su propio plan de copias de seguridad, incluso si todos los planes de copias de seguridad tienen la misma configuración.
- Solo se puede aplicar un plan de copias de seguridad a un servidor.
- No es compatible con la copia de seguridad compatible con la aplicación.
- El cifrado no está disponible.
- Las opciones de copia de seguridad no están disponibles.

Cuando elimina un servidor principal, las copias de seguridad también se eliminan.

Se realiza una copia de seguridad de un servidor de recuperación únicamente en estado de conmutación por error. Sus copias de seguridad siguen la secuencia de copia de seguridad del servidor original. Cuando se lleva a cabo una conmutación por recuperación, el servidor original puede continuar esta secuencia de copia de seguridad. Por lo tanto, las copias de seguridad del servidor de recuperación solo se pueden eliminar manualmente o como resultado de la aplicación de reglas de retención. Cuando se elimina un servidor de recuperación, sus copias de seguridad se conservan siempre.

Nota
Los planes de copias de seguridad para servidores de la nube se realizan en hora UTC.

Reglas de cortafuegos para servidores en la nube

Puede configurar las reglas de cortafuegos para controlar el tráfico de entrada y de salida del servidor principal y el de recuperación en su sitio de la nube.

Puede configurar las reglas de entrada después de suministrar una dirección IP pública para el servidor de la nube. De forma predeterminada, el puerto TCP 443 está habilitado y el resto de las conexiones de entrada están denegadas. Puede cambiar las reglas de cortafuegos predeterminadas

© Acronis International GmbH, 2003-2025

y añadir o eliminar excepciones de entrada. Si no se ha suministrado una IP pública, solo podrá ver las reglas de entrada, pero no configurarlas.

Puede configurar las reglas de salida después de suministrar acceso a Internet para el servidor de la nube. De forma predeterminada, el puerto TCP 25 está denegado y el resto de las conexiones de salida están permitidas. Puede cambiar las reglas de cortafuegos predeterminadas y añadir o eliminar excepciones de salida. Si no se ha suministrado acceso a Internet, solo podrá ver las reglas de salida, pero no configurarlas.

Nota
Por motivos de seguridad, hay reglas de cortafuegos predeterminadas que no puede cambiar.

Para las conexiones de entrada y de salida:

- Permiso ping: Solicitud de eco ICMP (tipo 8, código 0) y respuesta de eco ICMP (tipo: 0, código: 0)
- Permiso ICMP necesario para fragmentar (tipo 3, código 4)
- Permiso TTL excedido (tipo 11, código 0)

Solo para conexiones de entrada:

- Parte no configurable: Rechazar todos

Solo para conexiones de salida:

- Parte no configurable: Rechazar todo

Configuración de reglas de cortafuegos para servidores en la nube

Puede editar las reglas de cortafuegos predeterminadas para los servidores primarios y de recuperación en la nube.

Pasos para editar las reglas de cortafuegos de un servidor de su sitio en la nube

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Si desea editar las reglas de cortafuegos de un servidor de su sitio en la nube, haga clic en la pestaña **Servidores de recuperación**. De manera alternativa, si desea editar las reglas de cortafuegos de un servidor principal, haga clic en la pestaña **Servidores principales**.
3. Haga clic en el servidor y después haga clic en **Editar**.
4. Haga clic en la pestaña **Reglas de cortafuegos de la nube**.
5. Si desea cambiar la acción predeterminada para las conexiones de entrada:

© Acronis International GmbH, 2003-2025

a. En el campo desplegable **Entrada**, seleccione la acción predeterminada.

Acción	Descripción
Rechazar todo	Rechaza cualquier tráfico de entrada. Puede añadir excepciones y permitir el tráfico desde direcciones IP específicas, protocolos y puertos.
Permitir todo	Permite todo el tráfico TCP y UDP de entrada. Puede añadir excepciones y rechazar el tráfico desde direcciones IP específicas, protocolos y puertos.

Nota
Al cambiar la acción predeterminada se invalida y elimina la configuración de las reglas de entrada existentes.

b. [Opcional] Si desea guardar las excepciones existentes, seleccione **Guardar excepciones completadas** en la ventana de confirmación.

c. Haga clic en **Confirmar**.

6. Si desea añadir una excepción:

a. Haga clic en **Agregar Excepción**.

b. Especifique los parámetros del cortafuegos.

Parámetro de cortafuegos	Descripción
Protocolo	Seleccione el protocolo para la conexión. Se admiten las siguientes opciones: • **TCP** • **UDP** • **TCP+UDP**
Puerto del servidor	Seleccione los puertos a los que se aplica la regla. Puede especificar lo siguiente: • un número de puerto específico (por ejemplo, `2298`) • un intervalo de números de puerto (por ejemplo, `6000-6700`) • cualquier número de puerto. Utilice `*` si desea que la regla se aplique a cualquier número de puerto.
Dirección IP del cliente	Seleccione las direcciones IP a las que se aplica la regla. Puede especificar lo siguiente: • una dirección IP específica (por ejemplo, `192.168.0.0`) • un intervalo de direcciones IP que utilicen la notación CIDR (por ejemplo, `192.168.0.0/24`) • cualquier dirección IP. Utilice `*` si desea que la regla se aplique a cualquier dirección IP.

© Acronis International GmbH, 2003-2025

7. Si desea eliminar una excepción de entrada existente, haga clic en el icono de la papelera junto a la excepción.
8. Si desea cambiar la acción predeterminada para las conexiones de salida:
   a. En el campo desplegable **Salida**, seleccione la acción predeterminada.

Acción	Descripción
Rechazar todo	Rechaza cualquier tráfico de salida. Puede añadir excepciones y permitir el tráfico a direcciones IP específicas, protocolos y puertos.
Permitir todo	Deniega todo el tráfico de salida. Puede añadir excepciones y rechazar el tráfico desde direcciones IP específicas, protocolos y puertos.

Nota
Al cambiar la acción predeterminada se invalida y elimina la configuración de las reglas de salida existentes.

   b. [Opcional] Si desea guardar las excepciones existentes, seleccione **Guardar excepciones completadas** en la ventana de confirmación.
   c. Haga clic en **Confirmar**.
9. Si desea añadir una excepción:
   a. Haga clic en **Agregar Excepción**.
   b. Especifique los parámetros del cortafuegos.

Parámetro de cortafuegos	Descripción
Protocolo	Seleccione el protocolo para la conexión. Se admiten las siguientes opciones: • **TCP** • **UDP** • **TCP+UDP**
Puerto del servidor	Seleccione los puertos a los que se aplica la regla. Puede especificar lo siguiente: • un número de puerto específico (por ejemplo, `2298`) • un intervalo de números de puerto (por ejemplo, `6000-6700`) • cualquier número de puerto. Utilice `*` si desea que la regla se aplique a cualquier número de puerto.
Dirección IP del cliente	Seleccione las direcciones IP a las que se aplica la regla. Puede especificar lo siguiente: • una dirección IP específica (por ejemplo, `192.168.0.0`) • un intervalo de direcciones IP que utilicen la notación CIDR (por

© Acronis International GmbH, 2003-2025

Parámetro de cortafuegos	Descripción
	ejemplo, `192.168.0.0/24`) • cualquier dirección IP. Utilice `*` si desea que la regla se aplique a cualquier dirección IP.

10. Si desea eliminar una excepción de salida existente, haga clic en el icono de la papelera junto a la excepción.
11. Haga clic en **Guardar**.

Comprobación de las actividades del cortafuegos de la nube

Después de actualizar la configuración de las reglas del cortafuegos de un servidor de la nube, un registro de la actividad de actualización estará disponible en la consola de Cyber Protect. Puede ver el registro y comprobar la siguiente información:

- nombre del usuario que actualizó la configuración
- fecha y hora de la actualización
- configuración de cortafuegos para conexiones de entrada y de salida
- acciones predeterminadas para conexiones de entrada y de salida
- protocolos, puertos y direcciones IP de las excepciones para conexiones de entrada y de salida

Pasos para ver la información sobre el cambio de configuración de las reglas de un cortafuegos de la nube

1. En la consola de Cyber Protect, haga clic en **Supervisión** > **Actividades**.
2. Haga clic en la actividad correspondiente y en **Todas las propiedades**.
   La descripción de la actividad debe ser **Actualizando configuración del servidor en la nube**.
3. En el campo **contexto**, inspeccione la información que le interese.

Puntos de cálculo

En Disaster Recovery a Cyber Protect Cloud, los puntos de cálculo se utilizan para los servidores principales y los servidores de recuperación durante fallos en las pruebas y en la producción. Los puntos de cálculo reflejan los recursos de cálculo utilizados para ejecutar los servidores (máquinas virtuales) en la nube.

El consumo de los puntos de cálculo durante la recuperación ante desastres depende de los parámetros del servidor y la duración del periodo de tiempo durante el que el servidor se encuentra en el estado de conmutación por error. Cuanto más potente sea el servidor y más largo el periodo de tiempo, más puntos de cálculo se consumirán. Y cuantos más puntos de cálculo se consuman, mayor será el precio que se cobrará.

© Acronis International GmbH, 2003-2025

Todos los servidores que estén funcionando en Cyber Protect Cloud se cobrarán por puntos de cálculo en función de su configuración de variante e independientemente de su estado (encendido o apagado).

Los servidores de recuperación en estado de espera no consumen puntos de cálculo y no se cobrará por ellos.

En la siguiente tabla puede ver un ejemplo de ocho servidores en la nube con diferentes variantes y los puntos de cálculo correspondientes que consumirán por hora. Las variantes de los servidores se pueden cambiar en la pestaña **Detalles**.

Tipo	CPU	RAM	Puntos de cálculo
F1	1 vCPU	2 GB	1
F2	1 vCPU	4 GB	2
F3	2 vCPU	8 GB	4
F4	4 vCPU	16 GB	8
F5	8 vCPU	32 GB	16
F6	16 vCPU	64 GB	32
F7	16 vCPU	128 GB	64
F8	16 vCPU	256 GB	128

Con la información que figura en la tabla, puede estimar fácilmente cuántos puntos de cálculo consumirá un servidor (máquina virtual).

Por ejemplo, si quiere proteger una máquina virtual con 4 vCPU* de 16 GB de RAM con Disaster Recovery y una máquina virtual con 2 vCPU y 8 GB de RAM, la primera máquina virtual consumirá 8 puntos de cálculo por hora, y la segunda máquina virtual 4 puntos de cálculo por hora. Si ambas máquinas virtuales están en una conmutación por error, el consumo total será de 12 puntos de cálculo por hora o 288 puntos de cálculo por todo el día (12 puntos de cálculo x 24 horas = 288 puntos de cálculo).

* vCPU se refiere a una unidad central de procesamiento (CPU) física que se asigna a una máquina virtual y es una entidad dependiente del tiempo.

Nota
Si se alcanza el exceso de la cuota de **Puntos de cálculo**, todos los servidores principales y de recuperación se apagarán. No será posible utilizar estos servidores hasta el comienzo del siguiente período de facturación o hasta que aumente la cuota. El período de facturación predeterminado es un mes calendario completo.

© Acronis International GmbH, 2003-2025

Conmutación por error de prueba

Realizar una conmutación por error de prueba implica iniciar un servidor de recuperación en una VLAN de prueba aislada de su red productiva. Puede probar varios servidores de recuperación a la vez y comprobar su interacción. En la red de prueba, los servidores se comunican mediante sus direcciones IP de producción, pero no pueden iniciar las conexiones TCP o UDP en las cargas de trabajo de su red local.

Durante la conmutación por error de prueba, la máquina virtual (servidor de recuperación) no se apaga. El agente lee el contenido de los discos virtuales directamente desde la copia de seguridad y accede aleatoriamente a varias partes de ella. Esto podría hacer que el rendimiento del servidor de recuperación en el estado de conmutación por error de prueba sea más lento de lo normal.

Ejecución de una prueba de conmutación por error

Aunque la realización de una conmutación por error de prueba es opcional, le recomendamos que lo haga habitualmente con la frecuencia que considere adecuada, teniendo en cuenta el coste y la seguridad. Una práctica recomendada es crear un runbook, que es un conjunto de instrucciones en las que se describe la forma de iniciar el entorno de producción en el cloud.

Importante
Tiene que crear un servidor de recuperación antes para proteger sus dispositivos en caso de desastre.

Puede realizar una conmutación por error solo desde los puntos de recuperación (copias de seguridad) que se crearon después de crear el servidor de recuperación del dispositivo.

Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en un servidor de recuperación. Solo se permiten 100 puntos de recuperación como máximo.

Pasos para llevar a cabo una conmutación por error de prueba

1. Seleccione el equipo original o el servidor de recuperación que quiera probar.
2. Haga clic en **Disaster Recovery**.
   Se abre la descripción del servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione el tipo de conmutación por error **Conmutación por error de prueba**.
5. Seleccione el punto de recuperación (copia de seguridad) y haga clic en **Iniciar**.
6. Si la copia de seguridad que ha seleccionado está cifrada usando el cifrado como una propiedad del equipo:

© Acronis International GmbH, 2003-2025

a. Introduzca la contraseña de cifrado para la copia de seguridad establecida.

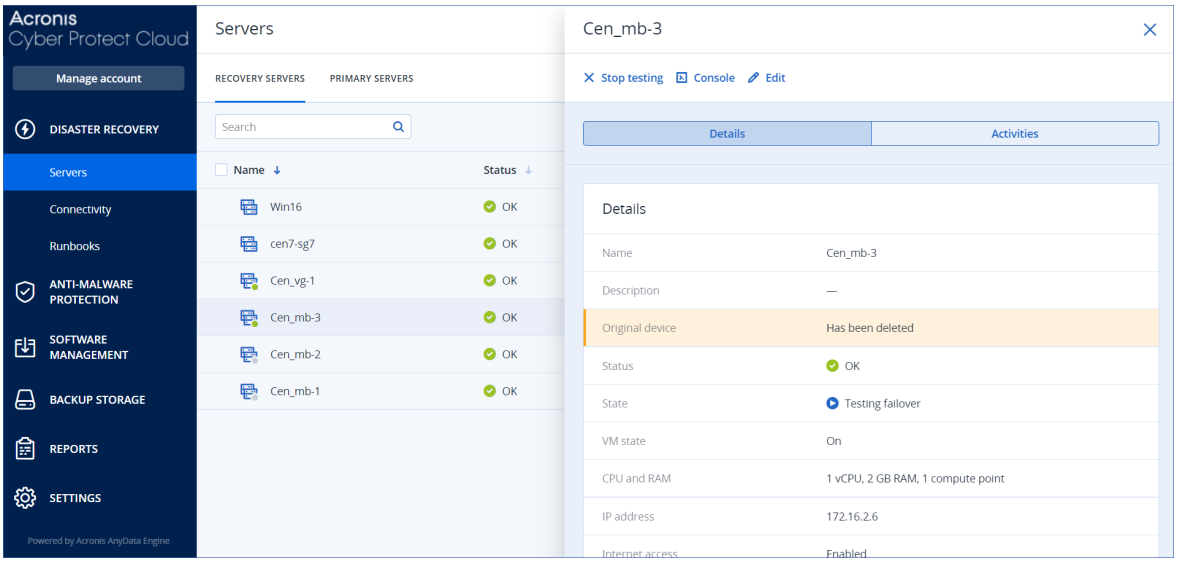
> **Nota**
> Solo se guardará la contraseña temporalmente y se utilizará para la operación de prueba de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales si se detiene la prueba de conmutación por error o una vez que esta se haya completado.

b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en el campo **Nombre de las credenciales**.

> **Importante**
> La contraseña se almacenará en un almacén de credenciales seguro y se aplicará automáticamente en las siguientes operaciones de conmutación por error. No obstante, es posible que incumpla sus obligaciones legales si guarda las contraseñas.

c. Haga clic en **Listo**.

Cuando el servidor de recuperación se inicia, su estado cambia a **Probando conmutación por error**.



7. Use uno de los siguientes métodos para probar el servidor de recuperación:
   - En **Disaster Recovery** > **Servidores**, seleccione el servidor de recuperación y, a continuación, haga clic en **Consola**.
   - Use el equipo remoto o SSH para conectarse al servidor de recuperación y a la dirección IP de prueba que especificó al crear el servidor de recuperación. Pruebe la conexión tanto desde el interior como desde el exterior de la red de producción (como se describe en "Conexión de punto a sitio").
   - Ejecute una secuencia de comandos en el servidor de recuperación.

© Acronis International GmbH, 2003-2025

El script puede comprobar la pantalla de inicio, si las aplicaciones se han iniciado, la conexión a Internet y la capacidad de otros equipos de conectarse al servidor de recuperación.

- Si el servidor de recuperación tiene acceso a Internet y una dirección IP pública, puede que quiera usar TeamViewer.

8. Cuando la prueba haya terminado, haga clic en **Detener comprobación**.
   El servidor de recuperación se detiene. Todos los cambios realizados en el servidor de recuperación durante la prueba de conmutación por error se pierden.

Conmutación por error de prueba automatizada

Con la conmutación por error de prueba automatizada, el servidor de recuperación se prueba automáticamente una vez al mes sin ninguna interacción manual.

El proceso de conmutación por error de prueba automatizada está formado por las siguientes partes:

1. creación de una máquina virtual desde el último punto de recuperación
2. captura de pantalla de la máquina virtual
3. análisis de si el sistema operativo de la máquina virtual empieza correctamente
4. notificación acerca del estado de la conmutación por error de prueba

Nota
La conmutación por error de prueba automatizada consume puntos de cálculo.

Puede configurar la conmutación por error de prueba automatizada en la configuración del servidor de recuperación. Para obtener más información, consulte "Configuración de la conmutación por error de prueba automatizada" (p. 1081).

Tenga en cuenta que, en casos muy excepcionales, la conmutación por error de prueba automatizada podría omitirse y no ejecutarse a la hora planificada. Esto se debe a que la conmutación por error de producción tiene mayor prioridad que la conmutación por error de prueba automatizada, de manera que los recursos de hardware (CPU y RAM) asignados para la conmutación por error de prueba automatizada podrían estar limitados temporalmente para garantizar que hay suficientes recursos para una conmutación por error de producción simultánea.

Si, por algún motivo, la conmutación por error de prueba se omite, se emitirá una alerta.

Nota
La conmutación por error de prueba automatizada fallará si las copias de seguridad del equipo original están cifradas utilizando el cifrado como una propiedad del equipo, y la contraseña de cifrado no se especifica al crear el servidor de recuperación. Para obtener más información sobre cómo especificar la contraseña de cifrado, consulte "Creación de un servidor de recuperación" (p. 1062).

© Acronis International GmbH, 2003-2025

Configuración de la conmutación por error de prueba automatizada

Al configurar la conmutación por error de prueba automatizada, puede probar el servidor de recuperación de forma mensual sin ejecutar ninguna acción manual.

Pasos para configurar la conmutación por error de prueba automatizada

1. En la consola, vaya a **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En la pestaña **Conmutación por error de prueba automatizada**, en el campo **Planificación**, seleccione **Mensual**.
4. [Opcional] En **Tiempo de espera de las capturas de pantalla**, cambia el valor predeterminado del periodo de tiempo máximo (en minutos) para que el sistema intente realizar la prueba de conmutación por error automatizada.
5. [Opcional] Si desea guardar el valor **Tiempo de espera de las capturas de pantalla** como predeterminado y que se rellene automáticamente cuando habilite la conmutación por error de prueba automatizada para el resto de servidores de recuperación, seleccione **Establecer como tiempo de espera predeterminado**.
6. Haga clic en **Guardar**.

Ver el estado de la conmutación por error de prueba automatizada

Puede ver la información de una conmutación por error de prueba automatizada completada, como el estado, la hora de inicio, la hora de finalización, la duración y la captura de pantalla de la máquina virtual.

Nota
La captura de pantalla de la máquina virtual se conserva hasta que la conmutación por error de la prueba automatizada se ejecuta de nuevo y genera una nueva captura de pantalla.

Pasos para ver el estado de la conmutación por error de prueba automatizada de un servidor de recuperación

1. En la consola, vaya a **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. En la sección **Conmutación por error de prueba automatizada**, compruebe la información de la última conmutación por error de prueba automatizada.
3. [Opcional] Para ver la captura de pantalla de la máquina virtual, haga clic en **Mostrar captura de pantalla**.

Deshabilitación de la conmutación por error de prueba automatizada

Puede deshabilitar la conmutación por error de prueba automatizada si desea ahorrar recursos o no necesita que se ejecute en determinado servidor de recuperación.

© Acronis International GmbH, 2003-2025

Pasos para deshabilitar la conmutación por error de prueba automatizada

1. En la consola, vaya a **Disaster Recovery** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En el asistente, haga clic en la pestaña **Conmutación por error de prueba automatizada**.
4. Desactive el interruptor **Conmutación por error de prueba automática**.
5. Haga clic en **Guardar**.

Conmutación por error de producción

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Al crear un servidor de recuperación, se queda en estado **En espera**. La máquina virtual correspondiente no existe hasta que inicie una conmutación por error. Antes de iniciar un proceso de conmutación por error, debe crear al menos una copia de seguridad de imágenes de disco (con volumen de arranque) del equipo original.

Al iniciar el proceso de conmutación por error, seleccione el punto de recuperación (copia de seguridad) del equipo original a partir del cual se creará una máquina virtual con los parámetros predefinidos. La operación de conmutación por error usa la funcionalidad "ejecutar equipo virtual a partir de una copia de seguridad". El servidor de recuperación obtiene el estado de transición **Finalización**. Este proceso consiste en transferir los discos virtuales del servidor desde el almacenamiento de copia de seguridad (almacenamiento "inactivo") hasta el almacenamiento de recuperación ante desastres (almacenamiento "de acceso frecuente").

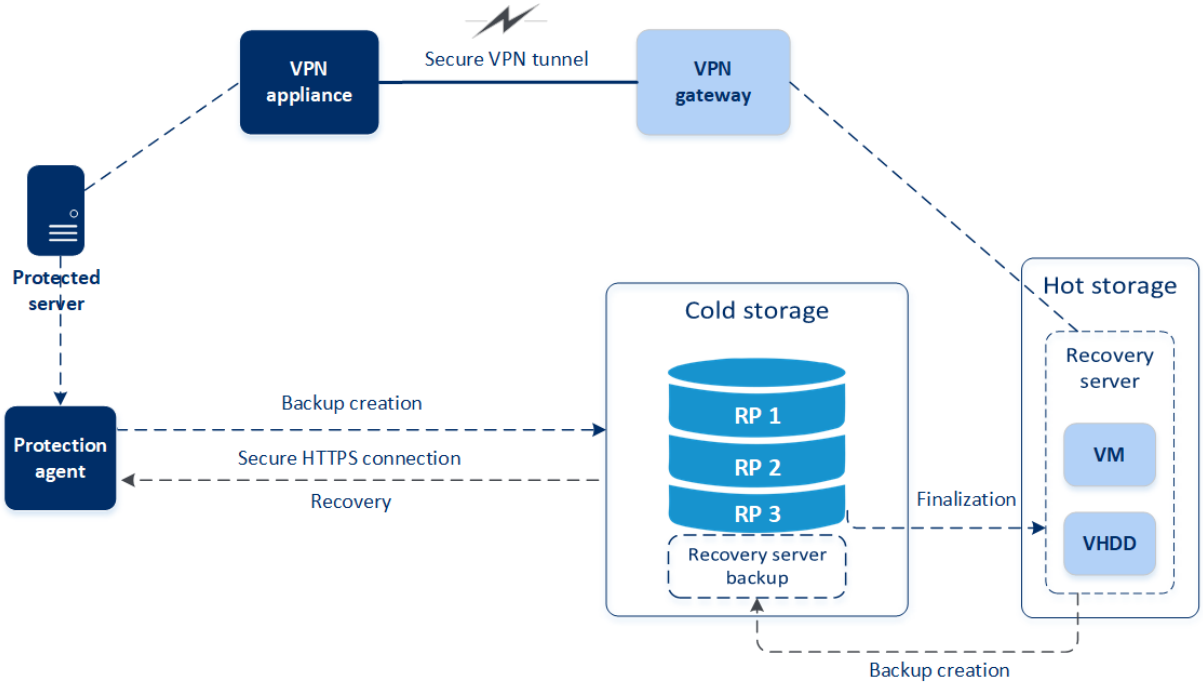
Nota
Durante el estado **Finalización**, el servidor es accesible y funcional, aunque su rendimiento será menor de lo normal. Puede abrir la consola del servidor haciendo clic en el enlace **La consola está lista**. El enlace está disponible en la columna **Estado de la máquina virtual** en la pantalla **Disaster Recovery** > **Servidores** y en la vista **Detalles** del servidor.

Cuando se complete el estado **Finalización**, el rendimiento del servidor alcanzará su valor normal. El estado del servidor cambia a **Conmutación por error**. Ahora, la carga de trabajo se traslada del equipo original al servidor de recuperación en el sitio en la nube.

Si el servidor de recuperación cuenta con un agente de protección en su interior, el servicio de agente se detiene para evitar que se produzca una interferencia (como el inicio de una copia de seguridad o la creación de informes sobre estados desactualizados al componente de copia de seguridad).

En el siguiente diagrama puede ver los procesos de conmutación por error y conmutación por recuperación.

© Acronis International GmbH, 2003-2025



Realización de una conmutación por error

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación por error es un proceso que consiste en mover una carga de trabajo a la cloud, además del estado en el que la carga de trabajo permanece en la cloud.

Al iniciar una conmutación por error, el servidor de recuperación se inicia en la red de producción. Para evitar interferencias y problemas no deseados, asegúrese de que la carga de trabajo original no está en línea ni se puede acceder a ella a través de la VPN.

Para evitar una interferencia de la copia de seguridad en el mismo archivo comprimido de la nube, revoque de forma manual el plan de protección de la carga de trabajo que se encuentra en el estado **Conmutación por error**. Para obtener más información sobre la revocación de planes, consulte Revocación de un plan de protección.

Importante
Tiene que crear un servidor de recuperación antes para proteger sus dispositivos en caso de desastre.

Puede realizar una conmutación por error solo desde los puntos de recuperación (copias de seguridad) que se crearon después de crear el servidor de recuperación del dispositivo.

Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en un servidor de recuperación. Solo se permiten 100 puntos de recuperación como máximo.

Puede seguir el procedimiento siguiente o ver el tutorial en vídeo.

© Acronis International GmbH, 2003-2025

Pasos para llevar a cabo una conmutación por error

1. Asegúrese de que el equipo original no esté disponible en la red.
2. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione **Conmutación por error en producción**.
5. Seleccione el punto de recuperación (copia de seguridad) y haga clic en **Iniciar**.
6. [Si la copia de seguridad que ha seleccionado está cifrada usando el cifrado como una propiedad del equipo]
   a. Introduzca la contraseña de cifrado para la copia de seguridad establecida.

      Nota
      Solo se guardará la contraseña temporalmente y se utilizará para la operación de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales una vez que se complete la operación de conmutación por error y el servidor vuelva al estado **En espera**.

   b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en el campo **Nombre de las credenciales**.

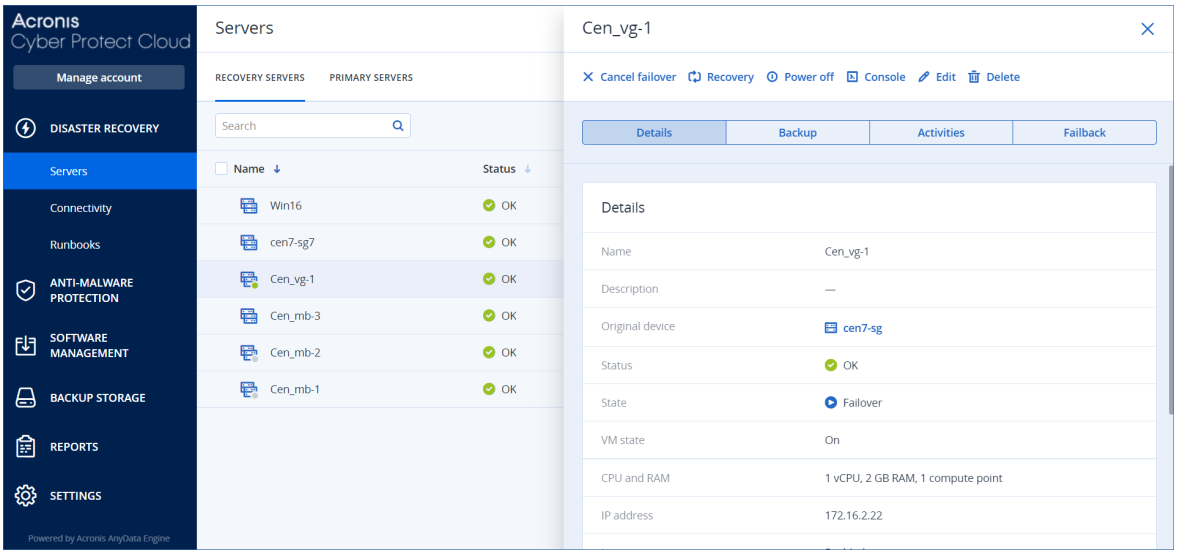
      Importante
      La contraseña se almacenará en un almacén de credenciales seguro y se aplicará automáticamente en las siguientes operaciones de conmutación por error. No obstante, es posible que incumpla sus obligaciones legales si guarda las contraseñas.

   c. Haga clic en **Listo**.

   Cuando el servidor de recuperación se inicia, su estado cambia a **Finalización** y, después de un tiempo, cambia a **Conmutación por error**.

Importante
Es importante saber que el servidor sigue estando disponible durante los estados **Finalización** y **Conmutación por error**. Durante el estado **Finalización**, puede acceder a la consola del servidor haciendo clic en el enlace **La consola está lista**. El enlace está disponible en la columna **Estado de la máquina virtual** en la pantalla **Disaster Recovery** > **Servidores** y en la vista **Detalles** del servidor.

© Acronis International GmbH, 2003-2025



7. Mire la consola del servidor de recuperación para asegurarse de que se ha iniciado. Haga clic en **Disaster Recovery** > **Servidores**, seleccione el servidor de recuperación y, a continuación, haga clic en **Consola**.
8. Asegúrese de que se pueda acceder al servidor de recuperación mediante la dirección IP de producción que haya especificado al crearlo.

Cuando el servidor de recuperación se haya apagado, se crea y se aplica automáticamente un nuevo plan de protección. Este plan de protección se basa en el que se usó para crear el servidor de recuperación, con ciertas limitaciones. En este plan, puede cambiar únicamente la planificación y las reglas de retención. Para obtener más información, consulte "Realización de copias de seguridad de servidores en la cloud".

Cómo realizar una conmutación por error de servidores mediante DNS local

Si su sitio local utiliza servidores DNS para resolver los nombres de los equipos, es posible que los servidores de recuperación no consigan comunicarse después de una conmutación por error. Esto sucede porque los servidores DNS de la nube son diferentes a los del sitio local. De manera predeterminada, los servidores de la nube recién creados utilizan los servidores DNS del sitio de la nube, pero puede configurar ajustes de DNS personalizados. Para obtener más información, consulte "Configuración de servidores DNS personalizados" (p. 1056).

Cómo se realiza una conmutación por error de un servidor DHCP

Su infraestructura local puede tener el servidor DHCP ubicado en un host Windows o Linux. Cuando se produce una conmutación por error al sitio de cloud en este tipo de host, se produce el problema de duplicación del servidor DHCP porque la puerta de enlace VPN en el cloud también realiza el rol DHCP. Para resolver este problema, realice uno de los siguientes procedimientos:

- Si solo se conmutó por error al cloud el host DHCP, mientras que el resto de los servidores locales siguen en el sitio local, deberá iniciar sesión en el host DHCP en el cloud y desactivar el servidor DHCP en él. De esta forma, no habrá conflictos y solo la puerta de enlace de VPN funcionará como el servidor DHCP.

© Acronis International GmbH, 2003-2025

- Si los servidores de cloud ya tienen la dirección IP del host DHCP, deberá iniciar sesión en el host DHCP en el cloud y desactivar el servidor DHCP en él. También debería iniciar sesión en los servidores del cloud y renovar la concesión DHCP para asignar las nuevas direcciones IP asignadas desde el servidor DHCP correcto (hospedado en la puerta de enlace de VPN).

Nota
Las instrucciones no serán válidas si su servidor DHCP en la nube se ha configurado con la opción **DHCP personalizado** y algunos de los servidores principales o de recuperación obtienen su dirección IP de dicho servidor DHCP.

Detener una conmutación por error

Puede detener una conmutación por error de producción en cualquier momento, durante cada fase del proceso.

Nota
Al detener una conmutación por error, se revierten todos los cambios que se realizaron desde el momento en que se inició, excepto las copias de seguridad del servidor de recuperación.

Pasos para detener una conmutación por error

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores** > **Servidores de recuperación**.
2. Seleccione el servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en el servidor de recuperación.
4. Haga clic en **Detener conmutación por error**.
5. En la ventana de confirmación que aparece, seleccione la casilla de verificación y, a continuación, haga clic en **Detener conmutación por error**.
   Se ha detenido la conmutación por error. El servidor de recuperación vuelve al estado **Espera**.

Conmutación por recuperación

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación por recuperación es un proceso que consiste en mover la carga de trabajo desde la nube a la máquina física o virtual en su sitio local. Puede realizar una conmutación tras recuperación en un servidor de recuperación en estado de **Conmutación por error** y seguir usando el servidor en su sitio local.

Puede ejecutar una conmutación por error automatizada en una máquina virtual o un equipo físico en su sitio local. Durante la conmutación tras recuperación, mientras la máquina virtual funciona en la nube, puede transferir los datos de la copia de seguridad al sitio local. Esta tecnología le ayuda a

© Acronis International GmbH, 2003-2025

obtener un tiempo de inactividad muy breve, que se calcula y aparece en la consola de Cyber Protect. Puede verlo y usar esta información para planificar sus actividades y, si fuese necesario, advertir a sus clientes sobre un próximo tiempo de inactividad. Si realiza conmutación tras recuperación basada en agente con un dispositivo de arranque, el tiempo de inactividad aún será menor, porque los cambios delta se transferirán al sitio local.

Para una conmutación tras recuperación a un equipo físico de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque. Para obtener más información, consulte "Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque" (p. 1089).

Para una conmutación tras recuperación a una máquina virtual de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque o la conmutación tras recuperación sin agente a través del agente de hipervisor. Para obtener más información, consulte "Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque" (p. 1089) y "Realización de conmutación tras recuperación sin agente a través de un agente de hipervisor" (p. 1093).

En casos específicos en los que no pueda usar el procedimiento de conmutación tras recuperación automatizada, puede realizarla de forma manual. Para obtener más información, consulte "Conmutación tras recuperación manual" (p. 1097).

Nota
Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Servidor de conmutación tras recuperación**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.

Conmutación tras recuperación basada en agente mediante dispositivo de arranque

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El proceso de conmutación tras recuperación basada en agente mediante dispositivos de arranque está optimizado para realizar una conmutación tras recuperación a la máquina física o virtual original. Durante este proceso, solo se transfieren los cambios delta al sitio local.

El proceso de conmutación tras recuperación basada en el agente a través de un dispositivo de arranque a una máquina física o virtual de destino consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras

© Acronis International GmbH, 2003-2025

recuperación y planifique el inicio de la transferencia de datos.

2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,

   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

   Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

   Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

   Nota

   El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.

   Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.
4. **Validación**. Durante esta fase, el equipo del sitio local estará listo y podrá reiniciarlo con un dispositivo de arranque basado en Linux. Compruebe que la máquina virtual funciona correctamente y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar la conmutación por error y volver a la fase de planificación.

   Nota

   Una vez que se haya reiniciado el dispositivo de arranque, no podrá volver a utilizarlo. Si descubre que algo va mal durante la fase de validación, debe registrar un nuevo dispositivo de arranque y volver a iniciar el proceso de conmutación tras recuperación.

   Sin embargo, al utilizarse la tecnología flashback, no se volverán a transferir los datos que ya estén en el sitio local y el proceso de conmutación tras recuperación será mucho más rápido.

© Acronis International GmbH, 2003-2025

Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación basada en agente mediante dispositivo de arranque en un equipo físico o una máquina virtual de destino en su sitio local.

Nota
El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.

Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Hay un dispositivo de arranque registrado disponible. Para obtener más información, consulte "Creación de dispositivos de arranque para recuperar sistemas operativos" en la guía del usuario de Cyber Protection.
- El equipo de destino es el equipo original en su sitio local o tiene el mismo firmware que el equipo original.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

Pasos para llevar a cabo una conmutación por recuperación de un equipo físico

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Tipo de conmutación tras recuperación**, seleccione **Basada en agente a través de dispositivo de arranque**.
5. En el campo **Dispositivo de arranque de destino**, haga clic en **Especificar**, seleccione el dispositivo de arranque y haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Nota
Le recomendamos que utilice un dispositivo de arranque listo porque ya estará configurado. Para obtener más información, consulte "Creación de dispositivos de arranque para recuperar sistemas operativos" en la guía del usuario de Cyber Protection.

6. [Opcional] Para cambiar la asignación de discos predeterminada, en el campo **Asignación de discos**, haga clic en **Especificar**, asigne los discos de la copia de seguridad a los discos del equipo de destino y haga clic en **Listo**.
7. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de transferencia de datos. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, los valores de **Progreso** aumentarán con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el progreso sea más rápido de lo que ha calculado inicialmente la consola.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el tiempo de inactividad sea mucho menor que el valor que ha mostrado inicialmente la consola.

8. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se iniciará la fase de cambio. La consola muestra la siguiente información:

© Acronis International GmbH, 2003-2025

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

9. Cuando se complete la fase de **cambio**, reinicie el dispositivo de arranque y compruebe que el equipo físico de su sitio local funciona según lo esperado.
   Para obtener más información, consulte "Recuperar discos usando dispositivos de arranque" en la guía del usuario de Cyber Protection.
10. Para finalizar el proceso, haga clic en **Confirmar la conmutación tras recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
    Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

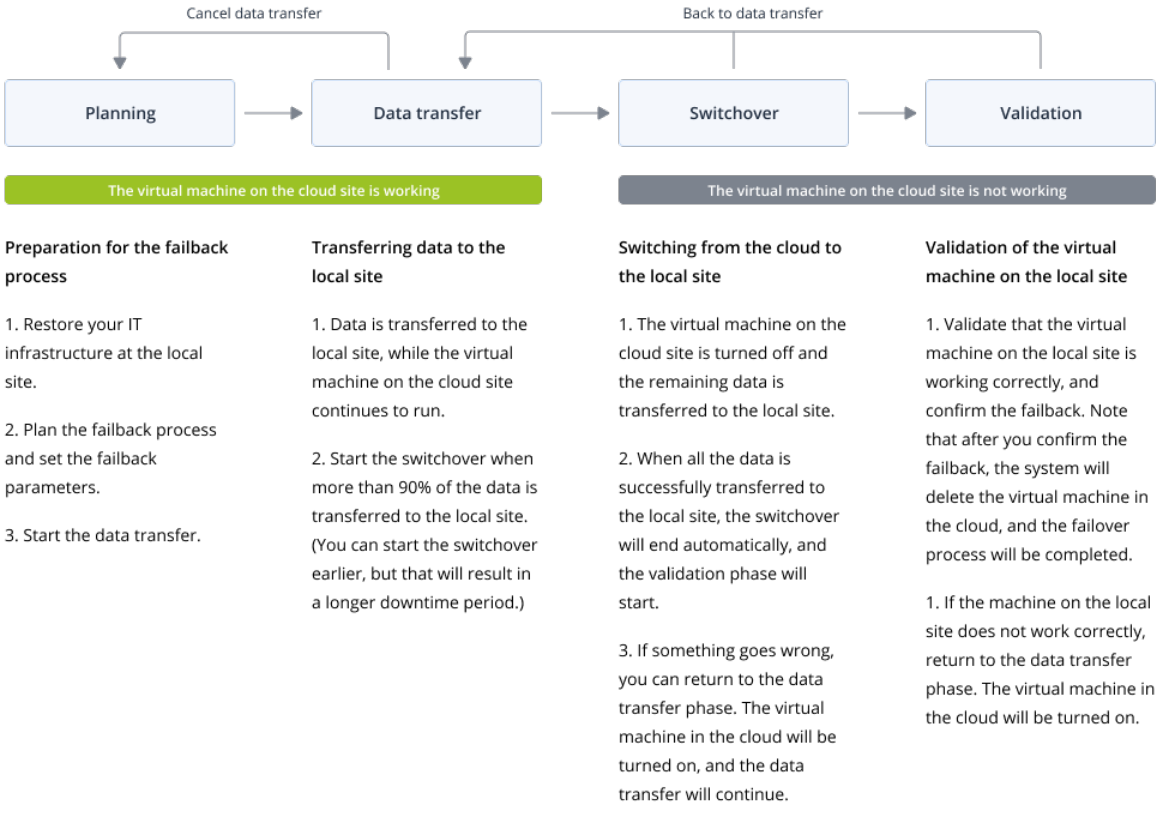
Conmutación tras recuperación sin agente a través de un agente de hipervisor

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación tras recuperación sin agente a través de un proceso de agente de hipervisor está optimizada para realizar una conmutación tras recuperación a una nueva máquina virtual. Si desea realizar una conmutación tras recuperación a la máquina virtual original, siga el procedimiento para la conmutación tras recuperación basada en agente mediante un dispositivo de arranque.

La conmutación tras recuperación sin agente mediante un agente de hipervisor consta de cuatro fases.

© Acronis International GmbH, 2003-2025



1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.

   Nota
   Para minimizar el tiempo total del proceso de conmutación tras recuperación, le recomendamos que inicie la fase de transferencia de datos inmediatamente después de configurar sus servidores locales y, a continuación, continúe con la configuración de la red y del resto de la infraestructura local durante la fase de transferencia de datos.

2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,

   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

© Acronis International GmbH, 2003-2025

Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

Si cancela el proceso de conmutación por recuperación durante la fase de transferencia de datos, los datos transferidos no se eliminarán del sitio local. Para evitar posibles problemas, elimine de forma manual los datos transferidos antes de iniciar un nuevo proceso de conmutación por recuperación. El posterior proceso de transferencia de datos se iniciará desde el principio.

3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.

   Puede ver el tiempo estimado de finalización (tiempo de inactividad) de esta fase en la consola de Cyber Protect. Cuando todos los datos se han transferido al sitio local (no hay pérdida de datos y la máquina virtual en el sitio local es una copia exacta de la máquina virtual en la nube), se completa la fase de cambio. Se recuperará la máquina virtual en el sitio local y se iniciará la fase de validación automáticamente.
4. **Validación**. Durante esta fase, la máquina virtual en el sitio local está lista y se inicia automáticamente. Puede verificar si la máquina virtual está funcionando correctamente, y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar el cambio y volver a la fase de transferencia de datos.

Realización de conmutación tras recuperación sin agente a través de un agente de hipervisor

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede realizar una conmutación tras recuperación sin agente a una máquina virtual de destino en su sitio local a través de un agente de hipervisor.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

© Acronis International GmbH, 2003-2025

Pasos para realizar una conmutación tras recuperación sin agente a una máquina virtual a través de un agente de hipervisor

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En la sección **Parámetros de la conmutación por recuperación**, en el campo **Tipo de conmutación tras recuperación**, seleccione **Sin agente a través del hipervisor** y, a continuación, configure los demás parámetros.

   Tenga en cuenta que, de manera predeterminada, algunos **Parámetros de la conmutación por recuperación** se establecen automáticamente con los valores sugeridos, pero puede cambiarlos.

   La siguiente tabla proporciona más información sobre los **Parámetros de la conmutación por recuperación**.

Parámetro	Descripción
Tamaño de la copia de seguridad	La cantidad de datos que se transferirán a su sitio local durante el proceso de conmutación por recuperación. Tras iniciar el proceso de conmutación por recuperación a un equipo virtual de destino, el **Tamaño de la copia de seguridad** aumentará durante la fase de transferencia de datos debido a que el equipo virtual en la nube seguirá funcionando y generando nuevos datos. Para calcular una estimación del período de inactividad durante el proceso de conmutación por recuperación a un equipo virtual de destino, tome el 10 % del valor del **Tamaño de la copia de seguridad** (puesto que recomendamos iniciar la fase de cambio tras haberse transferido el 90 % de los datos a su sitio local) y divídalo entre el valor de la velocidad de su conexión a Internet. **Nota** El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.
Ubicación del equipo de destino	Ubicación de la conmutación por recuperación: un servidor de VMware ESXi o de Microsoft Hyper-V. Puede elegir entre todos los servidores que tienen un agente registrado en el servicio de ciberprotección.
Agente	Agente que ejecutará la operación de conmutación por recuperación. Solo puede utilizar un agente para llevar a cabo una operación de conmutación por recuperación al mismo tiempo.

© Acronis International GmbH, 2003-2025

Parámetro	Descripción
	Puede seleccionar un agente que esté en línea y no se esté utilizando para otro proceso de conmutación por recuperación y que tenga una versión que admita la funcionalidad de conmutación por recuperación y derechos para acceder a la copia de seguridad. Tenga en cuenta que puede instalar varios agentes en servidores VMware ESXi e iniciar un proceso de conmutación por recuperación independiente con cada uno de ellos. Puede llevar a cabo estos procesos de conmutación por recuperación a la vez.
Configuración del equipo de destino	Configuración del equipo virtual: • **Procesadores virtuales**. Seleccione el número de procesadores virtuales. • **Memoria**. Seleccione cuánta memoria tendrá el equipo virtual. • **Unidades**. Seleccione las unidades para la memoria. • [Opcional] **Adaptadores de red**. Para añadir un adaptador de red, haga clic en **Agregar** y seleccione una red en el campo **Red**. Cuando haya acabado de hacer cambios, haga clic en **Listo**.
Ruta	(Para servidores de Microsoft Hyper-V) Carpeta en el servidor en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Almacén de datos	(Para servidores de VMware ESXi) Almacén de datos en el servidor en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Modo de aprovisionamiento	Método de asignación del disco virtual. Para servidores de Microsoft Hyper-V: • **Expansión dinámica** (valor predeterminado). • **Tamaño fijo**. Para servidores de Microsoft Hyper-V: • **Ligero** (valor predeterminado). • **Grueso**.
Nombre del equipo de destino	Nombre de la máquina de destino. De forma predeterminada, el nombre de la máquina de destino es el mismo que el del servidor de recuperación. El nombre del equipo de destino debe ser único en la **Ubicación del equipo de destino** seleccionada.

5. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

© Acronis International GmbH, 2003-2025

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de **transferencia de datos**. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, ambos valores del parámetro **Progreso** aumentarán con el paso del tiempo.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo.

6. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

7. Después de que se complete la fase de **Cambio** y se inicie automáticamente la máquina virtual en el sitio local, verifique que esté funcionando correctamente.
8. Para finalizar el proceso, haga clic en **Confirmar la conmutación por recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
   Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

© Acronis International GmbH, 2003-2025

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación manual

Nota
Le recomendamos que utilice el proceso de conmutación tras recuperación en un modo manual solo cuando se lo indique el equipo de soporte.

También puede iniciar un proceso de conmutación tras recuperación en un modo manual. En este caso, la transferencia de datos desde la copia de seguridad en la nube al sitio local no se llevará a cabo de forma automática. Se debe hacer de forma manual cuando la máquina virtual en la nube esté apagada. Esto hace que el proceso de conmutación tras recuperación en un modo manual sea mucho más lento y probablemente el tiempo de inactividad también sea mayor.

El proceso de conmutación tras recuperación en un modo manual consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.
2. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y se hará una copia de seguridad de los datos recién generados. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso. Cuando la copia de seguridad haya finalizado, restaure la máquina en el sitio local de forma manual. Puede recuperar el disco mediante un dispositivo de arranque o toda la máquina desde el almacenamiento de la copia de seguridad en la nube.
3. **Validación**. Durante esta fase, verifique que el equipo físico o la máquina virtual en el sitio local funciona correctamente y confirme la conmutación tras recuperación. Tras la confirmación, se eliminará la máquina virtual en el sitio en la nube y el servidor de recuperación volverá al estado **En espera**.

Realización de una conmutación tras recuperación manual

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación en un equipo físico o una máquina virtual de destino en su sitio local.

Pasos para llevar a cabo una conmutación tras recuperación manual

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Destino**, seleccione **Equipo físico**.
5. Haga clic en el icono de engranaje y habilite el conmutador **Usar el modo manual**.
6. [Opcional] Calcule una estimación del período de inactividad durante el proceso de conmutación por recuperación mediante la división del valor del **Tamaño de la copia de seguridad** entre el valor de la velocidad de su conexión a Internet.

   Nota
   El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.

7. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se apagará la máquina virtual en el sitio en la nube.

   Nota
   Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

8. Recupere el servidor desde una copia de seguridad en la nube al equipo físico o a la máquina virtual en su sitio local. Para obtener más información, consulte "Recuperar un equipo" en la guía del usuario de Cyber Protection.
9. Asegúrese de que la recuperación se complete y de que la máquina recuperada funcione correctamente y haga clic en **Se ha restaurado el equipo**.
10. Si todo funciona según lo esperado, haga clic en **Confirmar la conmutación por recuperación** y en la ventana de confirmación vuelva a hacer clic en **Confirmar**.
    El servidor de recuperación y los puntos de recuperación pasarán a estar disponibles para la conmutación por error. Para crear puntos de recuperación, aplique un plan de protección al nuevo servidor local.

    Nota
    Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

© Acronis International GmbH, 2003-2025

Conmutación tras recuperación desde Cyber Protect Cloud a una máquina virtual de Azure

Puede realizar una conmutación tras recuperación desde Cyber Protect Cloud al equipo virtual de Azure original siguiendo el procedimiento para "Realización de una conmutación tras recuperación manual" (p. 1097) y utilizando una de las siguientes opciones de recuperación en el paso 8.

Opciones de recuperación

- Recuperación sin agente

  Soporta la recuperación solo a una nueva máquina virtual de Microsoft Azure que se crea automáticamente.

  Configure la conexión de Azure en la consola de Cyber Protect (**Dispositivos** > **Agregar** > **Máquina virtual de Microsoft Azure**).

  Se despliega una máquina virtual de dispositivo de copia de seguridad en la suscripción de Azure para gestionar la recuperación.

  Flujo de recuperación:

  1. En la pantalla de **Almacenamiento de la copia de seguridad**, seleccione una copia de seguridad.
  2. Recupere como una máquina virtual de Azure.

  Puede utilizar el mismo flujo para copias de seguridad físicas, virtuales o basadas en agente.

  Para reducir los costes incurridos, la máquina virtual del dispositivo, cuando se utiliza solo para la recuperación, se puede encender solo durante la recuperación y luego se puede apagar manualmente.
- Recuperación basada en agente

  Admite la recuperación en la misma máquina virtual de Azure (si la máquina virtual original con el agente está disponible) o en una nueva máquina virtual de Azure que tenga un nuevo agente instalado.

  El proceso consiste en los siguientes pasos:

  1. Cree manualmente una máquina virtual limpia de Windows o Linux en Azure.
  2. Instale el agente de protección.
  3. Utilice el agente para examinar y recuperar copias de seguridad de Acronis Cloud Storage.

  Para obtener más información, consulte Recuperación de máquinas de Microsoft Azure y Amazon EC2.

Organización (runbooks)

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

© Acronis International GmbH, 2003-2025

Un runbook es un conjunto de instrucciones que describe cómo iniciar el entorno de producción en la nube. Puede crear runbooks en la consola de Cyber Protect.

Con los runbooks, puede:

- Automatizar la conmutación por error de uno o varios servidores.
- Hacer ping en la dirección IP del servidor y comprobar la conexión al puerto que especifique para poder comprobar automáticamente el resultado de la conmutación por error.
- Establecer la secuencia de operaciones de los servidores mediante la ejecución de aplicaciones distribuidas.
- Incluir operaciones manuales en el flujo de trabajo.
- Verifique la integridad de su solución de recuperación ante desastres mediante la ejecución de runbooks en modo de prueba.

Para acceder a la pantalla **Runbooks**, seleccione **Disaster Recovery** > **Runbooks**.

Creación de un runbook

Un runbook consiste en pasos que se ejecutan consecutivamente. Un paso consiste en acciones que comienzan simultáneamente.

Para crear un runbook, siga las instrucciones del siguiente procedimiento o del tutorial en vídeo.

Para crear un runbook

1. En la consola de Cyber Protection, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en **Crear runbook**.
3. Haga clic en **Añadir paso**.
4. Haga clic en **Añadir acción** y seleccione la acción que quiere añadir al paso.

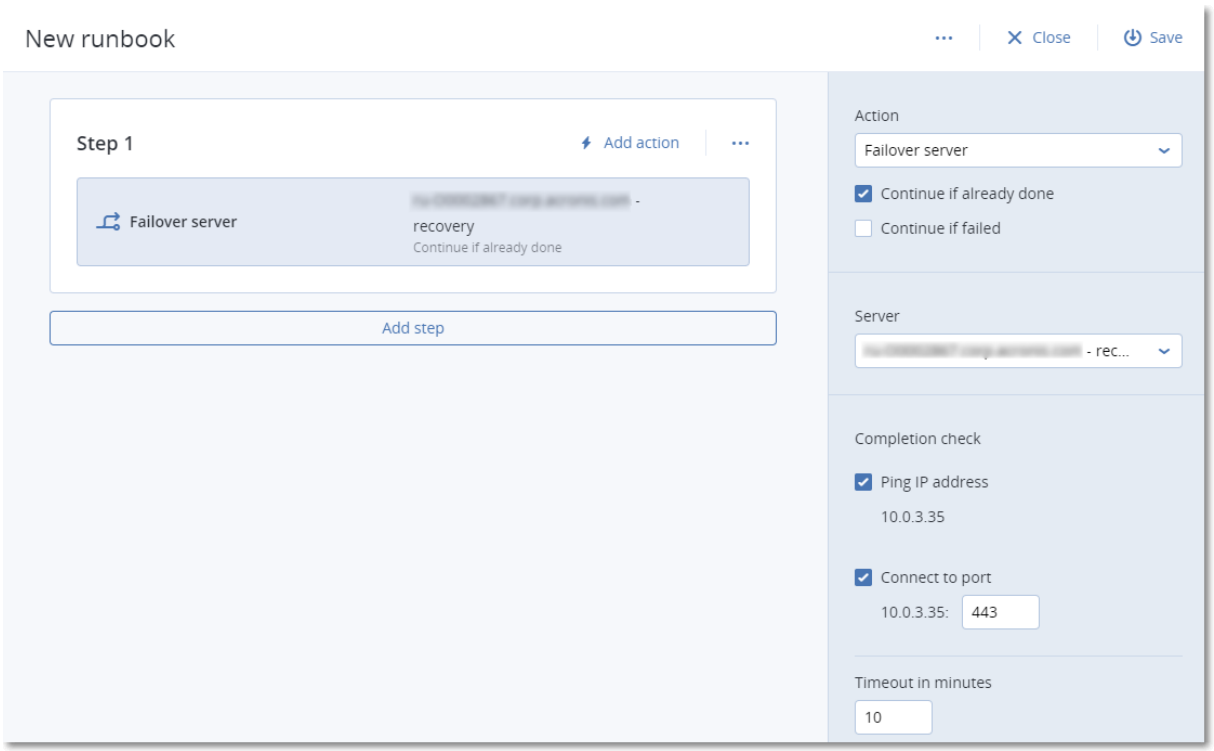
Acción	Descripción
Conmutar por error el servidor	Realiza una conmutación por error de un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook" (p. 1102). **Nota** Si la copia de seguridad del servidor que selecciona está cifrada utilizando el cifrado como una propiedad del equipo, la acción de **Conmutar por error el servidor** se detendrá y cambiará automáticamente a **Se requiere interacción**. Para continuar con la ejecución del runbook, tendrá que proporcionar la contraseña de la copia de seguridad cifrada.
Conmutar por recuperación el servidor	Realiza una conmutación tras recuperación de un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener

© Acronis International GmbH, 2003-2025

Acción	Descripción
	más información sobre estas configuraciones, consulte "Parámetros de runbook" (p. 1102). **Nota** Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Conmutar por recuperación el servidor**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.
Iniciar servidor	Inicia un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook" (p. 1102). **Nota** La acción de **Iniciar servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Detener servidor	Detiene un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook" (p. 1102). **Nota** La acción **Detener servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Operación manual	Una operación manual requiere una interacción de un usuario. Para definir esta acción, debe ingresar una descripción. Cuando una secuencia de runbook llega a una operación manual, el runbook se detendrá y no procederá hasta que un usuario realice la operación manual requerida, como hacer clic en el botón de confirmación.
Ejecutar runbook	Ejecuta otro runbook. Para definir esta acción, debe elegir un runbook. Un runbook puede estar formado únicamente por una ejecución de un runbook determinado. Por ejemplo, si añade la acción "ejecutar Runbook A", puede incluir la acción "ejecutar Runbook B", pero no puede añadir otra acción "ejecutar Runbook A".

© Acronis International GmbH, 2003-2025

5. Defina los parámetros del runbook para la acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook" (p. 1102).
6. [Opcional] Para añadir una descripción del paso:
   a. Haga clic en el icono de puntos suspensivos y, luego, en **Descripción**.
   b. Introduzca una descripción del paso.
   c. Haga clic en **Listo**.
7. Repita los pasos del 3 al 6 hasta que cree la secuencia de pasos y acciones deseada.
8. [Opcional] Para cambiar el nombre predeterminado del runbook:
   a. Haga clic en el icono de puntos suspensivos.
   b. Introduzca el nombre del runbook.
   c. Introduzca una descripción del runbook.
   d. Haga clic en **Listo**.
9. Haga clic en **Guardar**.
10. Haga clic en **Cerrar**.



Parámetros de runbook

Los parámetros de runbook son configuraciones específicas que debe configurar para definir una acción del runbook. Hay dos categorías de parámetros de runbook: parámetros de acción y parámetros de comprobación de si los archivos están completos.

Los parámetros de acción definen el comportamiento del runbook dependiendo del estado inicial de la acción o el resultado.

© Acronis International GmbH, 2003-2025

Los parámetros de comprobación de si los archivos están completos aseguran que el servidor esté disponible y ofrezca los servicios necesarios. Si una comprobación de si los archivos están completos falla, se considera que la acción ha fallado.

En la tabla a continuación se describen los parámetros configurables del runbook para cada acción.

Parámetro de runbook	Categoría	Disponible para actuar	Descripción
Continuar si ya se ha realizado	Parámetro de acción	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el servidor**	Este parámetro define el comportamiento del runbook cuando la acción requerida ya se ha realizado (por ejemplo, ya se ha realizado una conmutación por error o un servidor ya está en funcionamiento). Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook también falla. Por defecto, este parámetro está habilitado.
Continuar si falla	Parámetro de acción	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el servidor**	Este parámetro define el comportamiento del runbook cuando la acción requerida falla. Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook también falla. Por defecto, este parámetro está desactivado.
Hacer ping a la dirección IP	Verificación de finalización	• **Iniciar servidor**	El software hará ping a la dirección IP de producción del servidor en el cloud hasta que este responda o expire el tiempo de espera, lo que ocurra primero.
Conectar a puerto (443 de forma predeterminada)	Verificación de finalización	• **Conmutar por error el servidor** • **Iniciar servidor**	El software usará la dirección IP de producción del servidor en el cloud y el puerto que usted especifique para intentar conectarse a él hasta que se establezca la conexión o expire el tiempo de espera, lo que ocurra primero. De esta forma, puede comprobar si la aplicación que se detecta en el puerto especificado se encuentra en funcionamiento.

© Acronis International GmbH, 2003-2025

Parámetro de runbook	Categoría	Disponible para actuar	Descripción
Tiempo de espera en minutos	Verificación de finalización	• **Conmutar por error el servidor** • **Iniciar servidor**	El tiempo de espera predeterminado es de 10 minutos.

Operaciones con runbooks

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para acceder a la lista de operaciones, mueva el ratón sobre un runbook y haga clic en el icono de puntos suspensivos. Cuando un runbook no funciona, puede llevar a cabo las siguientes operaciones:

- **Ejecutar**
- **Editar**
- **Clonar**
- **Eliminar**

Ejecución de un runbook

Cada vez que haya clic en **Ejecutar**, se le pedirá que establezca los parámetros de la ejecución. Estos parámetros se aplicarán a todas las operaciones de conmutación por error y por recuperación incluidas en el runbook. Los runbooks especificados en las operaciones **Ejecutar runbook** heredan estos parámetros del runbook principal.

- **Modo conmutación por error y conmutación por recuperación**
  Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación por recuperación se corresponderá con el modo de conmutación por error elegido.
- **Punto de recuperación de conmutación por error**
  Elija el punto de recuperación más reciente (opción predeterminada) o seleccione un momento específico del pasado. Si elige la segunda opción, se seleccionarán los puntos de recuperación más cercanos a la fecha y la hora especificadas para cada servidor.

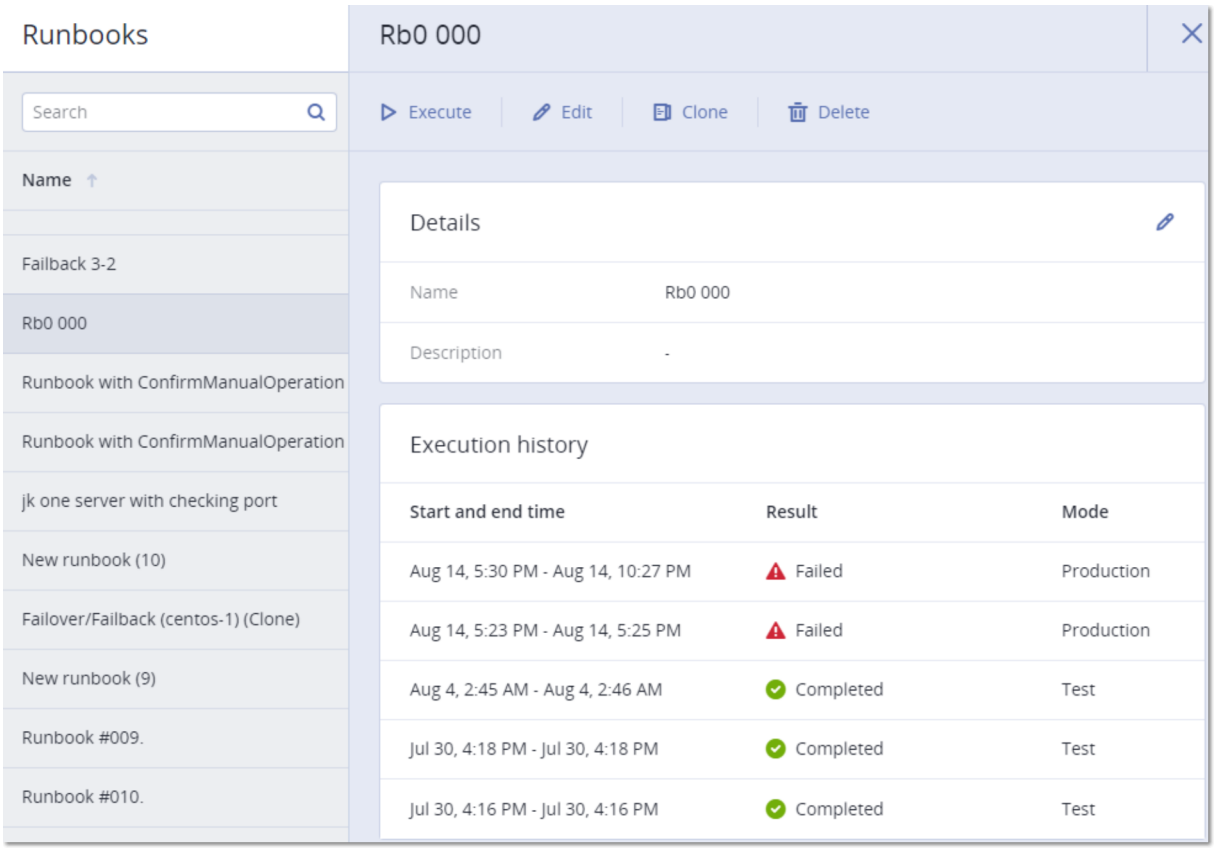
Detención de la ejecución de un runbook

Durante la ejecución de un runbook, puede seleccionar la opción **Detener** en la lista de operaciones. El software completará todas las acciones que ya se hayan iniciado excepto aquellas que requieran interacción del usuario.

© Acronis International GmbH, 2003-2025

Visualización del historial de ejecuciones

Al seleccionar un runbook de la pestaña **Runbooks**, el software muestra información sobre él y el historial de ejecuciones. Haga clic en la línea que corresponda a una ejecución específica para ver el registro de ejecuciones.



Eliminar el sitio de recuperación ante desastres

Puede eliminar el sitio de recuperación ante desastres. Esta acción eliminará automáticamente la puerta de enlace de VPN, las conexiones de VPN y todos los runbooks que se configuraron en el sitio.

Requisitos previos

No hay servidores en la nube disponibles en el sitio de recuperación de desastres.

Pasos para eliminar el sitio de recuperación ante desastres

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Haga clic en **Eliminar el sitio de recuperación ante desastres**.
4. En la ventana de confirmación, haga clic en **Eliminar**.

© Acronis International GmbH, 2003-2025

Disaster Recovery para Microsoft Azure

Disaster Recovery para Microsoft Azure es una solución de recuperación ante desastres asequible e integrada con el servicio Acronis Cyber Protection. Aprovecha la potencia y flexibilidad de la plataforma de nivel empresarial de Microsoft Azure como destino del sitio de DR. Esta solución utiliza copias de seguridad en frío (puntos de recuperación), que se pueden almacenar en Microsoft Azure, Acronis Cyber Protect Cloud o en un almacenamiento en la nube alojado por un partner. La configuración y orquestación del sitio de recuperación ante desastres se gestionan de forma centralizada desde la consola de Cyber Protect. Se utiliza su propia suscripción de Microsoft Azure como destino del sitio de DR.

La automatización y la orquestación incluyen las siguientes capacidades:

- Configuración inicial del sitio de DR
- Prueba de conmutación por error automatizada con verificación de captura de pantalla impulsada por IA
- Conmutación por error orquestada
- Conmutación tras recuperación automatizada a equipos físicos y máquinas virtuales, con un tiempo de inactividad casi nulo
- Runbooks para automatizar los escenarios clave de recuperación ante desastres
- Trabajadores bajo demanda (agentes temporales) que eliminan la necesidad de dispositivos virtuales permanentes
- DR en frío: las copias de seguridad se almacenan en el almacenamiento, pero no se ejecutan recursos de procesamiento (máquinas virtuales) hasta que se produce un desastre. DR en frío proporciona una recuperación rentable con un uso mínimo de la infraestructura de Azure.
- DR en caliente (disponible en futuras versiones): las copias de seguridad se replican de forma incremental en el almacenamiento intermedio de Azure y, en caso de desastre, están listas para ejecutarse como máquinas virtuales de Azure. El DR en caliente proporciona un RTO casi nulo.

Usted mantiene el control total sobre la infraestructura subyacente y las capacidades de Microsoft Azure, con la flexibilidad de utilizar los servicios nativos de Azure o integrar soluciones personalizadas, como firewalls de terceros y dispositivos SD-WAN, conectándolos a las redes de recuperación seleccionadas en el sitio de DR. Esta solución también admite la conmutación por error de escritorios de Windows que ejecutan Windows 10 o Windows 11.

Nota
Para utilizar Disaster Recovery en Microsoft Azure, debe tener una suscripción activa a Microsoft Azure.

© Acronis International GmbH, 2003-2025

Requisitos de software para Disaster Recovery en Microsoft Azure

Sistemas operativos compatibles

La protección con un servidor de recuperación en Microsoft Azure se ha probado para los siguientes sistemas operativos:

- Ubuntu 20.x, 21.x, 22.10, 23.04
- Debian 10.x, 11.x
- Red Hat Enterprise Linux 8.x, 9.x
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server
- Windows Server 2025: todas las opciones de instalación, excepto Nano Server
- Windows 10
- Windows 11

Es posible que este software funcione con otros sistemas operativos de Windows y distribuciones Linux, pero no se lo podemos asegurar.

Plataformas de virtualización compatibles

La protección de equipos virtuales con un servidor de recuperación se ha probado para las siguientes plataformas de virtualización:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Máquinas virtuales basadas en Kernel (KVM): solo invitados completamente virtualizados (HVM). No se admiten invitados paravirtualizados (PV).

Se admite las cargas de trabajo de Linux que tienen copias de seguridad sin agente desde un SO invitado y tienen volúmenes con las configuraciones de Logical Volume Manager (LVM).

© Acronis International GmbH, 2003-2025

Se admite las cargas de trabajo de Windows que tienen copias de seguridad sin agente desde un SO invitado y tienen configuraciones de discos dinámicos (LDM).

Puede que este software funcione con otras plataformas de virtualización y versiones, pero no se lo podemos asegurar.

Limitaciones

Las siguientes plataformas y configuraciones no son compatibles con Disaster Recovery en Microsoft Azure:

1. Plataformas no compatibles:
   - Agentes para Virtuozzo.
   - macOS
2. Configuraciones no compatibles:

   Microsoft Windows
   - El servicio de Active Directory no es compatible con la replicación FRS.
   - Los dispositivos extraíbles sin formateo GPT o MBR (también llamado "superfloppy") no son compatibles.

   Linux
   - Sistemas de archivos sin tabla de partición.
   - Cargas de trabajo de Linux de las que se realiza una copia de seguridad con un agente de desde un SO invitado y que tienen volúmenes con las siguientes configuraciones avanzadas de Logical Volume Manager (LVM): Volúmenes segmentados, volúmenes replicados o volúmenes RAID 0, RAID 4, RAID 5, RAID 6 o RAID 10.

   Nota
   Las cargas de trabajo con varios sistemas operativos instalados no son compatibles.
3. Modos de inquilino no compatibles:
   - La recuperación ante desastres no está disponible cuando el modo de cumplimiento está habilitado para el inquilino.
4. Tipos de copias de seguridad no compatibles:
   - Los puntos de recuperación de Protección continua de datos (CDP) no son compatibles.

     Importante
     Si crea un servidor de recuperación a partir de una copia de seguridad que tenga un punto de recuperación CDP, perderá los datos incluidos en este punto de recuperación durante la conmutación por recuperación o al crear una copia de seguridad de un servidor de recuperación.
   - Las copias de seguridad de datos forenses no se pueden usar para crear servidores de recuperación.

Los servidores en la cloud no se cifran.

© Acronis International GmbH, 2003-2025

Licencia de Disaster Recovery para Microsoft Azure

Para habilitar Disaster Recovery en Microsoft Azure, el elemento de oferta **DR y copia de seguridad directa en Azure** debe estar habilitado para su inquilino. Este elemento de oferta habilita:

- Disaster Recovery (DR) a Azure que utiliza la suscripción de Azure del cliente.
- Copia de seguridad directa en Azure que no requiere Advanced Backup.

Se consume una cuota del elemento de la oferta cuando se crea un servidor de recuperación o se habilita la copia de seguridad directa en Azure. Se utiliza solo una cuota por carga de trabajo, incluso si tanto DR como la copia de seguridad directa están activas.

La cuota para este elemento de oferta que se asigna a su inquilino representa el número máximo de cargas de trabajo que se pueden proteger. Un dispositivo que utiliza tanto Disaster Recovery a Azure como la protección de copia de seguridad directa en Azure consume una cuota.

Cuota estricta excedida

Cuando se reduce la cuota estricta del elemento de la oferta, los servidores de recuperación existentes pueden quedar sin licencia. El número de servidores de recuperación sin licencia depende del exceso. Los servidores de recuperación que estaban en conmutación por error de prueba o de producción siguen siendo funcionales, pero quedan sin licencia. Los servidores de recuperación sin licencia en modo de espera tienen operaciones de DR limitadas. No puede encender los servidores sin licencia hasta que vuelvan a tener una.

Aumentar la cuota del elemento de oferta asigna automáticamente licencias a dispositivos no licenciados y elimina las alertas relacionadas.

Alertas generadas

Se generan las siguientes alertas cuando hay problemas causados por la falta de licencias.

- **El servidor de recuperación no tiene licencia**: esta alerta se genera cuando un servidor queda sin licencia.
- **La protección de Disaster Recovery se desactivó para una carga de trabajo**: esta alerta se genera cuando no hay licencias disponibles.
- **La conmutación por error de prueba automatizada ha fallado**: esta alerta se genera cuando se bloquea una conmutación por error debido a que falta una licencia.

Trabajar con Disaster Recovery en Microsoft Azure

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

El flujo de trabajo básico para utilizar la recuperación ante desastres es el siguiente:

© Acronis International GmbH, 2003-2025

1. Configure su sitio de DR en Microsoft Azure. Para obtener más información, consulte "Creación de un sitio de recuperación ante desastres en Microsoft Azure" (p. 1113).
2. Cree un servidor de recuperación de la carga de trabajo que desea proteger. Para obtener más información, consulte "Creación de servidores de recuperación en Microsoft Azure" (p. 1122).
3. [Opcional] Configure la conectividad desde su sitio local al sitio en la nube en Microsoft Azure mediante los servicios nativos de Azure, como la VPN de sitio a sitio de Azure o Azure ExpressRoute. Para obtener más información, consulte "Conectividad y redes en Microsoft Azure" (p. 1115).
4. [Opcional] Configure los runbooks. Para obtener más información, consulte "Creación de un runbook en Microsoft Azure" (p. 1149).
5. Configure la conmutación por error de prueba automatizada o realice una conmutación por error de prueba. Para obtener más información, consulte "Configuración de la conmutación por error de prueba automatizada en Microsoft Azure" (p. 1132) y "Realización de una prueba de conmutación por error en Microsoft Azure" (p. 1130).
6. [Cuando se produce un desastre] Realice una conmutación por error de producción. Para obtener más información, consulte "Realización de una conmutación por error de producción en Microsoft Azure" (p. 1128).
7. [Después del desastre] Realice una conmutación tras recuperación al sitio local. Para obtener más información consulte "Conmutación tras recuperación en Microsoft Azure" (p. 1135).

Gestionar el acceso a su suscripción de Microsoft Azure

Disaster Recovery a Microsoft Azure requiere que se conecte a una suscripción de Microsoft Azure en la consola de Cyber Protect.

Puede configurar las suscripciones de Microsoft Azure en la pantalla **Infraestructura** > **Nubes públicas**. Allí también puede gestionar sus suscripciones, realizando las siguientes tareas: renovar el acceso a la suscripción, ver las propiedades y actividades de la suscripción o eliminar la suscripción.

La siguiente tabla proporciona los enlaces al procedimiento correspondiente para la tarea que desea realizar.

Tarea	Enlace
Añadir acceso a una suscripción de Microsoft Azure	"Añadir el acceso a una suscripción de Microsoft Azure" (p. 754)
Renovar el acceso a una suscripción de Microsoft Azure	"Renovar el acceso a una suscripción de Microsoft Azure" (p. 755)
Eliminar el acceso a una suscripción de Microsoft Azure	"Eliminar el acceso a una suscripción de Microsoft Azure" (p. 756)

© Acronis International GmbH, 2003-2025

Problemas de configuración entre suscripciones en Microsoft Azure

Si está utilizando dos suscripciones diferentes para Microsoft Azure: por ejemplo, una para la copia de seguridad directa en Microsoft Azure ("Suscripción 1") y otra para la configuración del sitio de DR en Microsoft Azure ("Suscripción 2"), pero elimina el acceso a "Suscripción 1", se producirán los siguientes problemas:

- La conmutación por error fallará

  No podrá iniciar una conmutación por error, ya que los datos de la copia de seguridad están almacenados en "Suscripción 1".
- La conmutación tras recuperación fallará

  Si se elimina el acceso a "Suscripción 1" después de realizar una conmutación por error, no será posible acceder a todos los datos de copia de seguridad que se almacenan en la suscripción. Por lo tanto, no será posible realizar operaciones de copia de seguridad de la máquina virtual en conmutación por error y conmutación tras recuperación. Mientras los datos de copia de seguridad permanezcan en "Suscripción 1", las operaciones de conmutación por error o recuperación dependen del acceso y los permisos válidos a la ubicación de almacenamiento original. La eliminación del acceso rompe esta dependencia, incluso si se inician operaciones de DR en una suscripción diferente.

Importante
No elimine ni revoque el acceso a la suscripción de Azure original si las copias de seguridad que se almacenan allí todavía se utilizan o se necesitan.

Creación de un plan de protección de recuperación ante desastres con Microsoft Azure

El plan de protección de recuperación ante desastres es un plan de protección en el que el módulo **Recuperación ante desastres** está habilitado.

Para Microsoft Azure, debe configurarse la ubicación del sitio de DR. No es posible aplicar un plan de protección con una ubicación de DR de Azure si no se ha configurado.

© Acronis International GmbH, 2003-2025

Nota

- La aplicación de un plan de protección de recuperación ante desastres crea servidores de recuperación en la nube. Las redes en la nube existentes no se modifican ni se vuelven a crear.
- Después de configurar la recuperación ante desastres podrá realizar una conmutación por error de prueba o de producción desde cualquier punto de recuperación (copias de seguridad) generado después de la creación del servidor de recuperación del dispositivo. No puede usar los puntos de recuperación que se generaron antes de que el dispositivo estuviese protegido con la recuperación ante desastres (antes de crear el servidor de recuperación).
- No se puede habilitar un plan de protección para la recuperación ante desastres si no se puede detectar la dirección IP de un dispositivo. Por ejemplo, cuando se realizan copias de seguridad sin agente de máquinas virtuales y no se les asigna una dirección IP. En este caso, recomendamos que cree un servidor de recuperación de forma manual.
- Cuando aplica un plan de protección, los servidores de recuperación se configuran en la subred que se configuró en las reglas de asignación durante la configuración de la ubicación del sitio de DR, en función de la dirección IP del dispositivo original. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red de recuperación de Azure y la subred correspondientes. El último octeto de la IP privada se tomará de la dirección IP del equipo original.

Para crear un plan de protección de recuperación ante desastres

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione los equipos que quiera proteger.
3. Haga clic en **Proteger** y, a continuación, en **Crear plan**.
   Se abre la configuración predeterminada del plan de protección.
4. Configure las opciones de copia de seguridad.
   Para usar la funcionalidad de recuperación ante desastres, el plan debe realizar copias de seguridad de todo el equipo o solo de los discos. Esto es necesario para arrancar y proporcionar los servicios necesarios a un almacenamiento en la nube o el almacenamiento de Microsoft Azure.
5. Active el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Recuperación ante desastres**.
6. En el campo **Ubicación**, seleccione **Microsoft Azure**.
7. Haga clic en **Crear**.
   El plan se crea y se aplica a los equipos seleccionados. Se crean los servidores de recuperación con los parámetros predeterminados.

Gestión del sitio de recuperación ante desastres en Microsoft Azure

Puede crear y configurar su sitio de recuperación ante desastres (DR) en Microsoft Azure como parte de la creación del plan de protección de recuperación ante desastres o como un procedimiento separado, desde la pantalla **Disaster Recovery**.

© Acronis International GmbH, 2003-2025

Cuando se aplica un plan de protección de recuperación ante desastres, la infraestructura de red en la nube del servidor de recuperación se crea solo si no existe ya. Los servidores en la nube y las redes existentes no se cambian ni se vuelven a crear.

No se puede habilitar un plan de protección para la recuperación ante desastres si no se puede detectar la dirección IP de un dispositivo. Por ejemplo, cuando se realizan copias de seguridad sin agente de máquinas virtuales y no se les asigna una dirección IP. En este caso, recomendamos que cree un servidor de recuperación de forma manual.

Cuando aplica un plan de protección, los servidores de recuperación se configuran en la subred que hay configurada en las reglas de asignación durante la configuración de la ubicación del sitio de DR, y se basan en la dirección IP del dispositivo original. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red de recuperación de Azure y en la subred correspondientes. El último octeto de la IP privada se tomará de la dirección IP del equipo original.

Creación de un sitio de recuperación ante desastres en Microsoft Azure

Requisitos previos

- Tiene una suscripción a Microsoft Azure.
- Su cuenta de Microsoft tiene uno de los siguientes roles de Entra ID: Administrador de aplicaciones en la nube, Administrador de aplicaciones o Administrador global.
- Su cuenta de Microsoft tiene el rol de Propietario para la suscripción de Azure.
- El elemento de oferta de DR y copia de seguridad directa en Azure está habilitado para su inquilino.

Desde todos los dispositivos

Crear un sitio de DR en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las cargas de trabajo que desea proteger.
3. En el menú **Acciones**, haga clic en **Proteger**.
4. Cree un plan de protección y configure los siguientes ajustes:
   a. En el módulo **Copia de seguridad**, en el campo **Dónde guardar las copias de seguridad**, seleccione la ubicación de almacenamiento para las copias de seguridad de sus cargas de trabajo.
   b. Active el módulo de **Recuperación ante desastres** y, a continuación, haga clic en el campo **Ubicación**.

© Acronis International GmbH, 2003-2025

Nota

Si solo está habilitado el elemento de oferta **DR y copia de seguridad directa en Azure** para su inquilino, la ubicación no se preseleccionará y verá un enlace para **Configurar**.

Si ambos elementos de oferta **DR en Acronis o en la nube híbrida** y **DR y copia de seguridad directa en Azure** están habilitados para su inquilino, Cyber Protect Cloud se preseleccionará como ubicación.

c. En el asistente de **Configuración del sitio de recuperación ante desastres**, en la pestaña **Ubicación del sitio**, seleccione **Microsoft Azure Cloud** y, a continuación, haga clic en **Siguiente**.

d. En la pestaña **Suscripción de Azure**, haga lo siguiente:
   - Si su suscripción de Microsoft Azure ya se había añadido a la consola de Cyber Protect, haga clic en ella y luego en **Siguiente**.
   - Si desea añadir una nueva suscripción de Microsoft Azure, haga clic en **Agregar suscripción**, añada la suscripción y luego pulse en ella y en **Siguiente**.

e. En la pestaña **Región de destino**, en el campo **Región de Azure**, seleccione la región de Azure para el sitio de DR.

f. En la pestaña **Red de recuperación**, configure las redes de recuperación para la conmutación por error de producción y prueba, y haga clic en **Siguiente**.

Opción	Descripción
Configuración predeterminada	Utilice esta opción si desea que las redes de producción y de prueba en Azure se creen automáticamente, con una red para cada entorno.
Configuración avanzada	Utilice esta opción si desea seleccionar sus redes de Azure existentes como redes de producción y prueba y configurar la asignación de redes.

g. En la pestaña **Resumen**, revise los parámetros de su sitio de DR y, a continuación, haga clic en **Configurar**.

El plan de protección se aplica correctamente a las cargas de trabajo seleccionadas. Se crea el sitio de DR en Azure, ubicado en la región de Azure seleccionada. En la pantalla **Disaster Recovery** > **Conectividad**, puede ver las redes de producción y prueba, así como los servidores de recuperación que se crearon, en **Modo de espera**.

Desde conectividad

Crear un sitio de DR en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery**.
2. Haga clic en **Configurar**.
3. En el asistente de **Configuración del sitio de recuperación ante desastres**, en la pestaña **Ubicación del sitio**, seleccione **Microsoft Azure Cloud** y, a continuación, haga clic en

© Acronis International GmbH, 2003-2025

Siguiente.

4. En la pestaña **Suscripción de Azure**, haga lo siguiente:
   - Si su suscripción de Microsoft Azure ya se había añadido a la consola de Cyber Protect, haga clic en ella y luego en **Siguiente**.
   - Si desea añadir una nueva suscripción de Microsoft Azure, haga clic en **Agregar suscripción**, añada la suscripción y luego pulse en ella y en **Siguiente**.
5. En la pestaña **Región de destino**, en el campo **Región de Azure**, seleccione la región de Azure para el sitio de DR.
6. En la pestaña **Red de recuperación**, configure las redes de recuperación para la conmutación por error de producción y prueba, y haga clic en **Siguiente**.

Opción	Descripción
Configuración predeterminada	Utilice esta opción si desea que las redes de producción y de prueba en Azure se creen automáticamente, con una red para cada entorno.
Configuración avanzada	Utilice esta opción si desea seleccionar sus redes de Azure existentes como redes de producción y prueba y configurar la asignación de redes.

7. En la pestaña **Resumen**, revise los parámetros de su sitio de DR y, a continuación, haga clic en **Configurar**.

   El sitio de DR se crea en Azure, ubicado en la región de Azure seleccionada. En la pantalla **Disaster Recovery** > **Conectividad**, puede ver las redes de producción y prueba.

Eliminar el sitio de DR de Microsoft Azure

Puede eliminar el sitio de DR de Microsoft Azure si ya no lo necesita o si desea cambiar la ubicación del sitio de DR.

Requisitos previos

No hay servidores de recuperación en el sitio de DR.

Para eliminar el sitio de DR de Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. Haga clic en **Eliminar el sitio de recuperación ante desastres**.
3. En la ventana **Eliminar el sitio de recuperación ante desastres**, introduzca su credencial de inicio de sesión y haga clic en **Eliminar**.

Conectividad y redes en Microsoft Azure

Disaster Recovery en Microsoft Azure permite la orquestación de pruebas, conmutación por error y conmutación tras recuperación, así como la selección de redes de recuperación (subredes y redes virtuales de Azure) para los escenarios de conmutación por error de producción y de prueba. Puede

© Acronis International GmbH, 2003-2025

configurar estas redes durante la configuración inicial del sitio de DR o más tarde: desde la pantalla de **Conectividad** o de forma individual para cada servidor de recuperación.

Mantiene el control total sobre la conexión a redes virtuales y la conectividad de Azure, y tiene la flexibilidad de aprovechar las capacidades nativas de la plataforma de Azure o de llevar soluciones personalizadas, como firewalls de terceros o dispositivos SD-WAN al sitio de DR, conectándolos a las redes de recuperación seleccionadas.

A continuación se presenta un resumen de los principales servicios de conexión a redes virtuales de Azure, su relevancia para los casos de uso de recuperación ante desastres y enlaces para obtener más información.

Azure Firewall

Azure Firewall proporciona un filtrado de tráfico de red centralizado y con estado en varias redes virtuales y subredes. Ayuda a hacer cumplir las reglas de seguridad entre cargas de trabajo después de una conmutación por error y admite escenarios en los que los entornos de DR deben cumplir con las políticas de cumplimiento o segmentación corporativas.

Puede utilizar Azure Firewall para controlar el tráfico saliente y entrante hacia y desde las máquinas virtuales con conmutación por error (por ejemplo, para limitar el acceso a Internet y permitir solo las fuentes de la lista de permitidos). Para la exposición administrada, coloque Azure Firewall entre la red in situ (a través de VPN) y las redes virtuales de DR de Azure.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Grupos de seguridad de red (NSG)

Los NSG permiten definir reglas granulares para permitir o denegar el tráfico de red a las máquinas virtuales o subredes. Los NSG funcionan a nivel de la NIC de la máquina virtual y de la subred.

Puede aplicar los NSG para controlar el acceso a las máquinas virtuales de recuperación, garantizar el aislamiento de las conmutaciones por error de prueba o exponer solo los puertos necesarios (por ejemplo, RDP y HTTP). Los NSG son esenciales para habilitar de forma segura la conectividad en función de si la máquina virtual de recuperación está en modo de prueba o de producción.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Servidores DNS

Las redes virtuales de Azure admiten configuraciones de servidor DNS personalizadas o integración con Azure DNS. Esto controla cómo funciona la resolución de nombres en el entorno de DR.

Asegúrese de que las máquinas virtuales de DR resuelvan los nombres correctamente, ya sea a otros servicios recuperados en Azure o a sistemas externos. El DNS personalizado es esencial al restaurar entornos integrados con AD o para el reenvío de DNS a sistemas locales.

Para obtener más información, consulte la Documentación de Microsoft Azure.

© Acronis International GmbH, 2003-2025

Enrutamiento de subredes (rutas definidas por el usuario)

Azure permite la creación de rutas personalizadas (UDR) para controlar el flujo de tráfico entre subredes y hacia redes in situ, anulando el enrutamiento predeterminado del sistema.

Cree rutas para dirigir el tráfico de las máquinas virtuales de recuperación a través de firewalls, a puertas de enlace de VPN o puntos de inspección. Esto ayuda a hacer cumplir las directivas de enrutamiento y garantizar la conectividad de vuelta a in situ a través de VPN o ExpressRoute.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Direcciones IP públicas

Se pueden asignar direcciones IP públicas (estáticas o dinámicas) a las máquinas virtuales de Microsoft Azure para permitir el acceso directo a Internet cuando sea necesario. Esto es útil para exponer servicios o para el acceso remoto.

Asigne direcciones IP públicas a cargas de trabajo con conmutación por error que requieran acceso externo (por ejemplo, servidores web y administración remota). Evite hacerlo para cargas de trabajo sensibles. Utilice Bastion o un VPN en su lugar, si es posible.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Azure Bastion

Azure Bastion permite el acceso seguro mediante RDP/SSH desde un navegador a las máquinas virtuales sin exponer las IP públicas. Funciona a través del portal de Azure y utiliza cifrado TLS.

Acceda a las máquinas virtuales recuperadas de forma segura para realizar diagnósticos o reconfiguraciones manuales tras la conmutación por error. Esto es especialmente útil en la conmutación por error de prueba, donde no se desea exponerlas a Internet.

Para obtener más información, consulte la Documentación de Microsoft Azure.

VPN de sitio a sitio de Azure

La VPN de sitio a sitio proporciona una conexión IPsec cifrada entre su red in situ y las redes virtuales de Azure, lo que permite la conectividad híbrida.

Garantiza el acceso fluido a las cargas de trabajo recuperadas desde las redes in situ. Resulta crítico para acceder a las apps internas o restaurar las dependencias cruzadas con los sistemas que aún se ejecutan in situ.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Azure ExpressRoute

ExpressRoute ofrece conectividad privada dedicada entre su centro de datos y Azure, saltándose Internet para mejorar la velocidad, la fiabilidad y la seguridad.

© Acronis International GmbH, 2003-2025

Recomendado para DR de nivel empresarial con grandes conjuntos de datos o requisitos de baja latencia. Utilícelo para conectar sistemas in situ con máquinas virtuales de DR en Microsoft Azure sin depender de una VPN.

Para obtener más información, consulte la Documentación de Microsoft Azure.

Gestión de redes en Microsoft Azure

Las redes de recuperación son redes virtuales de Azure (VNet) y subredes donde se ejecutarán sus sistemas de copia de seguridad (servidores de recuperación) si sus sistemas principales fallan.

Hay dos tipos de redes de recuperación: redes de recuperación de producción y redes de recuperación de prueba.

Red de recuperación de producción

Las redes de recuperación de producción se utilizan durante un desastre real cuando necesita mover sus servicios a Azure. Las cargas de trabajo (VM) con conmutación por error están conectadas a estas redes de recuperación para que se reanuden las operaciones de la empresa.

Este es un ejemplo de una red de producción:

VNet: `dr-prod-vnet-91a4e5bf`

Subred: `subnet-one (10.0.10.0/24)`

Red de recuperación de prueba

Las redes de recuperación de prueba se utilizan durante las conmutaciones por error de prueba manuales o automatizadas para verificar que la recuperación ante desastres funciona sin afectar a sus sistemas de producción.

Para evitar conflictos de IP o filtraciones de datos, las redes de recuperación de prueba deben estar aisladas del entorno de producción. Para evitar la superposición con las redes de producción, la mejor práctica es utilizar una red virtual dedicada.

Para obtener más información sobre la planificación y el diseño de redes virtuales, consulte la documentación de Microsoft Azure.

Mejores prácticas para la configuración de red de Disaster Recovery

Cuando configure las redes de recuperación en Disaster Recovery a Microsoft Azure, le recomendamos que siga las siguientes mejores prácticas:

- Separe las redes virtuales y subredes de producción y de prueba
  Mantenga los entornos de prueba y producción aislados.
- Utilice etiquetas y convenciones de nomenclatura de Azure
  Etiquete claramente las redes (por ejemplo, `dr-prod` y `dr-test`) para facilitar la identificación y la automatización.
- Planifique cuidadosamente los rangos de IP

© Acronis International GmbH, 2003-2025

Asegúrese de que las redes virtuales y las subredes no entren en conflicto con las redes in situ si hay conectividad entre el sitio de DR y el sitio in situ, por ejemplo, a través de una VPN IPsec o ExpressRoute.

Mantenga esquemas de dirección coherentes para facilitar el enrutamiento y la integración de identidades.

- Preconfigure los recursos de red necesarios

  Las NSG, las tablas de rutas, el DNS personalizado y las IP públicas deben configurarse de antemano para las redes de recuperación de prueba y producción.

Recomendaciones para la disponibilidad de servicios de dominio de Active Directory

Si tiene que autenticar sus cargas de trabajo protegidas en un controlador de dominio, le recomendamos que disponga de una instancia de Controlador de dominio de Active Directory (AD DC) en el sitio de DR de Microsoft Azure.

Recomendaciones para la disponibilidad de AD DS en el sitio de DR en Azure

Las recomendaciones para una instancia AD DC dedicada en el sitio de DR son las siguientes:

- Apague el firewall de Windows.
- Una el AD DC al servicio de Active Directory.
- Asegúrese de que la máquina virtual de Microsoft Azure tenga acceso a Internet.
- Añada la función de Active Directory.
- Despliegue al menos un controlador de dominio en el sitio de DR de Azure

  Las cargas de trabajo recuperadas necesitan autenticarse, aplicar directivas de grupo y resolver nombres. Despliegue una máquina virtual de controlador de dominio adicional en Azure por adelantado, antes de la conmutación por error.
- Utilice un controlador de dominio replicado (que no sea de solo lectura)

  Los controladores de dominio de solo lectura (RODC) pueden no ser compatibles con todos los escenarios de autenticación después de una conmutación por error. Despliegue un controlador de dominio escribible y replíquelo con su bosque de AD in situ.
- Asegúrese de que la configuración de DNS sea correcta

  Las máquinas virtuales recuperadas deben resolver nombres de dominio y localizar controladores de dominio. Configure la red virtual de recuperación para usar la dirección IP del controlador o de los controladores de dominio basado(s) en Azure como el servidor DNS personalizado.
- Replique SYSVOL y garantice la sincronización de tiempo

  Las directivas de grupo y las operaciones de dominio dependen de la replicación de SYSVOL y de la hora correcta. Asegúrese de que SYSVOL esté sincronizado y configure NTP o los ajustes de sincronización de hora para garantizar la coherencia entre Azure y los entornos in situ.

© Acronis International GmbH, 2003-2025

Configuración de la red de recuperación de prueba

Para asegurarse de que una conmutación por error de prueba no interfiera con las operaciones de producción, configure una red virtual (VNet) aislada en Azure para fines de prueba. Confirme que la VNet de prueba no tenga conexiones de enrutamiento o emparejamiento con la VNet de producción. Pruebe la conectividad desde una máquina virtual en la VNet de prueba para asegurarse de que no pueda acceder a los recursos de producción.

Agregar una red de recuperación de producción desde Microsoft Azure

Después de configurar el sitio de DR, puede agregar redes de recuperación de producción adicionales a partir de las que existen en Microsoft Azure.

Agregar una red de recuperación de producción desde Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En el panel **Redes de producción**, haga clic en **Agregar red**.
3. En la ventana **Añadir red de producción**, en el campo **Red virtual**, seleccione una red virtual.
4. En el campo **Subred**, seleccione la subred.
5. [Opcional] Para establecer esta subred como predeterminada, seleccione **Establecer esta subred como "Predeterminada" para la asignación**.
   Al aplicar el plan de protección de recuperación ante desastres a los dispositivos originales, los servidores de recuperación se configuran en la subred predeterminada.
6. En el campo **Asignación a la red local**, haga clic en **Agregar**.
   Puede definir reglas de asignación introduciendo una o más redes locales de origen en formato CIDR. El servicio comparará la dirección IP del dispositivo original con las reglas de asignación. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red y la subred de recuperación de Azure correspondientes.
7. Introduzca una o más redes locales de origen en el formato CIDR.
8. Para añadir la red, haga clic en **Listo**.

Agregar una red de recuperación de prueba desde Microsoft Azure

Después de configurar el sitio de DR, puede añadir redes de recuperación de prueba adicionales a las que existen en Microsoft Azure.

Para agregar una red de recuperación de prueba desde Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Conectividad**.
2. En el panel **Redes de prueba**, haga clic en **Agregar red**.
3. En la ventana **Añadir red de prueba**, en el campo **Red virtual**, seleccione una red virtual.
4. En el campo **Subred**, seleccione la subred.

© Acronis International GmbH, 2003-2025

5. [Opcional] Para establecer esta subred como predeterminada, seleccione **Establecer esta subred como "Predeterminada" para la asignación**.
   Al aplicar el plan de protección de recuperación ante desastres a los dispositivos originales, los servidores de recuperación se configuran en la subred predeterminada.
6. En el campo **Asignación a la red local**, haga clic en **Agregar**.
   Puede definir reglas de asignación introduciendo una o más redes locales de origen en formato CIDR. El servicio comparará la dirección IP del dispositivo original con las reglas de asignación. Si la dirección IP coincide con alguna de las redes locales de origen especificadas, el servidor de recuperación se creará en la red y la subred de recuperación de Azure correspondientes.
7. Introduzca una o más redes locales de origen en el formato CIDR.
8. Para añadir la red, haga clic en **Listo**.

Servidores de recuperación en Microsoft Azure

Un servidor de recuperación es una réplica del equipo original que se crea a partir de la copia de seguridad (punto de recuperación) del servidor protegido que se almacena en la nube (Cyber Protect Cloud o Microsoft Azure). En caso de desastre, la carga de trabajo se cambia del servidor original al servidor de recuperación en Microsoft Azure.

Los servidores de recuperación se crean manualmente o automáticamente, cuando aplica un plan de protección de recuperación ante desastres a una carga de trabajo.

No se cobran puntos de cálculo por ejecutar sus servidores de recuperación en Microsoft Azure. Todos el uso de cálculo se factura directamente a su suscripción de Microsoft Azure.

La configuración de la dirección MAC para los servidores de recuperación no está disponible en Disaster Recovery para Microsoft Azure.

Administración de servidores de recuperación

Las siguientes operaciones con servidores de recuperación están disponibles en Disaster Recovery para Microsoft Azure:

Operación	Descripción
Encender	(Para servidores en el estado de conmutación por error) Encender la máquina virtual de Microsoft Azure (servidor de recuperación).
Apagar	[Para servidores en el estado de conmutación por error] Apagar la máquina virtual de Microsoft Azure (servidor de recuperación). La operación de apagado detiene la máquina virtual de Microsoft Azure, pero no desasigna recursos. La máquina virtual estará en el estado Detenida (Asignada). En este estado, una máquina virtual de Microsoft Azure sigue reservando CPU y memoria, incurriendo en cargos de cálculo como si estuviera en ejecución. Este estado preserva la dirección IP y la ubicación del servidor de

© Acronis International GmbH, 2003-2025

Operación	Descripción
	la máquina virtual.
Apagado forzoso	[Para servidores en el estado de conmutación por error] Apagar forzosamente el servidor de recuperación.
Editar configuración	Modificar los ajustes del servidor de recuperación, como la configuración de la red o los umbrales de RPO desde la consola de Cyber Protect.
Conmutación por error de producción	Cambiar las cargas de trabajo al servidor de recuperación en la red de producción.
Conmutación por error de prueba	Probar el servidor de recuperación en la red de prueba aislada sin afectar la producción. Para evitar conflictos durante la conmutación por error, asegúrese de que redes de producción y de prueba estén configuradas correctamente. Pruebe regularmente las operaciones de conmutación por error para validar la funcionalidad del servidor de recuperación.
Conectar (a la consola)	[Para servidores en estado de conmutación por error] Después de hacer clic en **Conectar** y ser redirigido a Azure, puede conectarse a la máquina virtual de Azure utilizando las opciones nativas de Azure, como: • Asignar una dirección IP pública y conectarse mediante el protocolo de escritorio remoto (RDP) o SSH. • Usar Azure Bastion, un servicio seguro para conectarse a la máquina virtual sin una IP pública.

Creación de servidores de recuperación en Microsoft Azure

Los servidores de recuperación se crean automáticamente cuando aplica un plan de protección de recuperación ante desastres a una carga de trabajo. Si no se aplica un plan de protección de recuperación ante desastres a la carga de trabajo, puede crear un servidor de recuperación manualmente.

Requisitos previos

- Hay un plan de supervisión aplicado a la carga de trabajo.
- El sitio de DR en Microsoft Azure está configurado.

Para crear un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo que desea proteger con Disaster Recovery y, a continuación, en el menú **Acciones**, pulse en **Recuperación ante desastres**.
3. Haga clic en **Crear servidor de recuperación**.

© Acronis International GmbH, 2003-2025

4. En el asistente **Crear servidor de recuperación**, en la pestaña **Configuración del servidor**, ajuste la configuración y pulse en **Siguiente**.

Configuración	Descripción
CPU y RAM	Tamaño de la máquina virtual de Microsoft Azure. El uso de recursos de cálculo se cobra directamente en su suscripción de Microsoft Azure por parte de Microsoft o su partner. Si algunos tamaños de máquina virtual de Microsoft Azure no están disponibles, consulte las limitaciones de su suscripción de Azure. Los siguientes tipos de máquina virtual de Microsoft Azure están excluidos de la selección: • Serie A (obsoleta en Microsoft Azure) • Tipos de máquina virtual que se basan en la arquitectura ARM CPU La configuración predeterminada se determina automáticamente en función de la configuración de CPU y RAM del dispositivo original. La RAM se ajusta redondeando al tamaño de máquina virtual de la familia B más cercano que cumpla o supere el valor de RAM original y seleccionando el número de núcleos de CPU más bajo disponible que satisfaga el requisito de RAM. Si no hay datos de RAM del equipo original (por ejemplo, para máquinas virtuales de Microsoft Azure que utilizan copias de seguridad sin agente), se selecciona un tamaño mínimo de máquina virtual de la familia B de forma predeterminada. Si la serie o el tamaño de máquina virtual seleccionados no están disponibles en la región o suscripción de destino, el sistema selecciona automáticamente el tamaño más cercano disponible de cualquier serie de la familia B dentro de esa región.
Tipo de disco	Tipo de disco de la máquina virtual de Microsoft Azure. El tipo de disco que seleccione se aplicará a todos los discos del servidor de recuperación. Solo están disponibles para su selección los tipos de disco de almacenamiento redundante local (LRS). No se puede seleccionar Premium SSD v2 ni Ultra SSD. Premium SSD v2 se asigna automáticamente durante una conmutación por error si se detectan discos de sector de 4K en la copia de seguridad de la carga de trabajo original.
Nombre	Nombre del servidor de recuperación que es visible en la consola de Cyber Protect. Este nombre no se utiliza para la máquina virtual de Microsoft Azure.
Descripción	Descripción del servidor de recuperación

5. En la pestaña **Red**, configure la red de producción y de prueba y, a continuación, haga clic en **Siguiente**.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Red	(Para red de producción) La red virtual de Azure (VNet) y la subred para la conmutación por error de producción. Durante una conmutación por error de producción, el servidor se conectará a esta red de Azure.
Dirección IP en la red de producción	(Para red de producción) De forma predeterminada, se deriva el último octeto de la dirección IP del equipo original en el rango de la red de producción, pero puede cambiar la dirección IP en cualquier momento antes de la conmutación por error. Cuando el servidor está en el estado de conmutación por error, puede modificar la dirección IP directamente en Azure.
Red	(Para red de prueba) La red virtual y la subred de Azure para la conmutación por error de prueba. Recomendamos que la red de prueba esté aislada dentro de una red virtual separada. Durante una conmutación por error de prueba, el servidor se conectará a esta red de Azure.
Dirección IP en la red de prueba	(Para red de prueba) De forma predeterminada, se deriva el último octeto del equipo original, en el rango de la red prueba, pero puede cambiar la dirección IP en cualquier momento antes de la conmutación por error. Cuando el servidor se encuentra en el estado de conmutación por error de prueba, puede modificar la dirección IP directamente en Azure.

Nota

- Por motivos de seguridad, no se asigna ninguna IP pública al servidor de recuperación por defecto. Sin una IP pública, el servidor de recuperación solo es accesible desde la red local. Si es necesario, asigne una IP pública directamente en el portal de Azure.
- Por defecto, el acceso a Internet está habilitado para los recursos en Azure. No se requiere ninguna configuración adicional para permitir el tráfico de salida a Internet. Si necesita restringir o aislar el acceso a Internet saliente en una red de prueba, debe configurar los controles de seguridad apropiados, como las reglas de grupo de seguridad de red (NSG), las rutas definidas por el usuario (UDR) o las directivas de Azure Firewall, según sus requisitos.

6. En la pestaña **Conmutación por error de prueba automatizada**, realice lo siguiente:
   a. [Opcional] Active el interruptor **Conmutación por error de prueba automatizada**.
   b. [Opcional] Configure de los ajustes.

Configuración	Descripción
Planificación	La conmutación por error de prueba automatizada se ejecuta una

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	vez al mes.
Tiempo de espera de inicio de la MV / Minutos	El período máximo durante el cual el sistema intenta iniciar un equipo virtual en Azure y tomar una captura de pantalla para verificar si el sistema operativo se ha cargado correctamente. Este período de tiempo de espera no incluye el tiempo que se tarda en restaurar los datos de un archivo de copia de seguridad en frío, ya que esta duración depende del tamaño del archivo. Además, las horas de cálculo de las máquinas virtuales de Microsoft Azure no se cuentan durante el tiempo de restauración de datos.
Usar como tiempo de espera predeterminado	Seleccione esta casilla si desea guardar el valor de **Tiempo de espera de inicio de la MM / Minutos** como predeterminado. En este caso, el valor se rellenará automáticamente cuando active la conmutación por error de prueba automatizada para otros servidores de recuperación.

c. Haga clic en **Siguiente**.

7. En la pestaña **Configuración**, haga lo siguiente:
   a. [Opcional] El umbral de RPO determina el intervalo temporal máximo permitido entre el último punto de recuperación y el momento presente. Puede establecer un valor de entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
   b. [Opcional] [Si las copias de seguridad del equipo seleccionado están cifradas utilizando el cifrado como una propiedad del equipo], especifique la contraseña que se utilizará automáticamente al crear una máquina virtual para el servidor de recuperación a partir de la copia de seguridad cifrada.
      a. Haga clic en **Introducir contraseña**, introduzca la contraseña de la copia de seguridad cifrada y defina un nombre para las credenciales.
         De forma predeterminada, verá la copia de seguridad más reciente en la lista.
      b. Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.
      c. Haga clic en **Guardar**.

      Nota
      Tenga en cuenta que, aunque la contraseña que especifique se guardará en un almacén de credenciales seguro, es posible que incumpla sus obligaciones legales si la guarda.

8. Haga clic en **Crear**.

El servidor de recuperación se crea y está en estado de espera. No se cargan puntos de cálculo. Todo el uso de cálculo se factura directamente a su suscripción de Azure.

© Acronis International GmbH, 2003-2025

Nota
Puede configurar reglas de firewall para la máquina virtual solo en el portal de Azure. De forma predeterminada, para las máquinas virtuales en conmutación por error de prueba y producción, se prohíben todas las conexiones entrantes y se permiten todas las conexiones salientes a Internet dentro de la red virtual de producción y prueba.

Edición de la configuración del servidor de recuperación

Cuando cree y aplique un plan de protección de recuperación ante desastres, se creará un servidor de recuperación con la configuración predeterminada. Puede editar esta configuración predeterminada cuando sea necesario.

Para editar la configuración de un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga clic en el servidor cuyos ajustes desea editar y luego en **Editar**.
3. Edite la configuración del servidor de recuperación.
4. Haga clic en **Guardar**.

Eliminación de un servidor de recuperación

Puede eliminar los servidores de recuperación que creó en Microsoft Azure.

Para eliminar un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga click en el servidor que quiera eliminar y, a continuación, pulse en **Eliminar**.
3. Haga clic en **Eliminar** en la ventana de confirmación.

Conmutación por error en Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Conmutación por error de producción

La conmutación por error es el proceso que cambia la carga de trabajo del servidor original en su sitio local al servidor de recuperación.

Al crear un servidor de recuperación, se queda en **Modo de espera**. La máquina virtual correspondiente no existe en Microsoft Azure hasta que inicie una conmutación por error. Antes de iniciar una conmutación por error, debe crear al menos una copia de seguridad de imagen de disco (con volumen de arranque) del equipo original.

© Acronis International GmbH, 2003-2025

Al iniciar una conmutación por error, seleccione el punto de recuperación (copia de seguridad) del equipo original a partir del cual se creará una máquina virtual con los parámetros predefinidos en Microsoft Azure.

Cuando la conmutación por error se completa, el estado del servidor de recuperación cambia a **Conmutación por error**. La carga de trabajo se cambia ahora del equipo original al servidor de recuperación en Microsoft Azure.

Si el servidor de recuperación tiene un agente de protección, para evitar interferencias (como iniciar una copia de seguridad o informar sobre estados obsoletos al componente de copia de seguridad), se detiene el servicio de agente.

Conmutación por error de prueba

La conmutación por error de prueba es un proceso de creación de una máquina virtual temporal en una red virtual (VNet) de Azure aislada y para probar los procedimientos de recuperación, configuraciones y la funcionalidad de las aplicaciones. Para obtener más información, consulte "Conmutación por error de prueba en Microsoft Azure" (p. 1128).

Conmutación por error de prueba automatizada

La conmutación por error de prueba automatizada en Microsoft Azure valida la integridad de la copia de seguridad al arrancar una máquina virtual de servidor de recuperación desde la última copia de seguridad y hacer una captura de pantalla para confirmar que el sistema operativo se inició correctamente. Si está habilitada, la conmutación por error de prueba automatizada se inicia una vez al mes. Para obtener más información, consulte "Conmutación por error de prueba automatizada en Microsoft Azure" (p. 1131).

Manejo de conflictos de direcciones IP en la conmutación por error

Si la dirección IP configurada en la red de producción ya está en uso en el momento de la conmutación por error de producción, se asignará automáticamente otra dirección IP disponible de la misma red.

Si la dirección IP de la red de prueba configurada ya está en uso en el momento de la conmutación por error de la prueba, se asignará otra dirección IP disponible de la red de prueba.

Recuperación del servidor de recuperación en conmutación por error a un momento dado anterior

Para recuperar un servidor en conmutación por error, inicie una nueva conmutación por error desde un punto de recuperación diferente para restaurar las operaciones.

Widgets de conmutación por error

Durante la conmutación por error de producción y prueba, puede ver información sobre el rendimiento de la conmutación por error (velocidad de recuperación) y los cuellos de botella o

© Acronis International GmbH, 2003-2025

atascos en la pestaña **Actividades** de los detalles del servidor de recuperación. Para ver el widget **Atasco**, expanda la actividad **Creando equipo virtual** y, a continuación, en la subactividad **Copiar datos de la copia de seguridad a los discos del equipo virtual**, despliegue **Atasco**.

Realización de una conmutación por error de producción en Microsoft Azure

Cuando realiza una conmutación por error de producción, la carga de trabajo se cambia del equipo original al servidor de recuperación en Microsoft Azure.

Para realizar una conmutación por error de producción en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga clic en el servidor que desea conmutar por error y luego en **Conmutación por error**.
3. En la ventana **Conmutación por error de servidor**, seleccione **Conmutación por error de producción** y, a continuación, seleccione el punto de recuperación (copia de seguridad) desde el que se iniciará el servidor de la nube.
4. Haga clic en **Iniciar**.

Cuando la conmutación por error se completa, el servicio comienza a ejecutarse en la máquina virtual en Azure. Al hacer clic en **Conectar**, se le redirigirá a la máquina virtual en Azure.

Conmutación por error de prueba en Microsoft Azure

Una conmutación por error de prueba es una parte vital de la estrategia de Disaster Recovery como servicio (DRaaS) en Microsoft Azure. Permite a las organizaciones validar los procesos de recuperación sin afectar a los entornos de producción. Esto se realiza simulando la recuperación de una máquina virtual (MV) desde un punto de recuperación (copia de seguridad) seleccionado. El proceso crea una MV temporal en una red virtual (VNet) de Azure aislada para probar los procedimientos de recuperación, las configuraciones y la funcionalidad de las aplicaciones. Aunque son opcionales, se recomienda encarecidamente realizar pruebas de conmutación por error de forma regular para garantizar procesos de recuperación fiables y actualizados. Puede establecer una planificación de pruebas que se base en los requisitos de coste y salvaguarda de su organización.

Puede probar varios servidores de recuperación a la vez y comprobar su interacción. En la red de prueba, los servidores se comunican utilizando sus direcciones IP de producción, pero no pueden iniciar conexiones TCP o UDP con las cargas de trabajo de su red local.

Red de recuperación de prueba

Para asegurarse de que una prueba de conmutación por error no interfiera con las operaciones de producción, configure una red virtual (VNet) aislada en Azure para fines de prueba. Confirme que la VNet de prueba no tenga conexiones de enrutamiento o emparejamiento con la VNet de producción. Pruebe la conectividad desde una máquina virtual en la VNet de prueba para asegurarse de que no pueda acceder a los recursos de producción.

© Acronis International GmbH, 2003-2025

Proceso de la conmutación por error de prueba

El proceso de la conmutación por error de prueba consiste en las siguientes fases.

Iniciación

Durante esta fase, selecciona un punto de recuperación y comienza la conmutación por error de prueba.

Despliegue del trabajador (agente temporal)

Durante esta fase, se despliega automáticamente un trabajador que se utiliza para la operación de conmutación por error de prueba. El despliegue inicial del trabajador para una conmutación por error de prueba o producción puede tardar varios minutos. El inicio de los trabajadores para las conmutaciones por error posteriores debería ser más rápido.

Restauración de datos

Durante esta fase, los datos se copian desde el almacenamiento de copia de seguridad a un contenedor de Azure Blob Storage temporal. El tiempo que se tarda en copiar o restaurar los datos depende del tamaño de la carga de trabajo. Después de que se copien los datos, el contenido de Azure Blob Storage se convierte en un disco administrado, que se utiliza para iniciar la máquina virtual temporal.

Creación de máquina virtual de recuperación

La máquina virtual de recuperación está conectada a la red virtual aislada de Azure y a la subred preconfiguradas. De forma predeterminada, se asigna a la máquina virtual una dirección IP en la que el último octeto coincide con la dirección IP del equipo original. Puede modificar la dirección IP antes de la conmutación por error de prueba en la configuración del servidor de recuperación. Durante la conmutación por error de prueba, puede hacerlo directamente en el portal de Azure.

Asegúrese de que la red virtual esté aislada de la red de producción para evitar interacciones no deseadas.

Verificación

Después de la creación de la máquina virtual, al hacer clic en el botón **Conectar** se le redireccionará a la máquina virtual específica en el portal de Azure.

Realice todas las pruebas necesarias para verificar el comportamiento de la aplicación, la conectividad y los objetivos de recuperación en el entorno aislado.

La conmutación por error de prueba no sobrescribe los puntos de recuperación existentes, lo que garantiza que sus copias de seguridad permanezcan intactas.

Deteniendo la conmutación por error de prueba

Al detener la conmutación por error de prueba, se eliminan la máquina virtual temporal, los recursos asociados y el trabajador. Si se utilizó una contraseña de cifrado, se elimina

© Acronis International GmbH, 2003-2025

automáticamente del almacén de credenciales al detener o completar la conmutación por error de prueba.

Puede detener la prueba de conmutación por error en cualquier momento desde el portal de Azure.

Realización de una prueba de conmutación por error en Microsoft Azure

Aunque la realización de una conmutación por error de prueba es opcional, le recomendamos que lo haga habitualmente con la frecuencia que considere adecuada, teniendo en cuenta el coste y la seguridad.

Importante
Puede realizar una conmutación por error solo desde los puntos de recuperación (copias de seguridad) que se crearon después de crear el servidor de recuperación del dispositivo.

Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en un servidor de recuperación. Solo se permiten 100 puntos de recuperación como máximo.

Requisitos previos

- El servidor de recuperación está configurado en la ubicación de Azure y tiene al menos un punto de recuperación creado después de que se creó el servidor de recuperación.
- Una red virtual y una subred de Azure aisladas para la conmutación por error de prueba para garantizar que no haya interferencias con los entornos de producción.
- Las reglas del grupo de seguridad de red (NSG) están configuradas para cumplir con sus requisitos.

Para realizar una conmutación por error de prueba en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores de recuperación**.
2. Haga clic en el servidor que desea conmutar por error y luego en **Conmutación por error**.
3. En la ventana **Conmutación por error de servidor**, seleccione **Conmutación por error de prueba** y, a continuación, seleccione el punto de recuperación (copia de seguridad) desde el que se iniciará el servidor de la nube.
4. Haga clic en **Iniciar**.
5. Si la copia de seguridad que ha seleccionado está cifrada usando el cifrado como una propiedad del equipo:
   a. Introduzca la contraseña de cifrado para la copia de seguridad establecida.

      Nota
      Solo se guardará la contraseña temporalmente y se utilizará para la operación de prueba de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales si se detiene la prueba de conmutación por error o una vez que esta se haya completado.

© Acronis International GmbH, 2003-2025

b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en el campo **Nombre de las credenciales**.

Importante
La contraseña se almacenará en un almacén de credenciales seguro y se aplicará automáticamente en las siguientes operaciones de conmutación por error. No obstante, es posible que incumpla sus obligaciones legales si guarda las contraseñas.

c. Haga clic en **Listo**.

Cuando el servidor de recuperación se inicia, su estado cambia a **Probando conmutación por error**.

6. Use uno de los siguientes métodos para probar el servidor de recuperación:
   - En **Disaster Recovery** > **Servidores de recuperación**, seleccione el servidor de recuperación y, a continuación, haga clic en **Conectar**.
   - Use el equipo remoto o SSH para conectarse al servidor de recuperación y a la dirección IP de prueba que especificó al crear el servidor de recuperación. Pruebe la conexión tanto desde el interior como desde el exterior de la red de producción.
   - Ejecute una secuencia de comandos en el servidor de recuperación.
     El script puede comprobar la pantalla de inicio, si las aplicaciones se han iniciado, la conexión a Internet y la capacidad de otros equipos de conectarse al servidor de recuperación.
7. Cuando la prueba haya terminado, haga clic en **Detener comprobación**.
   El servidor de recuperación se detiene. No se guardan los cambios realizados en el servidor de recuperación durante la conmutación por error de prueba.

Conmutación por error de prueba automatizada en Microsoft Azure

La conmutación por error de prueba automatizada en Microsoft Azure valida la integridad de la copia de seguridad al arrancar una máquina virtual de servidor de recuperación desde la última copia de seguridad y realizar una captura de pantalla para confirmar que el sistema operativo se inició correctamente.

Con la conmutación por error de prueba automatizada, el servidor de recuperación se prueba automáticamente una vez al mes sin ninguna interacción manual.

El proceso de conmutación por error de prueba automatizada está formado por las siguientes partes:

1. Creación de una máquina virtual en Microsoft Azure a partir del último punto de recuperación.
2. Tomar una captura de pantalla de la máquina virtual.
3. Análisis de si el sistema operativo de la máquina virtual arranca correctamente.
4. Notificación acerca del estado de la conmutación por error de prueba.

© Acronis International GmbH, 2003-2025

Nota
La conmutación por error de prueba automatizada consume horas de cálculo de la máquina virtual de Microsoft Azure.

Puede configurar la conmutación por error de prueba automatizada en la configuración del servidor de recuperación. Para obtener más información, consulte "Configuración de la conmutación por error de prueba automatizada en Microsoft Azure" (p. 1132).

Si, por algún motivo, la conmutación por error de prueba se omite, se emitirá una alerta.

Nota
La conmutación por error de prueba automatizada fallará si las copias de seguridad del equipo original están cifradas utilizando el cifrado como una propiedad del equipo, y la contraseña de cifrado no se especifica al crear el servidor de recuperación. Para obtener más información sobre cómo especificar la contraseña de cifrado, consulte "Creación de servidores de recuperación en Microsoft Azure" (p. 1122).

Configuración de la conmutación por error de prueba automatizada en Microsoft Azure

Al configurar la conmutación por error de prueba automatizada, puede probar el servidor de recuperación de forma mensual sin ejecutar ninguna acción manual.

Para configurar la conmutación por error de prueba automatizada de un servidor de recuperación en Microsoft Azure

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Panel de control**.
2. En el widget **Conmutación por error de prueba automatizada**, haga clic en **Configurar**.
3. En el cuadro de diálogo **Configuración de la conmutación por error automátizada en modo de prueba**, seleccione uno o más servidores de recuperación para los que desee configurar la conmutación por error de prueba automatizada y, a continuación, haga clic en **Siguiente**.
4. Active el interruptor **Conmutación por error de prueba automatizada**.
5. En el campo **Planificación**, seleccione **Mensual**.
6. [Opcional] En **Tiempo de espera de inicio de la MV / Minutos**, cambie el valor predeterminado del período máximo durante el cual el sistema intenta iniciar la máquina virtual en Azure y tomar una captura de pantalla para verificar si el sistema operativo se cargó correctamente.

© Acronis International GmbH, 2003-2025

Nota

- Este tiempo de espera no incluye el tiempo necesario para restaurar datos desde un archivo de copia de seguridad en frío. El temporizador comienza cuando la máquina virtual empieza el arranque.
- Durante la restauración de datos en frío, Azure crea temporalmente un almacenamiento Blob estándar, que posteriormente se convierte en un disco administrado para la máquina virtual.
- Las horas de cálculo de la máquina virtual de Microsoft Azure no se contabilizan durante el proceso de restauración de datos.

7. [Opcional] Para guardar el valor **Tiempo de espera de inicio de la MV** como predeterminado y que se rellene automáticamente cuando habilite la conmutación por error de prueba automatizada para el resto de servidores de recuperación, seleccione **Establecer como tiempo de espera predeterminado**.
8. Haga clic en **Configurar**.

En la pestaña **Servidores de recuperación**, puede ver que se ha iniciado la conmutación por error de prueba automatizada. Después de que se complete, se eliminará la máquina virtual y podrá encontrar el enlace a la captura de pantalla del sistema operativo validado en los detalles del servidor de recuperación.

Ver el estado de la conmutación por error de prueba automatizada

Puede ver la información de una conmutación por error de prueba automatizada completada de un servidor de recuperación en Microsoft Azure, como el estado, la hora de inicio, la hora de finalización, la duración y la captura de pantalla de la máquina virtual.

Nota

La captura de pantalla de la máquina virtual se conserva hasta que la conmutación por error de la prueba automatizada se ejecuta de nuevo y genera una nueva captura de pantalla.

Pasos para ver el estado de la conmutación por error de prueba automatizada de un servidor de recuperación en Microsoft Azure

1. En la consola, vaya a **Disaster Recovery** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. En la sección **Conmutación por error de prueba automatizada**, compruebe la información de la última conmutación por error de prueba automatizada.
3. [Opcional] Para ver la captura de pantalla de la máquina virtual, haga clic en **Mostrar captura de pantalla**.

Deshabilitación de la conmutación por error de prueba automatizada

Puede deshabilitar la conmutación por error de prueba automatizada si desea ahorrar recursos o no necesita que se ejecute en un determinado servidor de recuperación en Microsoft Azure.

© Acronis International GmbH, 2003-2025

Para deshabilitar la conmutación por error de prueba automatizada para un servidor de recuperación en Microsoft Azure

1. En la consola, vaya a **Disaster Recovery** > **Servidores de recuperación** y seleccione el servidor de recuperación.
2. Haga clic en **Editar**.
3. En el asistente, haga clic en la pestaña **Conmutación por error de prueba automatizada**.
4. Desactive el interruptor **Conmutación por error de prueba automática**.
5. Haga clic en **Guardar**.

Requisitos y limitaciones para la conmutación por error de máquinas virtuales Linux a Microsoft Azure

Esta sección describe los principales requisitos y limitaciones para la conmutación por error de cargas de trabajo de Linux a Microsoft Azure, especialmente en entornos sin acceso a Internet.

Requisitos

Instalación del agente de máquina virtual de Microsoft Azure con acceso a Internet

El agente de la máquina virtual de Microsoft Azure se instala automáticamente durante la conmutación por error de prueba y producción.

Las herramientas de Linux necesarias (por ejemplo, **cloud-init**, controladores de red) se obtienen de repositorios públicos (por ejemplo, `archive.ubuntu.com` o `mirror.centos.org`).

Por motivos de seguridad, puede permitir la salida de HTTPS solo a repositorios específicos.

Instalación del Agente de máquina virtual de Microsoft Azure sin acceso a Internet

Debe instalar manualmente el Agente de máquina virtual de Microsoft Azure en el equipo Linux de origen antes de la conmutación por error.

Sin el agente, la conmutación por error puede fallar o resultar en una funcionalidad limitada de la máquina virtual.

Limitaciones

Dependencia de Internet

La falta de acceso a Internet en la máquina virtual de Microsoft Azure de destino requerirá que se preinstale un agente de Azure en la carga de trabajo original, lo que añade una sobrecarga de configuración.

La falta de acceso a Internet puede impedir las actualizaciones posteriores a la conmutación por error (por ejemplo, las herramientas de conexión a redes o de copia de seguridad).

© Acronis International GmbH, 2003-2025

Recomendaciones

- Permitir el acceso a Internet para la red virtual de producción y prueba antes de la conmutación por error. Este es un ajuste predeterminado.
- Restringir el acceso saliente a solo repositorios de Linux específicos si los conoce antes de una conmutación por error.
- Restringir el acceso a servicios de producción específicos durante las conmutaciones por error de prueba.
- Puede utilizar imágenes reflejadas internas o VPN para minimizar la dependencia de Internet.
- Ejecute pruebas de conmutación por error de forma regular para garantizar la disponibilidad del entorno.

Conmutación tras recuperación en Microsoft Azure

La conmutación tras recuperación es un proceso que consiste en mover la carga de trabajo desde la nube a la máquina física o virtual en su sitio local. Puede realizar una conmutación tras recuperación en un servidor de recuperación en estado de **Conmutación por error** y seguir usando el servidor en su sitio local.

Puede ejecutar una conmutación por error automatizada en una máquina virtual o un equipo físico en su sitio local. Durante la conmutación tras recuperación, mientras la máquina virtual funciona en la nube, puede transferir los datos de la copia de seguridad al sitio local. Esta tecnología le ayuda a obtener un tiempo de inactividad muy breve, que se calcula y aparece en la consola de Cyber Protect. Puede verlo y usar esta información para planificar sus actividades y, si fuese necesario, advertir a sus clientes sobre un próximo tiempo de inactividad. Si realiza conmutación tras recuperación basada en agente con un dispositivo de arranque, el tiempo de inactividad aún será menor, porque los cambios delta se transferirán al sitio local.

Para una conmutación tras recuperación a un equipo físico de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque. Para obtener más información, consulte "Conmutación tras recuperación basada en agente mediante dispositivos de arranque de Microsoft Azure" (p. 1136).

Para una conmutación tras recuperación a una máquina virtual de destino, puede utilizar la conmutación tras recuperación basada en agente a través de un dispositivo de arranque o la conmutación tras recuperación sin agente a través del agente de hipervisor. Para obtener más información, consulte "Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure" (p. 1137) y "Realización de conmutación tras recuperación sin agente a través de un agente hipervisor desde Microsoft Azure" (p. 1142).

Cuando no pueda usar el procedimiento de conmutación tras recuperación automatizada, puede realizarla de forma manual. Para obtener más información, consulte "Conmutación tras recuperación manual desde Microsoft Azure" (p. 1146).

© Acronis International GmbH, 2003-2025

Nota
Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso de **Ejecutar una conmutación por recuperación del servidor**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.

Conmutación tras recuperación basada en agente mediante dispositivos de arranque de Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El proceso de conmutación tras recuperación basada en agente mediante dispositivos de arranque está optimizado para realizar una conmutación tras recuperación a la máquina física o virtual original. Durante este proceso, solo se transfieren los cambios delta al sitio local.

El proceso de conmutación tras recuperación basada en el agente a través de un dispositivo de arranque a una máquina física o virtual de destino consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.
2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,
   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

   Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

   Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

© Acronis International GmbH, 2003-2025

Nota
El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.
Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.
4. **Validación**. Durante esta fase, el equipo del sitio local estará listo y podrá reiniciarlo con un dispositivo de arranque basado en Linux. Compruebe que la máquina virtual funciona correctamente y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar la conmutación por error y volver a la fase de planificación.

Nota
Una vez que se haya reiniciado el dispositivo de arranque, no podrá volver a utilizarlo. Si descubre que algo va mal durante la fase de validación, debe registrar un nuevo dispositivo de arranque y volver a iniciar el proceso de conmutación tras recuperación.
Sin embargo, al utilizarse la tecnología flashback, no se volverán a transferir los datos que ya estén en el sitio local y el proceso de conmutación tras recuperación será mucho más rápido.

Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure a un equipo físico o una máquina virtual de destino en su sitio local.

© Acronis International GmbH, 2003-2025

Nota
El proceso de transferencia de datos utiliza una tecnología flashback. Esta tecnología compara los datos disponibles en el equipo de destino con los de la máquina virtual en la nube. Si parte de los datos ya están disponibles en el equipo de destino, no se transferirán de nuevo. Esta tecnología agiliza la fase de transferencia de datos.

Por ese motivo, le recomendamos que restaure el servidor en el equipo original en el sitio local.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Hay un dispositivo de arranque registrado disponible.
  Para obtener más información, consulte "Creación de soportes de arranque para recuperar sistemas operativos" (p. 983).
- El equipo de destino es el equipo original en su sitio local o tiene el mismo firmware que el equipo original.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

Pasos para llevar a cabo una conmutación por recuperación de un equipo físico

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Tipo de conmutación tras recuperación**, seleccione **Basada en agente a través de dispositivo de arranque**.
5. En el campo **Dispositivo de arranque de destino**, haga clic en **Especificar**, seleccione el dispositivo de arranque y haga clic en **Listo**.

   Nota
   Le recomendamos que utilice un dispositivo de arranque listo porque ya estará configurado. Para obtener más información, consulte "Creación de soportes de arranque para recuperar sistemas operativos" (p. 983).

6. [Opcional] Para cambiar la asignación de discos predeterminada, en el campo **Asignación de discos**, haga clic en **Especificar**, asigne los discos de la copia de seguridad a los discos del equipo de destino y haga clic en **Listo**.
7. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

© Acronis International GmbH, 2003-2025

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de transferencia de datos. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, los valores de **Progreso** aumentarán con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el progreso sea más rápido de lo que ha calculado inicialmente la consola.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo. Como el sistema utiliza una tecnología flashback durante la transferencia de datos y no transfiere los datos que están disponibles en el equipo de destino, puede que el tiempo de inactividad sea mucho menor que el valor que ha mostrado inicialmente la consola.

8. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

© Acronis International GmbH, 2003-2025

9. Cuando se complete la fase de **cambio**, reinicie el dispositivo de arranque y compruebe que el equipo físico de su sitio local funciona según lo esperado.
   Para obtener más información, consulte "Recuperar discos usando dispositivos de arranque" (p. 693).
10. Para finalizar el proceso, haga clic en **Confirmar la conmutación tras recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
    Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

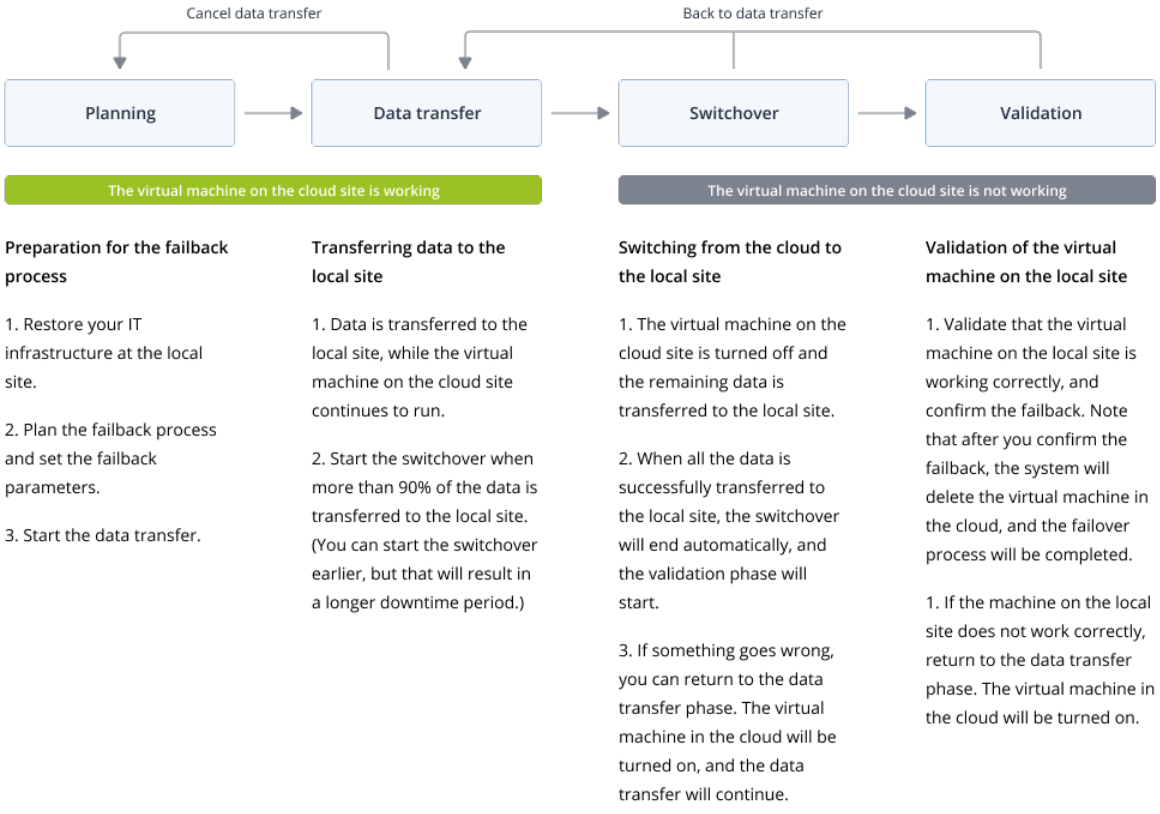
Conmutación tras recuperación sin agente mediante un agente de hipervisor desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La conmutación tras recuperación sin agente mediante un proceso de agente de hipervisor está optimizada para realizar una conmutación tras recuperación desde Microsoft Azure a una nueva máquina virtual. Si desea realizar una conmutación tras recuperación a la máquina virtual original, siga el procedimiento para la conmutación tras recuperación basada en agente mediante dispositivos de arranque.

La conmutación tras recuperación sin agente mediante un agente de hipervisor consta de cuatro fases.

© Acronis International GmbH, 2003-2025



1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.

   Nota
   Para minimizar el tiempo total del proceso de conmutación tras recuperación, le recomendamos que inicie la fase de transferencia de datos inmediatamente después de configurar sus servidores locales y, a continuación, continúe con la configuración de la red y del resto de la infraestructura local durante la fase de transferencia de datos.

2. **Transferencia de datos**. Durante esta fase, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos del sitio en la nube al sitio local. Puede iniciar la siguiente fase de cambio en cualquier momento durante la transferencia de datos, pero deberá tener en cuenta la siguientes relaciones.

   Cuanto más tiempo pase en la fase de transferencia de datos,

   - más tiempo se seguirá ejecutando la máquina virtual en la nube;
   - mayor será la cantidad de datos transferidos a su sitio local;
   - mayor será el coste que pagará (gasta más en puntos de cálculo);
   - menor será el tiempo de inactividad que experimente durante la fase de cambio.

© Acronis International GmbH, 2003-2025

Si desea reducir el tiempo de inactividad, inicie la fase de cambio cuando se haya transferido más del 90 % de los datos al sitio local.

Si no puede permitirse tener un tiempo de inactividad más largo y no desea gastar más puntos de cálculo para ejecutar la máquina virtual en la nube, puede empezar la fase de cambio antes.

Si cancela el proceso de conmutación por recuperación durante la fase de transferencia de datos, los datos transferidos no se eliminarán del sitio local. Para evitar posibles problemas, elimine de forma manual los datos transferidos antes de iniciar un nuevo proceso de conmutación por recuperación. El posterior proceso de transferencia de datos se iniciará desde el principio.

3. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y los datos restantes, incluido el incremento de la última copia de seguridad, se transferirán al sitio local. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso.

   Puede ver el tiempo estimado de finalización (tiempo de inactividad) de esta fase en la consola de Cyber Protect. Cuando todos los datos se han transferido al sitio local (no hay pérdida de datos y la máquina virtual en el sitio local es una copia exacta de la máquina virtual en la nube), se completa la fase de cambio. Se recuperará la máquina virtual en el sitio local y se iniciará la fase de validación automáticamente.
4. **Validación**. Durante esta fase, la máquina virtual en el sitio local está lista y se inicia automáticamente. Puede verificar si la máquina virtual está funcionando correctamente, y:
   - Si todo funciona según lo esperado, confirme la conmutación por recuperación. Tras la confirmación de la conmutación por recuperación, se eliminará la máquina virtual en la nube y el servidor de recuperación volverá al estado **En espera**. El proceso de conmutación por recuperación habrá terminado.
   - Si algo va mal, puede cancelar el cambio y volver a la fase de transferencia de datos.

Realización de conmutación tras recuperación sin agente a través de un agente hipervisor desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede realizar una conmutación tras recuperación sin agente desde Microsoft Azure a una máquina virtual de destino en su sitio local a través de un agente hipervisor.

Requisitos previos

- El agente que utilizará para ejecutar la conmutación por recuperación está en línea y no se está utilizando actualmente en otra operación de conmutación por recuperación.
- Su conexión a Internet es estable.
- Existe al menos una copia de seguridad completa de la máquina virtual en la nube.

© Acronis International GmbH, 2003-2025

Pasos para realizar una conmutación tras recuperación sin agente a una máquina virtual a través de un agente de hipervisor

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En la sección **Parámetros de la conmutación por recuperación**, en el campo **Tipo de conmutación tras recuperación**, seleccione **Sin agente a través del hipervisor** y, a continuación, configure los demás parámetros.

   Algunos **Parámetros de la conmutación por recuperación** se establecen automáticamente con los valores sugeridos, pero puede cambiarlos.

   La siguiente tabla proporciona más información sobre los **Parámetros de la conmutación por recuperación**.

Parámetro	Descripción
Tamaño de la copia de seguridad	La cantidad de datos que se transferirán a su sitio local durante el proceso de conmutación por recuperación. Tras iniciar el proceso de conmutación por recuperación a un equipo virtual de destino, el **Tamaño de la copia de seguridad** aumentará durante la fase de transferencia de datos debido a que el equipo virtual en la nube seguirá funcionando y generando nuevos datos. Para calcular una estimación del período de inactividad durante el proceso de conmutación por recuperación a un equipo virtual de destino, tome el 10 % del valor del **Tamaño de la copia de seguridad** (puesto que recomendamos iniciar la fase de cambio tras haberse transferido el 90 % de los datos a su sitio local) y divídalo entre el valor de la velocidad de su conexión a Internet. **Nota** El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.
Ubicación del equipo de destino	Ubicación de la conmutación por recuperación: un servidor de VMware ESXi o de Microsoft Hyper-V. Puede elegir entre todos los servidores que tienen un agente registrado en el servicio de ciberprotección.
Agente	Agente que ejecutará la operación de conmutación por recuperación. Solo puede utilizar un agente para llevar a cabo una operación de conmutación por recuperación al mismo tiempo. Puede seleccionar un agente que esté en línea y no se esté utilizando para otro proceso de conmutación por recuperación y

© Acronis International GmbH, 2003-2025

Parámetro	Descripción
	que tenga una versión que admita la funcionalidad de conmutación por recuperación y derechos para acceder a la copia de seguridad. Puede instalar varios agentes en hosts VMware ESXi e iniciar un proceso de conmutación por recuperación independiente con cada uno de ellos. Puede llevar a cabo estos procesos de conmutación por recuperación a la vez.
Configuración del equipo de destino	Configuración del equipo virtual: • **Procesadores virtuales**. Seleccione el número de procesadores virtuales. • **Memoria**. Seleccione cuánta memoria tendrá el equipo virtual. • **Unidades**. Seleccione las unidades para la memoria. • [Opcional] **Adaptadores de red**. Para añadir un adaptador de red, haga clic en **Agregar** y seleccione una red en el campo **Red**. Cuando haya acabado de hacer cambios, haga clic en **Listo**.
Ruta	(Para servidores de Microsoft Hyper-V) Carpeta en el servidor en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Almacén de datos	[Para hosts VMware ESXi] Almacén de datos en el host en el que se almacenará su máquina. Asegúrese de que hay suficiente espacio de memoria libre en el servidor para la máquina.
Modo de aprovisionamiento	Método de asignación del disco virtual. Para servidores de Microsoft Hyper-V: • **Expansión dinámica** (valor predeterminado). • **Tamaño fijo**. Para servidores de Microsoft Hyper-V: • **Ligero** (valor predeterminado). • **Grueso**.
Nombre del equipo de destino	Nombre de la máquina de destino. De forma predeterminada, el nombre de la máquina de destino es el mismo que el del servidor de recuperación. El nombre del equipo de destino debe ser único en la **Ubicación del equipo de destino** seleccionada.

5. Haga clic en **Iniciar transferencia de datos** y, en la ventana de confirmación, haga clic en **Iniciar**.

© Acronis International GmbH, 2003-2025

Nota
Si no hay una copia de seguridad de la máquina virtual en la nube, el sistema realizará una copia de seguridad automáticamente antes de la fase de transferencia de datos.

Se iniciará la fase de **transferencia de datos**. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra cuántos datos se han transferido ya al sitio local y la cantidad total de datos que se transferirán. La cantidad total de datos incluye los de la copia de seguridad más reciente antes de que se iniciase la fase de transferencia de datos y las copias de seguridad de los datos recién generados (incrementos de copia de seguridad), mientras que la máquina virtual sigue ejecutándose en la fase de transferencia de datos. Por este motivo, ambos valores del parámetro **Progreso** aumentarán con el paso del tiempo.
Estimación del tiempo de inactividad	Este parámetro muestra cuánto tiempo dejará de estar disponible la máquina virtual en la nube si inicia la fase de cambio ahora. El valor se calcula según los valores del parámetro **Progreso** y disminuye con el paso del tiempo.

6. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se iniciará la fase de cambio. La consola muestra la siguiente información:

Campo	Descripción
Progreso	Este parámetro muestra el progreso de restauración del equipo en el sitio local.
Tiempo estimado para finalizar	Este parámetro muestra el tiempo aproximado en el que se completará la fase de cambio y tras el que podrá encender el equipo en el sitio local.

Nota
Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

7. Después de que se complete la fase de **Cambio** y se inicie automáticamente la máquina virtual en el sitio local, verifique que esté funcionando correctamente.
8. Para finalizar el proceso, haga clic en **Confirmar la conmutación por recuperación** y, en la ventana de confirmación, haga clic en **Confirmar**.
   Se eliminará el equipo virtual en la nube y el servidor de recuperación volverá al estado **En espera**.

© Acronis International GmbH, 2003-2025

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación manual desde Microsoft Azure

Nota
Le recomendamos que utilice el proceso de conmutación tras recuperación en un modo manual solo cuando se lo indique el equipo de soporte.

También puede iniciar un proceso de conmutación tras recuperación en un modo manual. En este caso, la transferencia de datos desde la copia de seguridad en la nube al sitio local no se llevará a cabo de forma automática. Se debe hacer de forma manual cuando la máquina virtual en la nube esté apagada. Esto hace que el proceso de conmutación tras recuperación en un modo manual sea mucho más lento y probablemente el tiempo de inactividad también sea mayor.

El proceso de conmutación tras recuperación en un modo manual consta de las siguientes fases:

1. **Planificación**. Durante esta fase, restaure la infraestructura de TI en su sitio local (como los servidores y las configuraciones de red), configure los parámetros de la conmutación tras recuperación y planifique el inicio de la transferencia de datos.
2. **Cambio**. Durante esta fase, la máquina virtual en la nube se apagará y se hará una copia de seguridad de los datos recién generados. Si no se aplica ningún plan de copias de seguridad en el servidor de recuperación, se ejecutará automáticamente una copia de seguridad durante la fase de cambio y ralentizará el proceso. Cuando la copia de seguridad haya finalizado, restaure la máquina en el sitio local de forma manual. Puede recuperar el disco mediante un dispositivo de arranque o toda la máquina desde el almacenamiento de la copia de seguridad en la nube.
3. **Validación**. Durante esta fase, verifique que el equipo físico o la máquina virtual en el sitio local funciona correctamente y confirme la conmutación tras recuperación. Tras la confirmación, se eliminará la máquina virtual en el sitio en la nube y el servidor de recuperación volverá al estado **En espera**.

Realización de una conmutación tras recuperación manual desde Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación manual desde Microsoft Azure en un equipo físico o virtual de destino en su sitio local.

Pasos para llevar a cabo una conmutación tras recuperación manual

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Servidores**.
2. Seleccione un servidor de recuperación cuyo estado sea **Conmutación por error**.
3. Haga clic en la pestaña **Conmutación por recuperación**.
4. En el campo **Destino**, seleccione **Equipo físico**.
5. Haga clic en el icono de engranaje y habilite el conmutador **Usar el modo manual**.
6. [Opcional] Calcule una estimación del período de inactividad durante el proceso de conmutación por recuperación mediante la división del valor del **Tamaño de la copia de seguridad** entre el valor de la velocidad de su conexión a Internet.

   Nota
   El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.

7. Haga clic en **Cambio** y en la ventana de confirmación vuelva a hacer clic en **Cambio**.
   Se apagará la máquina virtual en el sitio en la nube.

   Nota
   Si no se aplica ningún plan de copias de seguridad en la máquina virtual de la nube, se ejecutará automáticamente una copia de seguridad durante la fase de cambio, lo cual ralentizará el proceso.

8. Recupere el servidor desde una copia de seguridad en la nube al equipo físico o a la máquina virtual en su sitio local.
   Para obtener más información, consulte "Recuperación del equipos virtuales" (p. 678) y "Recuperación de equipos físicos" (p. 663).

   Nota
   Si está realizando una conmutación tras recuperación desde una máquina virtual de Microsoft Azure a la máquina virtual de Azure original, utilice las opciones de recuperación que se describen en "Conmutación tras recuperación desde Microsoft Azure a una máquina virtual de Azure" (p. 1148).

9. Asegúrese de que la recuperación se complete y de que la máquina recuperada funcione correctamente y haga clic en **Se ha restaurado el equipo**.
10. Si todo funciona según lo esperado, haga clic en **Confirmar la conmutación por recuperación** y en la ventana de confirmación vuelva a hacer clic en **Confirmar**.
    El servidor de recuperación y los puntos de recuperación pasarán a estar disponibles para la conmutación por error. Para crear puntos de recuperación, aplique un plan de protección al nuevo servidor local.

© Acronis International GmbH, 2003-2025

Nota
Aplicar un plan de protección en el servidor recuperado no forma parte del proceso de conmutación por recuperación. Una vez que finalice este proceso, aplique un plan de protección en el servidor recuperado para asegurarse de que vuelve a estar protegido. Puede aplicar el mismo plan de protección que se aplicó al servidor original o un nuevo plan que tenga habilitado el módulo **Recuperación ante desastres**.

Conmutación tras recuperación desde Microsoft Azure a una máquina virtual de Azure

Puede realizar una conmutación tras recuperación desde una máquina virtual de Microsoft Azure a la máquina virtual de Azure original siguiendo el procedimiento para "Realización de una conmutación tras recuperación manual desde Microsoft Azure" (p. 1146) y utilizando una de las siguientes opciones de recuperación en el paso 8:

Opciones de recuperación

- Recuperación sin agente

  Soporta la recuperación solo a una nueva máquina virtual de Microsoft Azure que se crea automáticamente.

  Proceso: configure la conexión de Azure en la consola de Cyber Protect (**Dispositivos** > **Agregar** > **Máquina virtual de Microsoft Azure**).

  Se despliega una máquina virtual de dispositivo de copia de seguridad en la suscripción de Azure para gestionar la recuperación.

  Flujo de recuperación:

  En la pantalla **Almacenamiento de la copia de seguridad**, seleccione una copia de seguridad. Recupérela como una máquina virtual de Azure.

  Puede utilizar el mismo flujo para copias de seguridad físicas, virtuales o basadas en agente.

  Consideración de costes: la máquina virtual de dispositivo, cuando se utiliza solo para la recuperación, únicamente se puede encender durante la recuperación y luego se apaga manualmente.
- Recuperación basada en agente

  Admite la recuperación en la misma máquina virtual de Microsoft Azure (si la máquina virtual original con el agente está disponible) o en una nueva máquina virtual de Azure que tenga un nuevo agente instalado.

  Proceso: cree manualmente una máquina virtual limpia con Windows/Linux en Azure. Instale el agente de protección. Utilice el agente para examinar y recuperar copias de seguridad del almacenamiento en Acronis Cloud Storage.

  Para obtener más información, consulte Recuperación de máquinas de Microsoft Azure y Amazon EC2.

© Acronis International GmbH, 2003-2025

Runbooks en Microsoft Azure

Un runbook es un conjunto de instrucciones en las que se describe la forma de lanzar el entorno de producción en la nube.

Con los runbooks, puede:

- Automatizar la conmutación por error de uno o varios servidores.
- Hacer ping en la dirección IP del servidor y comprobar la conexión al puerto que especifique para poder comprobar automáticamente el resultado de la conmutación por error.
- Establecer la secuencia de operaciones de los servidores mediante la ejecución de aplicaciones distribuidas.
- Incluir operaciones manuales en el flujo de trabajo.
- Verifique la integridad de su solución de recuperación ante desastres mediante la ejecución de runbooks en modo de prueba.

Runbooks para automatizar la operación de conmutación por error y garantizar que sus sistemas se recuperen en el orden correcto para abordar las dependencias entre aplicaciones.

Los runbooks le permiten automatizar una conmutación por error de uno o varios servidores. Puede configurar la secuencia correcta de las operaciones de conmutación por error para los servidores ejecutando las aplicaciones distribuidas. Puede ejecutar runbooks en modo de producción o prueba para comprobar la integridad de su solución de recuperación ante desastres.

Creación de un runbook en Microsoft Azure

Un runbook consiste en pasos que se ejecutan consecutivamente. Un paso consiste en acciones que comienzan simultáneamente.

Para crear un runbook en Microsoft Azure

1. En la consola de Cyber Protection, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en **Crear runbook**.
3. Haga clic en **Añadir paso**.
4. Haga clic en **Añadir acción** y seleccione la acción que quiere añadir al paso.

Acción	Descripción
Conmutar por error el servidor	Realiza una conmutación por error de un servidor de recuperación. Para definir esta acción, debe seleccionar un servidor de recuperación y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook en Microsoft Azure" (p. 1151).

© Acronis International GmbH, 2003-2025

Acción	Descripción
	Nota Si la copia de seguridad del servidor que selecciona está cifrada utilizando el cifrado como una propiedad del equipo, la acción de **Conmutar por error el servidor** se detendrá y cambiará automáticamente a **Se requiere interacción**. Para continuar con la ejecución del runbook, tendrá que proporcionar la contraseña de la copia de seguridad cifrada.
Conmutar por recuperación el servidor	Realiza una conmutación tras recuperación de un servidor en la nube. Para definir esta acción, debe seleccionar un servidor en la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook en Microsoft Azure" (p. 1151). **Nota** Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Conmutar por recuperación el servidor**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Disaster Recovery** > **Servidores**.
Iniciar servidor	Inicia un servidor de la nube. Para definir esta acción, debe seleccionar un servidor de la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estas configuraciones, consulte "Parámetros de runbook en Microsoft Azure" (p. 1151). **Nota** La acción de **Iniciar servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Detener servidor	Detiene un servidor en la nube. Para definir esta acción, debe seleccionar un servidor en la nube y configurar los parámetros del runbook que están disponibles para esta acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook en Microsoft Azure" (p. 1151). **Nota** La acción **Detener servidor** no es aplicable para operaciones de conmutación por error de prueba en runbooks. Si intenta ejecutar dicha acción, fallará con el mensaje de error siguiente: Error: La acción no se aplica al estado actual del servidor.
Operación manual	Una operación manual requiere una interacción de un usuario. Para definir esta acción, debe ingresar una descripción.

© Acronis International GmbH, 2003-2025

Acción	Descripción
	Cuando una secuencia de runbook llega a una operación manual, el runbook se detendrá y no procederá hasta que un usuario realice la operación manual requerida, como hacer clic en el botón de confirmación.
Ejecutar runbook	Ejecuta otro runbook. Para definir esta acción, debe elegir un runbook. Un runbook puede estar formado únicamente por una ejecución de un runbook determinado. Por ejemplo, si añade la acción "ejecutar Runbook A", puede incluir la acción "ejecutar Runbook B", pero no puede añadir otra acción "ejecutar Runbook A".

5. Defina los parámetros del runbook para la acción. Para obtener más información sobre estos parámetros, consulte "Parámetros de runbook" (p. 1102).
6. [Opcional] Para añadir una descripción del paso:
   a. Haga clic en el icono de puntos suspensivos y, luego, en **Descripción**.
   b. Introduzca una descripción del paso.
   c. Haga clic en **Listo**.
7. Repita los pasos del 3 al 6 hasta que cree la secuencia de pasos y acciones deseada.
8. [Opcional] Para cambiar el nombre predeterminado del runbook:
   a. Haga clic en el icono de puntos suspensivos.
   b. Introduzca el nombre del runbook.
   c. Introduzca una descripción del runbook.
   d. Haga clic en **Listo**.
9. Haga clic en **Guardar**.
10. Haga clic en **Cerrar**.

Parámetros de runbook en Microsoft Azure

Los parámetros de runbook son configuraciones específicas que debe configurar para definir una acción de runbook. Definen el comportamiento del runbook dependiendo del estado inicial o resultado de la acción.

En la tabla a continuación se describen los parámetros configurables del runbook para cada acción.

Parámetro de runbook	Disponible para actuar	Descripción
Continuar si ya se ha realizado	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el**	Este parámetro define el comportamiento del runbook cuando la acción requerida ya se ha realizado (por ejemplo, ya se ha realizado una conmutación por error o un servidor ya está en funcionamiento). Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook

© Acronis International GmbH, 2003-2025

Parámetro de runbook	Disponible para actuar	Descripción
	servidor	también falla. Por defecto, este parámetro está habilitado.
Continuar si falla	• **Conmutar por error el servidor** • **Iniciar servidor** • **Detener servidor** • **Conmutar por recuperación el servidor**	Este parámetro define el comportamiento del runbook cuando la acción requerida falla. Cuando está habilitado, el runbook emite un aviso y continúa. Cuando está deshabilitado, la acción falla y luego el runbook también falla. Por defecto, este parámetro está desactivado.

Operaciones con runbooks en Microsoft Azure

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Cuando un runbook no se está ejecutando, están disponibles las siguientes operaciones: ejecutar, editar, clonar, ver detalles y eliminar.

Ejecutar

Cada vez que haga clic en **Ejecutar**, se le pedirá que establezca los parámetros de la ejecución. Estos parámetros se aplicarán a todas las operaciones de conmutación por error y tras recuperación incluidas en el runbook. Si hay runbooks especificados en las operaciones de **Ejecutar runbook**, heredarán estos parámetros del runbook principal.

Para ejecutar un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en el runbook que quiera ejecutar y luego en **Ejecutar**.

© Acronis International GmbH, 2003-2025

3. En la ventana **Parámetros de ejecución**, configure los parámetros.

Parámetro	Descripción
Modo conmutación por error y conmutación por recuperación	Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación tras recuperación se corresponderá con el modo de conmutación por error seleccionado.
Punto de recuperación de conmutación por error	Seleccione el punto de recuperación más reciente (por defecto) o seleccione un momento dado en el pasado. Si selecciona un momento dado en el pasado, se seleccionarán los puntos de recuperación más cercanos antes de la fecha y hora especificadas para cada servidor.

4. Haga clic en **Iniciar**.

   La ejecución del runbook comienza. Puede detener la ejecución del runbook. El software completará todas las acciones ya iniciadas, excepto las que requieran interacción del usuario.

Editar

Pasos para editar un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en el runbook que quiera ejecutar y luego en **Editar**.
3. Edite el runbook.
4. Haga clic en **Guardar**.

Clonar

Cuando clona un runbook, el historial del runbook original no se clona.

Pasos para clonar un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en el runbook que quiera ejecutar y luego en **Clonar**.
3. [Opcional] En la ventana de clonación, edite el nombre predeterminado y escriba una descripción.
4. Haga clic en **Clonar**.

Ver detalles

Para ver los detalles de un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga clic en el runbook cuyos detalles desea ver.
   Se muestran los detalles del runbook y el historial de ejecución.

© Acronis International GmbH, 2003-2025

3. [Opcional] Para ver el registro de ejecución de una ejecución en concreto, haga clic en la línea que le corresponda.

Eliminar

Para eliminar un runbook

1. En la consola de Cyber Protect, vaya a **Disaster Recovery** > **Runbooks**.
2. Haga click en el runbook que quiera eliminar y, a continuación, pulse en **Eliminar**.
3. Haga clic en **Eliminar** en la ventana de confirmación.

Recursos de Azure que se crean durante la configuración del sitio de DR y la conmutación por error

Cuando añade una conexión a su suscripción de Azure, el sistema crea un grupo de recursos con el prefijo `cyber-protect-rg*` en la región de Azure que seleccionó durante la configuración de la conexión de Azure. Este grupo de recursos tiene la siguiente etiqueta: **Application:CyberProtect**. Para obtener más información, consulte Seguridad y auditoría de la conexión de Microsoft Azure (72684).

Cuando se completa la configuración del sitio de DR, se crea un grupo de recursos con el prefijo `dr-rg*` para agregar los recursos para la conmutación por error. Este grupo de recursos tiene la siguiente etiqueta: **Application:DisasterRecovery**.

Durante las operaciones de recuperación ante desastres, se despliegan trabajadores temporales (agentes) para orquestar la conmutación por error, la conmutación tras recuperación y las operaciones de copia de seguridad posteriores a la conmutación por error. Estas son máquinas virtuales de Microsoft Azure temporales que se ejecutan en el grupo de recursos `cyber-protect-rg*`. Todos los recursos de Azure que se requieren para una conmutación por error de recuperación ante desastres, como las cuentas de almacenamiento y las máquinas virtuales que han fallado, se crean en el grupo de recursos `dr-rg*`. Puede gestionar la región de Azure para el grupo de recursos de conexión de Azure, el grupo de recursos de DR y sus recursos asociados durante la configuración del sitio de DR.

Eliminación reversible de inquilinos que tienen un sitio de recuperación en Microsoft Azure

La función de eliminación reversible de inquilinos (papelera de reciclaje) es compatible con la configuración del sitio de DR de Microsoft Azure.

Para garantizar la continuidad de la actividad empresarial durante la eliminación reversible y definitiva, las máquinas virtuales de Microsoft Azure en conmutación por error no se detendrán ni se eliminarán.

Caso extremo

© Acronis International GmbH, 2003-2025

Si desactiva el elemento de oferta **DR y copia de seguridad directa en Azure** (ya sea intencionadamente o accidentalmente), se activa una eliminación reversible de la configuración de la recuperación ante desastres (DR) de Azure. Esto significa que la configuración se elimina, pero permanece en la papelera de reciclaje durante 30 días. Si durante este período configura un nuevo sitio de DR en una ubicación diferente (no en Microsoft Azure), para recuperar la configuración inicial de DR en Microsoft Azure, debe habilitar el elemento de oferta **DR y copia de seguridad directa en Azure**, eliminar la nueva configuración y, a continuación, recuperar la inicial.

Trabajadores en Microsoft Azure

Los trabajadores (workers) son agentes temporales y bajo demanda que se ejecutan en su suscripción de Azure en el grupo de recursos del sistema (con el prefijo: "cyber-protect-rg*") durante las operaciones de recuperación ante desastres, como la conmutación por error, la copia de seguridad tras la conmutación por error y la conmutación tras recuperación. Se despliega un trabajador para cada operación y se elimina tras la finalización de la operación. Este modelo bajo demanda ayuda a reducir costes al desplegar automáticamente los trabajadores solo durante las operaciones de DR activas y eliminarlos después.

El despliegue inicial del trabajador para una conmutación por error de prueba o producción puede tardar varios minutos. Iniciar trabajadores para las conmutaciones por error posteriores debería ser más rápido.

Para supervisar el estado de los trabajadores activos, vaya a **Nubes públicas**, haga clic en la conexión a su suscripción de Microsoft Azure y luego pulse en la pestaña **Trabajadores**.

Si una operación de recuperación ante desastres falla debido a un error con el trabajador, puede generar un informe y ver más información sobre dicho error. Para ello, vaya a la pestaña **Trabajadores**, active el interruptor **Resolución de problemas**, haga clic en el enlace **Instrucciones** y siga las instrucciones.

Panel de control de recuperación ante desastres

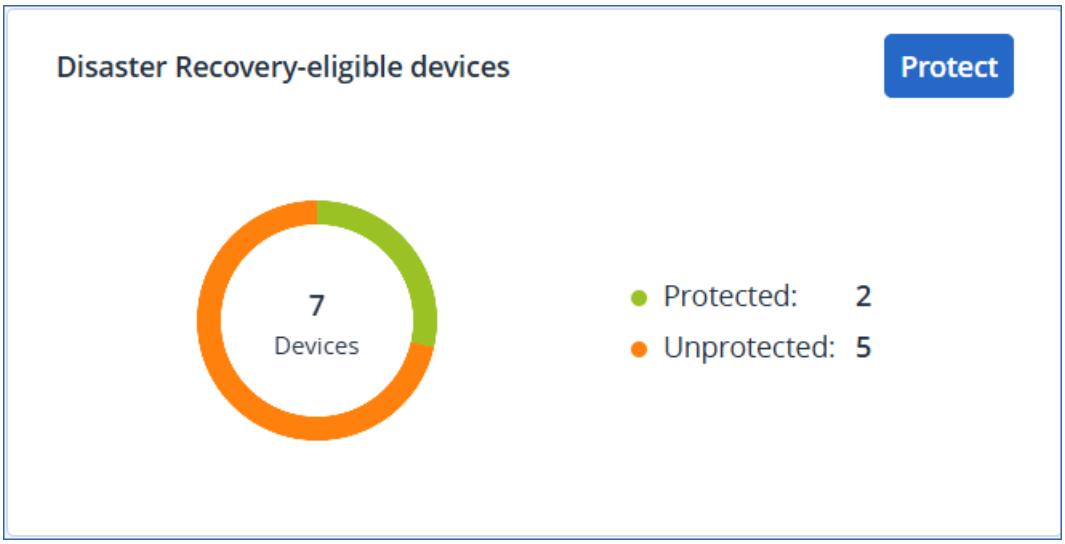
La página del **Panel de control** de Disaster Recovery contiene widgets que proporcionan un resumen en tiempo real y conocimientos prácticos para su sitio de recuperación ante desastres a lo largo de su ciclo de vida. Esto le ayuda a:

- Detecte y resuelva rápidamente los problemas mediante la supervisión del estado de los servidores de recuperación y principales.
- Evite el uso excesivo de puntos de cálculo al supervisar el número de servidores que los consumen.

Dispositivos elegibles para la recuperación ante desastres

El widget muestra el número total de dispositivos que están protegidos por recuperación ante desastres (tienen un servidor de recuperación) y el número total de dispositivos que son elegibles para la protección por recuperación ante desastres.

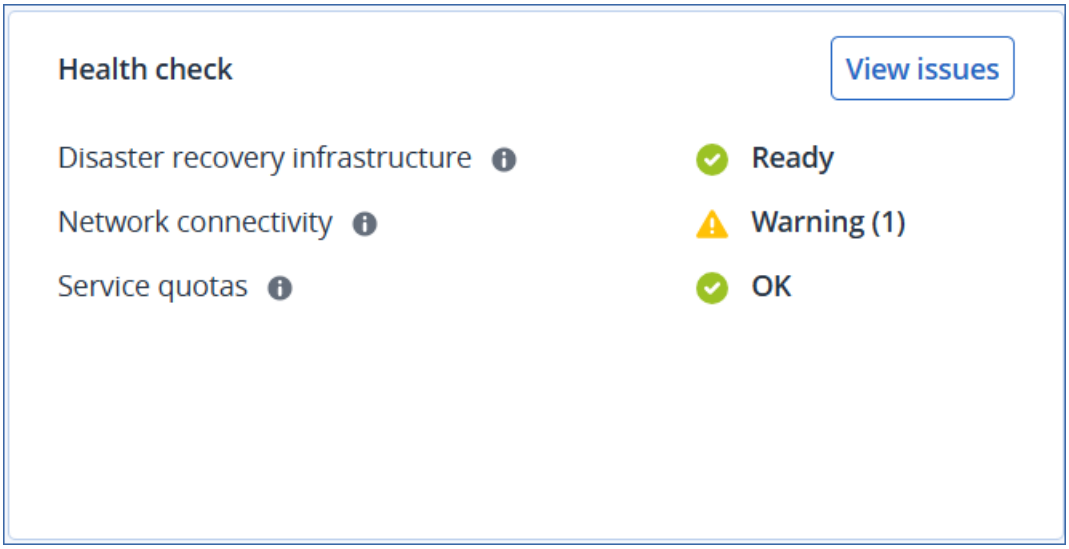
© Acronis International GmbH, 2003-2025



Para ir a la página **Todos los dispositivos** donde puede configurar la recuperación ante desastres para los dispositivos elegibles, haga clic en **Proteger**.

Comprobación del estado

El widget muestra información sobre el estado de su infraestructura de recuperación ante desastres. Puede comprobar el estado de la configuración del sitio, la disponibilidad de la red (solo disponible para Disaster Recovery en Cyber Protect Cloud) y si hay cuotas de servicio que faltan.

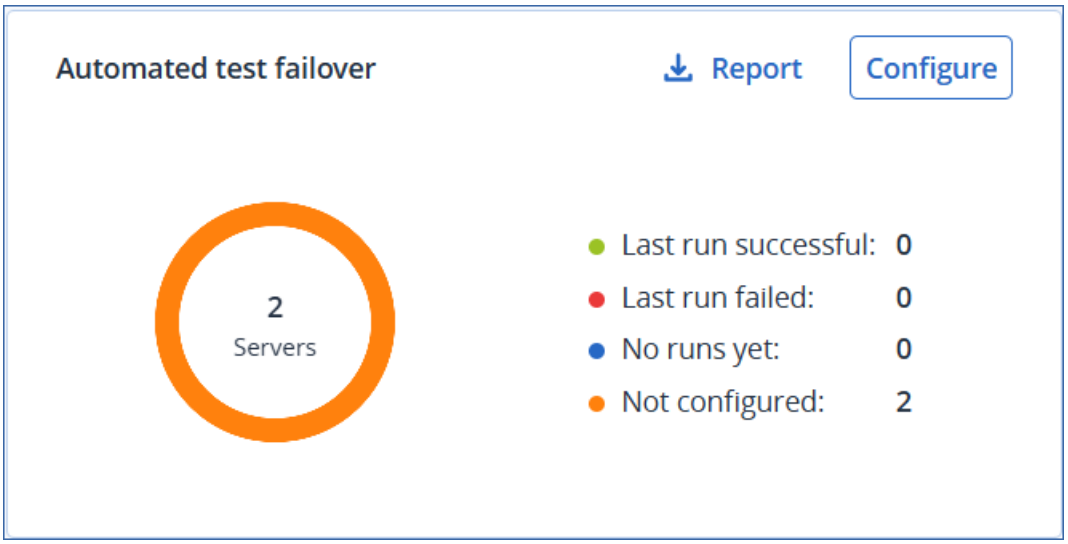


Para ver más información acerca de los problemas detectados (avisos o errores), haga clic en **Ver problemas**.

Conmutación por error de prueba automatizada

El widget muestra información acerca de las operaciones de conmutación por error de prueba automatizada de sus servidores de recuperación.

© Acronis International GmbH, 2003-2025



Para comenzar a configurar la conmutación por error de prueba automatizada para sus servidores, haga clic en **Configurar**.

Para descargar los datos del widget, haga clic en **Informe**.

Servidores de recuperación en modo de conmutación por error

El widget muestra el número y el estado de los servidores de recuperación que están en producción o en conmutación por error en una prueba.

Si no hay servidores de recuperación en ejecución en la nube, verá un cero. Si hay un problema con algún servidor, verá un aviso o un estado de error.

El uso de puntos de cálculo por hora que se muestra es una instantánea en tiempo real, no un valor histórico. Esto significa que, si, por ejemplo, tiene dos servidores de recuperación y cada uno de ellos utiliza ocho puntos, verá un total de 16 puntos mostrados en el widget.

Puede utilizar esta información para estimar el coste de ejecución de estos servidores y también como recordatorio para detener la conmutación por error de un servidor que ya no necesita.

Servidores principales

El widget solo está disponible para Disaster Recovery en Cyber Protect Cloud. Muestra el número y el estado de los servidores principales en su entorno y su uso de puntos de cálculo por hora. Puede utilizar esta información para detectar y resolver rápidamente cualquier problema.

El uso de puntos de cálculo por hora que se muestra es una instantánea en tiempo real, no un valor histórico. Esto significa que, si, por ejemplo, tiene dos servidores de recuperación y cada uno de ellos utiliza ocho puntos, verá un total de 16 puntos mostrados en el widget.

Puede utilizar esta información para estimar el coste de ejecución de estos servidores y también como recordatorio para detener la conmutación por error de un servidor que ya no necesita.

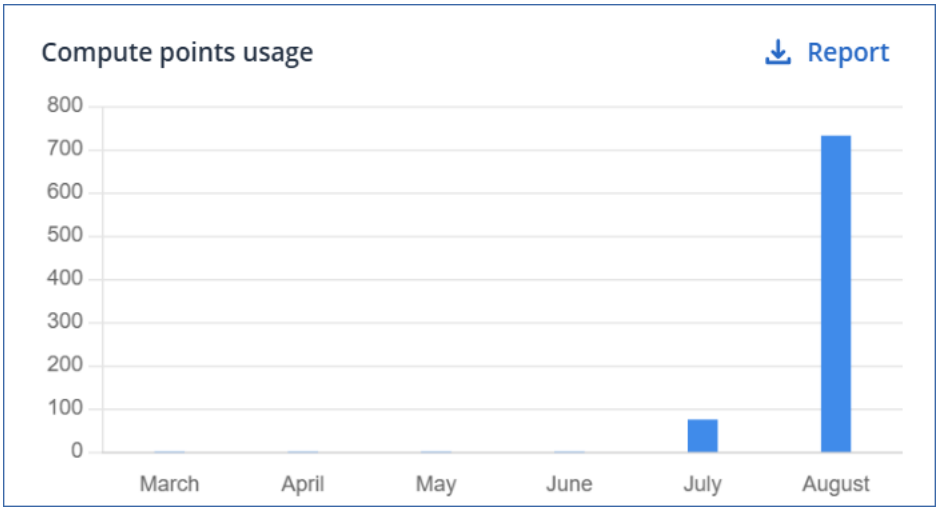
© Acronis International GmbH, 2003-2025

Alertas del servidor en la nube

El widget muestra las alertas más recientes por gravedad, para que pueda ver las alertas críticas de un vistazo. Los valores de **Tipo de alerta** y **Servidor de recuperación** en el widget son enlaces que abren los detalles de la alerta y los detalles del servidor de recuperación, respectivamente.

Uso de puntos de cálculo

Este widget muestra el número de puntos de cálculo que se han utilizado en su entorno durante los últimos 6 meses: el mes actual y cada uno de los cinco meses anteriores.



Puede descargar un informe detallado como un archivo CSV o PDF. El informe incluye la siguiente información sobre los servidores que usaron puntos de cálculo, para cada mes: nombre del servidor, tipo de servidor, estado, iniciado por, hora de inicio, hora de parada, horas activas durante el mes, uso de cálculo por hora y uso total de puntos de cálculo para el mes.

Para descargar los datos del widget, haga clic en **Informe** y, a continuación, seleccione el formato de archivo que prefiera.

Compatibilidad de Disaster Recovery con el software de cifrado

La recuperación ante desastres es compatible con el software de cifrado a nivel de disco siguiente:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

© Acronis International GmbH, 2003-2025

Nota

- Para cargas de trabajo con cifrado a nivel de disco, recomendamos que instale el agente de protección en el sistema operativo invitado de la carga de trabajo y cree copias de seguridad basadas en agente.
- La conmutación por error y la conmutación tras recuperación no serán compatibles con copias de seguridad sin agente de recursos informáticos cifrados.

Para obtener más información sobre la compatibilidad de Cyber Protection con el software de cifrado, consulte "Compatibilidad con software de cifrado" (p. 531).

© Acronis International GmbH, 2003-2025

Configuración de la protección antivirus y antimalware

Nota
En equipos Windows, las funciones de protección antimalware y filtrado de URL requieren la instalación del agente de protección antimalware y del filtrado de URL. Este agente se instalará automáticamente para los recursos informáticos protegidos si la **Protección antivirus y antimalware** y/o las opciones de **Filtrado de URL** están habilitadas en sus planes de protección.

Con la protección antimalware de Cyber Protection obtendrá los siguientes beneficios:

- Protección de calidad en todas las fases: proactivas, activas y reactivas.
- Cuatro tecnologías antimalware diferentes incluidas para proporcionar lo mejor de la protección de varias capas.
- Gestión de Microsoft Security Essentials y del antivirus Microsoft Defender.

  Nota
  La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Importante
El archivo de prueba EICAR se detecta solo cuando está habilitada la opción **Antimalware avanzado** en el plan de protección. Sin embargo, si no se detecta el archivo EICAR no afectará a las capacidades antimalware de Cyber Protection.

Sistemas operativos compatibles para la protección antivirus y antimalware

Nota
Esta funcionalidad solo es compatible con las siguientes CPU, que soportan el conjunto de instrucciones de CPU SSE4.2:

- CPU de Intel después de 2011
- CPU de AMD después de 2012

Las funciones de protección activa, antivirus y antimalware son compatibles con las plataformas siguientes.

Sistema operativo	Versión/distribución
Windows	• Windows 7 Service Pack 1 y posteriores • Windows Server 2008 R2 Service Pack 1 y posteriores

© Acronis International GmbH, 2003-2025

Sistema operativo	Versión/distribución
	Nota En Windows 7, debe instalar las siguientes actualizaciones de Microsoft antes de instalar el agente de protección: • Actualizaciones de seguridad ampliadas de Windows 7 (ESU) • KB4474419 • KB4490628 Consulte este artículo de la base de conocimientos para obtener más información sobre las actualizaciones requeridas.
Linux	• Red Hat Linux 7.x, 8.x, 9.x • CloudLinux 6.10, 7.x, 8.x • CentOS 6.5 y versiones 6.x, 7.x y 8.x posteriores • Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 • Debian 8.x, 9.x, 10,x, 11.x • Oracle Linux 7.x, 8.x, 9.x • SUSE Enterprise Linux 15.x • openSUSE Leap 15.x **Nota** El motor de análisis de comportamiento es compatible con las siguientes versiones de Linux: • CentOS 7.x • Debian 10.x, 11.x • CloudLinux 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04 y 22.04
macOS	• macOS 10.13.x y posterior

Funciones compatibles por plataforma

Nota
La protección antimalware para Linux y macOS está disponible con el paquete Advanced Security y requiere compras adicionales.

Protección contra malware y antivirus

Característica	Windows	Linux	macOS
Funcionalidad Active Protection integrada por completo	Sí	No	No
Protección contra malware en tiempo real	Sí	Sí	Sí

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Protección contra malware en tiempo real avanzada con detección basada en firmas locales	Sí	Sí	Sí
Análisis estadístico para archivos ejecutables portátiles	Sí	No	Sí1
Análisis antimalware bajo demanda	Sí	Sí2	Sí
Protección de carpetas de red	Sí	No3	No
Protección del servidor	Sí	No	No
Análisis de archivos del archivo comprimido	Sí	No	Sí
Análisis de unidades extraíbles	Sí	No	Sí
Análisis únicamente de archivos nuevos y cambiados	Sí	No	Sí
Exclusiones de archivos/carpetas	Sí	Sí	Sí4
Exclusiones de procesos	Sí	No	Sí
Motor de análisis de comportamiento	Sí	Sí5	Sí
Prevención de vulnerabilidades	Sí	No	No
Cuarentena	Sí	Sí	Sí
Limpieza automática en cuarentena	Sí	Sí	Sí
Filtrado de URL (http/https)	Sí	No	No
Lista blanca corporativa	Sí	No	Sí
Gestión del firewall6	Sí	No	No
Gestión del antivirus Microsoft Defender 7	Sí	No	No
Gestión de Microsoft Security Essentials	Sí	No	No
Registro y gestión de la protección antivirus y antimalware mediante Windows Security Center	Sí	No	No

1 El análisis estático de archivos ejecutables portátiles solo se admite para análisis programados en macOS.

2 En Linux, las condiciones para un análisis bajo demanda no están admitidas.

3 Las carpetas de red en Linux se tratan como carpetas locales, por lo que Active Protection protegerá automáticamente las carpetas de red en el sistema operativo Linux, como si fueran carpetas locales.

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
4 Las exclusiones de archivos/carpetas solo se admiten cuando se especifican archivos y carpetas que no se analizarán mediante la protección en tiempo real ni los análisis programados en macOS. 5 El motor de análisis de comportamiento es compatible con las siguientes versiones de Linux: • CentOS 7.x • Debian 10.x, 11.x • CloudLinux 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04 y 22.04 6 La gestión del cortafuegos es compatible con Windows 8 y versiones posteriores. Windows Server no es compatible. 7 La administración de Microsoft Defender Antivirus es compatible con Windows 8.1 y versiones posteriores. Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).			

Active Protection

Característica	Windows	Linux	macOS
Detección inserciones de procesos	Sí	No	No
Recuperación automática de archivos afectados de la caché local	Sí	Sí	Sí
Autodefensa de las copias de seguridad de Acronis	Sí	No	No
Autodefensa de las copias de seguridad del software Acronis	Sí	No	Sí (Solo Active Protection y componentes antimalware)
Gestión de procesos de confianza/bloqueados	Sí	No	Sí
Exclusiones de procesos/carpetas	Sí	Sí	Sí
Detección de ransomware basada en el comportamiento de un proceso (basada en IA)	Sí	Sí	Sí
Detección del proceso de criptominería basada en el comportamiento de procesos	Sí	No	No
Protección de unidades externas (discos duros, unidades flash y tarjetas SD)	Sí	No	Sí

© Acronis International GmbH, 2003-2025

Característica	Windows	Linux	macOS
Protección de carpetas de red	Sí	No*	Sí
Protección del servidor	Sí	No	No
Protección de Zoom, Cisco Webex, Citrix Workspace y Microsoft Teams	Sí	No	No

*Las carpetas de red en Linux se tratan como carpetas locales, por lo que Active Protection protegerá automáticamente las carpetas de red en el sistema operativo Linux, como si fueran carpetas locales.

Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Protección antivirus y antimalware

Nota
Algunas características podrían requerir una licencia adicional, dependiendo del modelo de licencia aplicado.

El módulo **Antivirus y antimalware** protege sus máquinas Windows, Linux y macOS de todas las amenazas de malware recientes. Consulte la lista completa de funciones antimalware compatibles en "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

La protección antimalware y antivirus es compatible con el centro de protección de Windows y viene registrada en él.

Características de la protección antimalware

- Detección de malware en archivos en los modos de protección en tiempo real y bajo demanda
- Detección de comportamientos maliciosos en los procesos (para Windows)
- Bloqueo de acceso a URL maliciosas (para Windows)
- Puesta en cuarentena de archivos peligrosos
- Inclusión de aplicaciones corporativas de confianza en la lista blanca

Tipos de análisis

Podrá configurar la protección antimalware y antivirus para que funcione de forma constante en segundo plano o a demanda.

© Acronis International GmbH, 2003-2025

Protección en tiempo real

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La protección en tiempo real comprueba todos los archivos que se van a ejecutar o abrir en una máquina para evitar las amenazas de malware.

La protección en tiempo real no funciona de forma paralela con otras soluciones antivirus que también utilizan funcionalidades en tiempo real para evitar posibles problemas de compatibilidad y rendimiento. El estado de otras soluciones antivirus instaladas se determinan mediante el Centro de seguridad de Windows. Si el equipo Windows ya está protegido por otra solución antivirus, la protección en tiempo real se apaga de forma automática.

Para habilitar la protección en tiempo real, deshabilite o desinstale la otra solución antivirus. La protección en tiempo real puede reemplazar la protección en tiempo real de Microsoft Defender de forma automática.

Nota
En máquinas que ejecutan sistemas operativos de Windows Server, Microsoft Defender no se apagará de forma automática cuando se habilite la protección en tiempo real. Los administradores deben apagar Microsoft Defender de forma manual para evitar posibles problemas de compatibilidad.

Puede escoger uno de los siguientes modos de análisis:

- La detección **En acceso inteligente** es aquella en la que el programa antimalware se ejecuta en segundo plano, y analiza de forma activa y constante su equipo en busca de virus y otras amenazas maliciosas. Además, se lleva a cabo siempre que el sistema esté encendido. En ambos casos, el malware se detectará cuando se ejecute un archivo y durante las operaciones con el mismo, por ejemplo, al abrirlo para su lectura o modificación.
- La detección **en ejecución** significa que los archivos ejecutables solo se escanean en el momento de su ejecución para garantizar que estén limpios y que no causarán ningún daño al equipo o a los datos. No se detectará la copia de un archivo infectado.

Análisis planificado

El análisis antimalware se lleva a cabo según una planificación.

Puede escoger uno de los siguientes modos de análisis.

- **Análisis rápido**: solo comprueba los archivos del sistema de carga de trabajo.
- **Análisis completo**: comprueba todos los archivos de su carga de trabajo.

© Acronis International GmbH, 2003-2025

- **Análisis personalizado**: comprueba los archivos y las carpetas que añadió el administrador al plan de protección.

Una vez que finalice el análisis antimalware, podrá ver los detalles sobre las cargas de trabajo que se vieron afectadas por amenazas en el widget **Supervisión** > **Información general** > Elementos afectados recientemente.

Configuración de los ajustes de la protección antivirus y antimalware

En esta sección se describen las funciones que puede configurar en el módulo **Protección antivirus y antimalware** de un plan de protección. Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 250).

Nota
No todos los sistemas operativos admiten las funciones de protección antivirus y antimalware. Para obtener más información sobre los sistemas operativos y las funciones compatibles, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160). Algunas funciones requieren una licencia específica para estar disponibles en su plan de protección.

Puede configurar las siguientes funciones en el módulo de Protección antivirus y antimalware para un plan de protección:

Active Protection

Active Protection protege su sistema del ransomware. El ransomware es un tipo de software malicioso que bloquea el acceso a sus archivos, sistemas o conexiones a redes virtuales cifrándolos, y luego exige un pago (rescate) para restaurar el acceso. Un ataque de ransomware puede causar una interrupción operativa grave, pérdida de datos y daño reputacional para su organización.

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Configuración predeterminada: **Habilitado**.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Nota
Debe instalarse un agente de protección en el equipo protegido. Para obtener más información sobre los sistemas operativos y las funciones compatibles, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Pasos para configurar Active Protection

© Acronis International GmbH, 2003-2025

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Active Protection**.
3. En la sección **Acción sobre la detección**, seleccione una de las opciones disponibles:
   - **Solo notificar**: el software genera una alerta sobre el proceso sospechoso de actividad de ransomware.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso sospechoso de actividad de ransomware.
   - **Revertir usando la caché**: el software genera una alerta, detiene el proceso y revierte los cambios de los archivos usando la caché de servicios.

   Configuración predeterminada: Revertir usando la caché
4. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Antimalware avanzado

Este motor utiliza una base de datos mejorada de firmas de virus para mejorar la eficiencia de la detección antimalware tanto en los análisis rápidos como completos.

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Pasos para configurar el antimalware avanzado

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. En la sección **Antimalware avanzado**, utilice el conmutador para habilitar el motor basado en firmas locales.

Nota
La protección antivirus y antimalware para macOS y Linux también requiere el motor basado en firmas locales. Para Windows, la protección antivirus y antimalware está disponible con o sin este motor.

Protección de carpetas de red

La función **Protección de carpetas de red** define si la protección antivirus y antimalware protege las carpetas de red que están asignadas como unidades locales. Esta protección se aplica a carpetas compartidas por protocolos SMB o NFS.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Pasos para configurar la protección de carpetas de red

© Acronis International GmbH, 2003-2025

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección de carpetas de red**.
3. Añada los archivos en los que quiera hacer la copia de seguridad de las carpetas de red:
   - Por ejemplo, si la carga de trabajo es Windows, en el campo **Windows**, introduzca la ruta al archivo de Windows en el que quiera hacer la copia de seguridad de las carpetas de red. Valor predeterminado: C:\ProgramData\Acronis\Restored Network Files.
   - Por ejemplo, si la carga de trabajo es macOS, en el campo **macOS**, introduzca la ruta a los archivos de macOS en los que quiera hacer la copia de seguridad de las carpetas de red. Valor predeterminado: /Library/Application Support/Acronis/Restored Network Files/.

   Nota
   Introduzca la ruta a una carpeta local. No se admiten carpetas de red, ni siquiera las de unidades asignadas, como destino de copias de seguridad para las carpetas de red.
4. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Protección del servidor

Esta función define si Active Protection protege las carpetas de la red que comparte de conexiones entrantes externas de otros servidores de la red que puedan suponer una amenaza.

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Configuración predeterminada: **Apagado**.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Nota
La protección del servidor no es compatible con Linux.

Pasos para establecer conexiones de confianza

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **De confianza**.
5. En el campo **Conexiones de confianza**, haga clic en **Agregar** para definir las conexiones que podrán modificar datos.

© Acronis International GmbH, 2003-2025

6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Haga clic en la marca de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Pasos para establecer conexiones bloqueadas

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **Bloqueadas**.
5. En el campo **Conexiones bloqueadas**, haga clic en **Agregar** para definir las conexiones que no podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Seleccione la casilla de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Autoprotección

La autoprotección evita los cambios no autorizados en los procesos propios del software, los archivos de registro, los archivos ejecutables y de configuración, y las copias de seguridad que se encuentran en las carpetas locales.

Los administradores pueden habilitar **Autoprotección**, sin habilitar **Active Protection**.

Configuración predeterminada: **Activado**.

Nota
La autoprotección no es compatible con Linux.

Pasos para habilitar la autoprotección

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Autoprotección**.
3. Utilice el conmutador **Autoprotección** para habilitarla.

© Acronis International GmbH, 2003-2025

Protección de desinstalación del agente

La configuración **Protección contra la desinstalación del agente** impide que los usuarios o el software desinstalen Agent for Windows o modifiquen sus componentes fuera de la ventana de mantenimiento configurada.

Configuración predeterminada: **Habilitado**

Pasos para deshabilitar la Protección de desinstalación del agente

Advertencia.
Si deshabilita la **Protección de desinstalación del agente** pone en riesgo la seguridad de los recursos informáticos protegidos.

1. Una vez que la función de **Autoprotección** está habilitada, puede seleccionar la casilla de verificación **Protección de desinstalación del agente**.
2. Haga clic en **Listo**.

Nota
Esta opción no impide las actualizaciones automáticas del agente de Cyber Protection.

Cada intento de desinstalar o modificar el agente de protección fuera de la ventana de mantenimiento activa una alerta.

Un usuario administrador puede revisar la alerta y decidir si permite modificaciones al agente durante 1 hora o configurar una ventana de mantenimiento con una duración entre 1 hora y 7 días. Consulte "Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada" (p. 213).

Permitir que procesos específicos modifiquen las copias de seguridad

La configuración **Permitir que procesos específicos modifiquen las copias de seguridad** solo está disponible si está habilitada la configuración **Autoprotección**.

Se aplica a archivos en carpetas locales con las siguientes extensiones:

- .tibx
- .tib
- .tia

La configuración **Permitir que procesos específicos modifiquen las copias de seguridad** le permite especificar los procesos que pueden modificar los archivos de copia de seguridad, aunque estos estén protegidos por autoprotección. Esto resulta útil, por ejemplo, si elimina archivos de copia de seguridad o los mueve a una ubicación diferente mediante un script.

Cuando esta configuración está desactivada, los archivos de copia de seguridad solo pueden ser modificados por procesos firmados por el proveedor del software de copia de seguridad. Esto

© Acronis International GmbH, 2003-2025

permite al software aplicar reglas de retención y eliminar copias de seguridad cuando un usuario lo solicita desde la interfaz web. Otros procesos, independientemente de que sean sospechosos o no, no pueden modificar las copias de seguridad.

Cuando esta configuración está habilitada, puede permitir que otros procesos modifiquen las copias de seguridad.

Configuración predeterminada: **Deshabilitado**.

Para habilitar Permitir que procesos específicos modifiquen las copias de seguridad

1. Cuando la función **Autoprotección** está habilitada, seleccione la casilla de verificación **Permitir que procesos específicos modifiquen las copias de seguridad**.
2. En el campo **Proceso para modificar copias de seguridad**, haga clic en **Agregar**.
3. Introduzca la ruta completa al archivo ejecutable del proceso, comenzando por la letra de la unidad.
4. Haga clic en la marca de verificación situada a la derecha para guardar el proceso.

Detección del proceso de criptominería

El malware de criptominería afecta al rendimiento de aplicaciones de utilidad, aumenta el importe de las facturas de electricidad, puede hacer que el sistema se bloquee e, incluso, dañar el hardware debido a su explotación. La función **Detección del proceso de criptominería** protege los dispositivos del malware de criptominería para impedir el uso no autorizado de los recursos del equipo.

Los administradores pueden habilitar **Detección del proceso de criptominería**, sin habilitar **Active Protection**. Configuración predeterminada: **Habilitado**.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Nota
La detección del proceso de criptominería no es compatible con Linux.

Para configurar la detección del proceso de criptominería

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Detección del proceso de criptominería**.
3. Utilice el conmutador **Detectar procesos de criptominería** para habilitar o deshabilitar la función.
4. Seleccione qué se debe hacer con los procesos sospechosos de actividad de criptominería:

   Configuración predeterminada: **Detener el proceso**

   - **Solo notificar**: el software genera una alerta.

© Acronis International GmbH, 2003-2025

- **Detener el proceso**: el software genera una alerta y detiene el proceso.

5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Configuración de cuarentena

La carpeta Cuarentena sirve para aislar los archivos sospechosos (posiblemente infectados) o potencialmente peligrosos.

Pasos para configurar Cuarentena

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Cuarentena**.
3. En el campo **Eliminar archivos en cuarentena después de**, puede definir el periodo en días tras el que se eliminarán los archivos que están puestos en cuarentena.
   Configuración predeterminada: **30 días**
4. Haga clic en **Listo**.

Para obtener más información sobre esta función, consulte Cuarentena.

Motor de comportamiento

La función **Motor de comportamiento** protege un sistema contra el malware aplicando un método heurístico de comportamiento para identificar procesos maliciosos.

Configuración predeterminada: **Habilitado**.

Pasos para configurar la protección de carpetas de red

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Motor de comportamiento**.
3. Utilice el conmutador **Motor de comportamiento** para habilitar o deshabilitar la función.
4. En la sección **Acción sobre la detección**, seleccione la acción que el software deberá realizar al detectar una actividad de malware:
   Configuración predeterminada: **Cuarentena**
   - **Solo notificar**: el software genera una alerta sobre el proceso sospechoso de actividad de malware.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso sospechoso de actividad de malware.
   - **Cuarentena**: el software genera una alerta, detiene el proceso y traslada los archivos ejecutables a la carpeta de cuarentena.
5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

© Acronis International GmbH, 2003-2025

Prevención de vulnerabilidades

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La prevención de vulnerabilidades detecta e impide que los procesos infectados se expandan y se aprovechen de las vulnerabilidades de software de los sistemas. Cuando se detecta una vulnerabilidad de seguridad, el software puede generar una alerta y detener el proceso sospechoso de actividad de vulnerabilidades.

La prevención de vulnerabilidades solo está disponible con agentes de versiones 12.5.23130 (21.08, lanzada en agosto de 2020) o posteriores.

Configuración predeterminada: **Habilitado** para planes de protección creados recientemente, y **Deshabilitado** para planes de protección existentes, creados con versiones de agente anteriores.

Nota
La prevención de vulnerabilidades no es compatible con Linux.

Puede seleccionar lo que debe hacer el programa cuando se detecte una vulnerabilidad y los métodos de prevención de vulnerabilidades que aplica el programa.

Pasos para configurar la prevención de vulnerabilidades

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Prevención de vulnerabilidades**.
3. En la sección **Acción sobre la detección**, seleccione una de las opciones disponibles:

   Configuración predeterminada: **Detener el proceso**

   - **Solo notificar**
     El software generará una alerta sobre el proceso sospechoso de actividades de vulnerabilidades.
   - **Detener el proceso**
     El software generará una alerta y detendrá el proceso sospechoso de actividades de vulnerabilidades.
4. En la sección **Técnicas de prevención de vulnerabilidades habilitadas**, seleccione de las opciones disponibles las que quiera aplicar:
   Configuración predeterminada: **Todos los métodos están habilitados**

   - **Protección de memoria**
     Detecta e impide la modificación sospechosa de los derechos de ejecución de las páginas de memoria. Los procesos maliciosos aplican estas modificaciones en las propiedades de las

© Acronis International GmbH, 2003-2025

páginas para permitir la ejecución de códigos de shell desde áreas de memoria no ejecutables, como las pilas o los montones.

- **Protección de la programación orientada al retorno (ROP)**

  Detecta y previene intentos de uso de la técnica de vulnerabilidad ROP.
- **Protección de escalada de privilegios**

  Detecta y evita los intentos de elevación de privilegios que ejecuta un código o una aplicación no autorizados. La escalada de privilegios la utilizan los códigos maliciosos para obtener el acceso completo del equipo atacado y luego llevar a cabo tareas esenciales y sensibles. Un código no autorizado no puede acceder a los recursos críticos del sistema ni modificar la configuración del sistema.
- **Protección de inyección de código**

  Detecta y previene la inyección de código malicioso en los procesos remotos. La inyección de código sirve para ocultar las intenciones maliciosas de una aplicación detrás de procesos limpios o benignos con el objetivo de evadir la detección por parte de los productos antimalware.

5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Nota
Los procesos que aparecen como procesos de confianza en la lista de exclusiones no se examinarán para buscar vulnerabilidades.

Protección en tiempo real

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La **Protección en tiempo real** comprueba constantemente el sistema informático para detectar virus y otras amenazas maliciosas durante todo el tiempo que el sistema esté encendido, a menos que el usuario lo detenga.

Configuración predeterminada: **Habilitado**.

Pasos para configurar la protección en tiempo real

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección en tiempo real**.
3. En la lista desplegable **Acción sobre la detección**, seleccione una de las opciones disponibles:

   Configuración predeterminada: **Cuarentena**

   - **Solo notificar**

     El software genera una alerta sobre el proceso sospechoso de actividad de ransomware.

© Acronis International GmbH, 2003-2025

- **Bloquear y notificar**

  El software bloquea el proceso y genera una alerta del proceso sospechoso de actividades de malware.

- **Cuarentena**

  El software genera una alerta, detiene el proceso y traslada el archivo ejecutable a la carpeta de cuarentena.

4. En la sección **Modo de análisis**, seleccione la acción que el software deberá realizar al detectar un virus u otra amenaza maliciosa:
   Configuración predeterminada: **En acceso inteligente**
   - **En acceso inteligente**: supervisa todas las actividades del sistema y analiza automáticamente los archivos cuando se accede a ellos para su lectura o escritura, o cuando se inicia un programa.
   - **En ejecución**: escanea de forma automática solo los archivos ejecutables cuando se inician para garantizar que estén limpios y que no causarán ningún daño al equipo o a los datos.
5. Haga clic en **Listo**.

Planificar análisis

El análisis bajo demanda comprueba el sistema de su equipo en busca de virus según la planificación especificada. Un análisis completo comprueba todos los archivos de su equipo, mientras que un análisis rápido solo comprueba los archivos de sistema del equipo.

Pasos para configurar Planificar análisis

Configuración predeterminada:

- **Análisis personalizado** está deshabilitado.
- Se ha programado el escaneado **Rápido** y **Completo**.

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Planificar análisis**.
3. Utilice el conmutador para habilitar el tipo de análisis que quiera aplicar al equipo.

Tipos de análisis disponibles:

- **Completo**: tarda mucho tiempo en terminar en comparación con el análisis rápido porque se comprueban todos los archivos.
- **Rápido**: solo comprueba las zonas habituales en las que suele residir el malware en el equipo.
- **Personalizado**: comprueba los archivos y las carpetas que seleccionó el administrador para el plan Protección.

© Acronis International GmbH, 2003-2025

Nota
Puede planificar los tres análisis, **Rápido**, **Completo** y **Personalizado**, dentro de un único plan de protección.

Pasos para configurar el análisis personalizado

- Utilice el conmutador **Análisis personalizado** para habilitar o deshabilitar este tipo de análisis.
- En la lista desplegable **Acción sobre la detección**, seleccione una de las opciones disponibles:

Configuración predeterminada: **Cuarentena**

Cuarentena

El software genera una alerta y traslada el archivo ejecutable a la carpeta de cuarentena.

Solo notificar

El software genera una alerta del proceso sospechoso de ser malware.

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario inicie sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario cierre sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación. • **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes:

© Acronis International GmbH, 2003-2025

Campo	Descripción
	• **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.
Especifique una cuenta de usuario que al cerrar sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el

© Acronis International GmbH, 2003-2025

Campo	Descripción
	retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo** • **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.

- Selecciona la casilla de verificación **Analizar únicamente archivos nuevos y modificados** si desea analizar solo los archivos que se hayan creado recientemente y los que se hayan modificado.

Configuración predeterminada: **Habilitado**

- Se mostrarán dos opciones adicionales para **Análisis personalizado** únicamente si se selecciona **Análisis completo**:

1. **Analizar archivos del archivo comprimido**

   Configuración predeterminada: **Habilitado**.

   Máxima profundidad de recursión

   Configuración predeterminada: **16**

   Número de niveles de archivos incrustados que se pueden analizar. Por ejemplo, documento MIME > archivo zip > archivo comprimido de Office > contenido del documento.

   Tamaño máx.

   Configuración predeterminada: **100**

   Tamaño máximo de los archivos de un archivo comprimido que se vaya a escanear.

2. **Analizar unidades extraíbles**

Configuración predeterminada: **Deshabilitado**

- **Unidades de red asignadas (remotas)**
- **Dispositivos de almacenamiento USB** (como memorias y discos duros externos)
- **CD/DVD**

© Acronis International GmbH, 2003-2025

Nota
El análisis de unidades extraíbles no es compatible con Linux.

Exclusiones de protección

Las exclusiones de protección le permiten eliminar falsos positivos cuando un programa de confianza se considera ransomware o malware. Puede definir los elementos de confianza y los bloqueados. Para ello, añádalos a la lista de exclusiones de protección.

En la lista de elementos de confianza, puede añadir archivos, procesos y carpetas para que el sistema los considere seguros y evitar que los detecte en el futuro.

En la lista de elementos bloqueados, puede añadir procesos y hash. Esta opción garantiza que se bloquean esos procesos y su carga de trabajo estará a salvo.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Elemento de exclusión de protección	Bloqueado	De confianza
Hash	Cuando se añada un hash a la lista de bloqueados, el sistema detendrá el proceso, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, se bloquea el proceso asociado a dicho hash.	Cuando se añada un hash a la lista de confianza, el sistema sabrá qué procesos debe ignorar mediante la supervisión, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, el proceso asociado a este hash se considera de confianza y se excluye de la supervisión.
Proceso	Cuando se añada un proceso a la lista de bloqueados, el sistema sabrá que debe supervisar esos procesos, y los procesos se bloquearán siempre. Por ejemplo, si añade esta ruta **C:\Users\user1\application\nppInstaller.exe** a la lista de bloqueados, se bloqueará este proceso específico y, cuando intente abrirlo, no podrá iniciarse.	Cuando se añada un proceso a la lista de confianza, el sistema excluirá ese proceso de la supervisión. Por ejemplo, si añade esta ruta: `C:\Users\user1\application\nppInstaller.exe`, este proceso específico se excluirá de la supervisión y el antivirus no interferirá con este proceso. Si añade esta expresión: `C:\Users\user1\application\*.exe`, se excluirán todos los procesos de la carpeta `application`.

© Acronis International GmbH, 2003-2025

Elemento de exclusión de protección	Bloqueado	De confianza
		Nota Los procesos firmados por Microsoft siempre son de confianza.
Archivo/carpeta		Cuando se añada un archivo o una carpeta a la lista de confianza, el sistema sabrá que dichos archivos o carpetas se considerarán siempre seguros y no es necesario analizarlos o supervisarlos.

Pasos para especificar los elementos que siempre serán de confianza

1. Abre el plan de protección para editarlo.
   Por ejemplo, haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones**.
   Se mostrará la ventana **Exclusiones de protección**.
4. En la sección **Elementos de confianza**, haga clic en **Agregar** para seleccionar entre las opciones disponibles:
   - Para añadir archivos, carpetas o procesos a los elementos de confianza, seleccione la opción **Archivo/carpeta/proceso**. Se mostrará la ventana **Añadir archivo/carpeta/proceso**.
     - En el campo **Archivo/proceso/carpeta**, escriba la ruta para cada proceso, carpeta o archivo en una nueva línea.
     - Seleccione la casilla de verificación **Añadir como archivo/carpeta** para añadir el archivo o carpeta a los elementos de confianza.
       Ejemplos de descripciones de carpetas: `D:\folder\`, `/home/Folder/folder2`, `F:\`
     - Seleccione la casilla de verificación **Añadir como proceso** para añadir el proceso a los elementos de confianza. Los procesos seleccionados se excluirán de la supervisión.
       Puede especificar la ruta completa a un proceso o usar un comodín. Por ejemplo, para excluir todos los procesos en la carpeta `Temp`, puede introducir `C:\Windows\Temp\*.exe`.
       También se admiten rutas de red local. Por ejemplo, `\\localhost\folderpath\file.exe`
   - Para añadir los hashes MD5 a la lista de elementos de confianza, seleccione la opción **Hash**. Se abrirá la ventana **Añadir hash**.
     - Aquí puede insertar los hash MD5 en líneas separadas para que se incluyan como de confianza en la lista de exclusiones de protección. En función de estos hash, Cyber Protection excluirá los procesos descritos por los hash MD5 de la supervisión.
5. [Opcional] En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos de confianza. Por ejemplo, motivos y propósitos de

© Acronis International GmbH, 2003-2025

la exclusión, fecha/hora, etc.

Nota
Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

6. Haga clic en **Agregar** y luego en **Listo**.

Pasos para especificar los elementos que siempre se bloquearán

1. Abra el plan de protección.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones de protección**.
   Se mostrará la ventana **Exclusiones de protección**.
4. En la sección **Elementos bloqueados**, haga clic en **Agregar** y seleccione entre las opciones disponibles:
   - Para bloquear procesos, seleccione la opción **Proceso**. Se mostrará la ventana **Añadir proceso**.
     - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea.

     Nota
     Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.

   - Para bloquear un hash, seleccione la opción **Hash**. Se abrirá la ventana **Añadir hash**.
     - En el campo **Hash**, escriba el hash de cada proceso en una nueva línea.
5. [Opcional]
   En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos bloqueados. Por ejemplo, motivos y propósitos de la exclusión, fecha/hora, etc.

   Nota
   Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

6. Haga clic en **Agregar** y luego en **Listo**.

Uso de comodines para definir exclusiones

Para definir exclusiones, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. El signo de pregunta (?) sustituye exactamente cero o un carácter. No pueden usarse variables de entorno, como `%AppData%`.

Puede usar un comodín (*) para añadir elementos a las listas de exclusión.

- Los comodines se pueden usar en medio o al final de la descripción.

Ejemplos de comodines aceptados en descripciones:

© Acronis International GmbH, 2003-2025

C:*.pdf

D:\carpetas\archivo.*

C:\Users*\AppData\Roaming

- No se pueden utilizar caracteres comodín al principio de la descripción.

Ejemplos de comodines que no se aceptan en descripciones:

*.docx

*:\carpeta\

Uso de variables para definir exclusiones

También puede usar variables para añadir elementos a las listas de exclusiones de protección, con las siguientes limitaciones:

- Para Windows, solo se admiten las variables del SISTEMA. No se admiten las variables específicas del usuario, por ejemplo, %USERNAME% o %APPDATA%. No se admiten variables con {username}. Para obtener más información, consulte https://ss64.com/nt/syntax-variables.html.
- Para macOS, no se admiten las variables de entorno.
- Para Linux, no se admiten las variables de entorno.

Ejemplos de formatos compatibles:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Configuración personalizada

En casos específicos, el equipo de soporte puede ayudarle a resolver problemas indicándole que cambie la configuración del plan de protección.

Advertencia.
Utilice **Configuración personalizada** solo según las instrucciones del equipo de soporte. La inclusión de una configuración personalizada incorrecta puede afectar negativamente a su carga de trabajo y el proveedor de servicios no será responsable de ello.

Para configurar la Configuración personalizada

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Configuración personalizada**.
3. En la sección **Configuración personalizada**, haga clic en **Agregar**.

© Acronis International GmbH, 2003-2025

4. En el campo de valor, introduzca la configuración personalizada proporcionada por el equipo de soporte.
5. Configure el interruptor **Verdadero/Falso** según las instrucciones del equipo de soporte.
6. Haga clic en la marca de verificación situada a la derecha para guardar la configuración personalizada.
7. En el cuadro de diálogo **Agregar ajuste personalizado**, haga clic en **Agregar**.
8. Haga clic en **Listo**.

El ajuste personalizado se aplica ahora al plan de protección.

Aplicación potencialmente no deseada

Las aplicaciones no deseadas son aplicaciones que puede que haya instalado en sus cargas de trabajo sin querer. Puede configurar las acciones que el sistema realizará cuando detecte aplicaciones potencialmente no deseadas. De esta forma, puede proteger sus cargas de trabajo de software que puede reducir su rendimiento, evitar la visualización de anuncios no deseados y rastrear el uso de Internet con la intención de vender datos a terceros.

Configuración predeterminada: **Habilitado**.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Para configurar acciones contra aplicaciones potencialmente no deseadas

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Aplicación potencialmente no deseada**.
3. En la lista desplegable **Acción sobre la detección**, seleccione una de las siguientes opciones:

   Configuración predeterminada: **Bloquear y notificar**

   - **Solo notificar**
   - **Bloquear y notificar**
   - **Cuarentena**
4. Haga clic en **Listo**.

Active Protection en la edición Cyber Backup Standard

En las edición de Cyber Backup Standard, Active Protection es un módulo independiente del plan de protección. Por lo tanto, se puede configurar de forma independiente y aplicar a distintos dispositivos o grupos de dispositivos.

© Acronis International GmbH, 2003-2025

Para todas las demás ediciones del servicio de ciberprotección, Active Protection es parte del módulo **Antivirus y antimalware** del plan de protección.

Configuración predeterminada: **Habilitado**.

Nota
Debe instalarse un agente de protección en el equipo protegido. Para obtener más información sobre los sistemas operativos y las funciones compatibles, consulte "Sistemas operativos compatibles para la protección antivirus y antimalware" (p. 1160).

Cómo funciona

Active Protection controla los procesos que se ejecutan en el equipo protegido. Si el proceso de un tercero intenta cifrar algún archivo o minar criptomonedas, Active Protection genera una alerta y lleva a cabo otras acciones, según se especifica en el plan de protección.

Además, Active Protection evita los cambios no autorizados en los procesos propios del software de copia de seguridad, los archivos de registro, los archivos ejecutables y de configuración y las copias de seguridad que se encuentran en las carpetas locales.

Para identificar los procesos maliciosos, Active Protection utiliza la heurística basada en el comportamiento. Active Protection compara la cadena de acciones realizadas por un proceso con las cadenas de eventos registradas en la base de datos de patrones de conducta maliciosos. Este enfoque permite a Active Protection detectar malware nuevo identificando su comportamiento típico.

Configuración de Active Protection en Cyber Backup Standard

En la edición Cyber Backup Standard, podrá configurar las siguientes funciones de Active Protection:

- Acción sobre la detección
- Autoprotección
- Protección de carpetas de red
- Protección del servidor
- Detección del proceso de criptominería
- Exclusiones

Nota
Active Protection para Linux es compatible con las opciones de configuración siguientes: Acción sobre la detección, protección de carpetas de red y exclusiones. La protección de carpetas de red siempre está activa y no es configurable.

Acción sobre la detección

En la sección **Acción sobre la detección**, seleccione una de las opciones disponibles:

© Acronis International GmbH, 2003-2025

- **Solo notificar**
  El software generará una alerta sobre el proceso sospechoso de actividad de ransomware.
- **Detener el proceso**
  El software generará una alerta y detendrá el proceso sospechoso de actividad de ransomware.
- **Revertir usando la caché**
  El software generará una alerta, detendrá el proceso y revertirá los cambios de los archivos usando la caché de servicios.

Configuración predeterminada: **Revertir usando la caché**.

Autoprotección

La autoprotección evita los cambios no autorizados en los procesos propios del software, los archivos de registro, los archivos ejecutables y de configuración, y las copias de seguridad que se encuentran en las carpetas locales.

Los administradores pueden habilitar **Autoprotección**, sin habilitar **Active Protection**.

Configuración predeterminada: **Activado**.

Nota
La autoprotección no es compatible con Linux.

Pasos para habilitar la autoprotección

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Autoprotección**.
3. Utilice el conmutador **Autoprotección** para habilitarla.

Protección de desinstalación del agente

La configuración **Protección contra la desinstalación del agente** impide que los usuarios o el software desinstalen Agent for Windows o modifiquen sus componentes fuera de la ventana de mantenimiento configurada.

Configuración predeterminada: **Habilitado**

Pasos para deshabilitar la Protección de desinstalación del agente

Advertencia.
Si deshabilita la **Protección de desinstalación del agente** pone en riesgo la seguridad de los recursos informáticos protegidos.

1. Una vez que la función de **Autoprotección** está habilitada, puede seleccionar la casilla de verificación **Protección de desinstalación del agente**.
2. Haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Nota
Esta opción no impide las actualizaciones automáticas del agente de Cyber Protection.

Cada intento de desinstalar o modificar el agente de protección fuera de la ventana de mantenimiento activa una alerta.

Un usuario administrador puede revisar la alerta y decidir si permite modificaciones al agente durante 1 hora o configurar una ventana de mantenimiento con una duración entre 1 hora y 7 días. Consulte "Pasos para permitir la modificación de un agente con la protección de desinstalación habilitada" (p. 213).

Permitir que procesos específicos modifiquen las copias de seguridad

La configuración **Permitir que procesos específicos modifiquen las copias de seguridad** solo está disponible si está habilitada la configuración **Autoprotección**.

Se aplica a archivos en carpetas locales con las siguientes extensiones:

- .tibx
- .tib
- .tia

La configuración **Permitir que procesos específicos modifiquen las copias de seguridad** le permite especificar los procesos que pueden modificar los archivos de copia de seguridad, aunque estos estén protegidos por autoprotección. Esto resulta útil, por ejemplo, si elimina archivos de copia de seguridad o los mueve a una ubicación diferente mediante un script.

Cuando esta configuración está desactivada, los archivos de copia de seguridad solo pueden ser modificados por procesos firmados por el proveedor del software de copia de seguridad. Esto permite al software aplicar reglas de retención y eliminar copias de seguridad cuando un usuario lo solicita desde la interfaz web. Otros procesos, independientemente de que sean sospechosos o no, no pueden modificar las copias de seguridad.

Cuando esta configuración está habilitada, puede permitir que otros procesos modifiquen las copias de seguridad.

Configuración predeterminada: **Deshabilitado**.

Para habilitar Permitir que procesos específicos modifiquen las copias de seguridad

1. Cuando la función **Autoprotección** está habilitada, seleccione la casilla de verificación **Permitir que procesos específicos modifiquen las copias de seguridad**.
2. En el campo **Proceso para modificar copias de seguridad**, haga clic en **Agregar**.
3. Introduzca la ruta completa al archivo ejecutable del proceso, comenzando por la letra de la unidad.
4. Haga clic en la marca de verificación situada a la derecha para guardar el proceso.

© Acronis International GmbH, 2003-2025

Protección de carpetas de red

La configuración **Proteger carpetas de red asignadas como dispositivos locales** define si Active Protection protege las carpetas de la red que están asignadas como dispositivos locales de los procesos maliciosos locales.

Esta configuración se aplica a carpetas compartidas por protocolos SMB o NFS.

Si un archivo se encontraba al principio en un dispositivo asignado, no se puede guardar en la ubicación original cuando se extraiga de la caché mediante la acción **Revertir usando la caché**. En su lugar, se guardará en la carpeta especificada en esta configuración. La carpeta predeterminada es `C:\ProgramData\Acronis\Restored Network Files` para Windows y `Library/Application Support/Acronis/Restored Network Files/` para macOS. Si esta carpeta no existe, se creará. Si quiere cambiar la ruta, especifique una carpeta local. No se admiten carpetas de red, ni siquiera las de dispositivos asignados.

Configuración predeterminada: **Activado**.

Protección del servidor

Esta función define si Active Protection protege las carpetas de la red que comparte de conexiones entrantes externas de otros servidores de la red que puedan suponer una amenaza.

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Configuración predeterminada: **Apagado**.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Nota
La protección del servidor no es compatible con Linux.

Pasos para establecer conexiones de confianza

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **De confianza**.
5. En el campo **Conexiones de confianza**, haga clic en **Agregar** para definir las conexiones que podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.

© Acronis International GmbH, 2003-2025

7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Haga clic en la marca de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Pasos para establecer conexiones bloqueadas

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Protección del servidor**.
3. Utilice el conmutador **Protección del servidor** para habilitarla.
4. Seleccione la pestaña **Bloqueadas**.
5. En el campo **Conexiones bloqueadas**, haga clic en **Agregar** para definir las conexiones que no podrán modificar datos.
6. En el campo **Nombre del equipo/Cuenta**, escriba el nombre del ordenador y la cuenta del equipo donde está instalado el agente de protección. Por ejemplo, `MyComputer\TestUser`.
7. En el campo **Nombre del servidor**, escriba el nombre del servidor del equipo que tiene permitido conectarse a este con el agente de protección.
8. Seleccione la casilla de verificación de la derecha para guardar la definición de la conexión.
9. Haga clic en **Listo**.

Detección de Cryptomining

El malware de criptominería afecta al rendimiento de aplicaciones de utilidad, aumenta el importe de las facturas de electricidad, puede hacer que el sistema se bloquee e, incluso, dañar el hardware debido a su explotación. La función **Detección del proceso de criptominería** protege los dispositivos del malware de criptominería para impedir el uso no autorizado de los recursos del equipo.

Los administradores pueden habilitar **Detección del proceso de criptominería**, sin habilitar **Active Protection**. Configuración predeterminada: **Habilitado**.

Importante
La disponibilidad de esta característica depende de la licencia que tenga.

Nota
La detección del proceso de criptominería no es compatible con Linux.

Para configurar la detección del proceso de criptominería

1. En la ventana **Crear plan de protección**, amplíe el módulo **Protección antivirus y antimalware**.
2. Haga clic en **Detección del proceso de criptominería**.

© Acronis International GmbH, 2003-2025

3. Utilice el conmutador **Detectar procesos de criptominería** para habilitar o deshabilitar la función.
4. Seleccione qué se debe hacer con los procesos sospechosos de actividad de criptominería:

   Configuración predeterminada: **Detener el proceso**

   - **Solo notificar**: el software genera una alerta.
   - **Detener el proceso**: el software genera una alerta y detiene el proceso.
5. Haga clic en **Listo** para aplicar las opciones seleccionadas a su plan de protección.

Exclusiones

Las exclusiones de protección le permiten eliminar falsos positivos cuando un programa de confianza se considera ransomware o malware. Puede definir los elementos de confianza y los bloqueados. Para ello, añádalos a la lista de exclusiones de protección.

En la lista de elementos de confianza, puede añadir archivos, procesos y carpetas para que el sistema los considere seguros y evitar que los detecte en el futuro.

En la lista de elementos bloqueados, puede añadir procesos y hash. Esta opción garantiza que se bloquean esos procesos y su carga de trabajo estará a salvo.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Elemento de exclusión de protección	Bloqueado	De confianza
Hash	Cuando se añada un hash a la lista de bloqueados, el sistema detendrá el proceso, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, se bloquea el proceso asociado a dicho hash.	Cuando se añada un hash a la lista de confianza, el sistema sabrá qué procesos debe ignorar mediante la supervisión, según el hash proporcionado. Por ejemplo, cuando añade este hash MD5, 938c2cc0dcc05f2b68c4287040cfcf71, el proceso asociado a este hash se considera de confianza y se excluye de la supervisión.
Proceso	Cuando se añada un proceso a la lista de bloqueados, el sistema sabrá que debe supervisar esos procesos, y los procesos se bloquearán siempre. Por ejemplo, si añade esta ruta **C:\Users\user1\application\nppInstaller.exe** a la lista de bloqueados, se bloqueará este proceso específico y,	Cuando se añada un proceso a la lista de confianza, el sistema excluirá ese proceso de la supervisión. Por ejemplo, si añade esta ruta: `C:\Users\user1\application\nppInstaller.exe`, este proceso específico se excluirá de la supervisión y el antivirus no interferirá con este

© Acronis International GmbH, 2003-2025

Elemento de exclusión de protección	Bloqueado	De confianza
	cuando intente abrirlo, no podrá iniciarse.	proceso. Si añade esta expresión: `C:\Users\user1\application\*.exe`, se excluirán todos los procesos de la carpeta `application`. **Nota** Los procesos firmados por Microsoft siempre son de confianza.
Archivo/carpeta		Cuando se añada un archivo o una carpeta a la lista de confianza, el sistema sabrá que dichos archivos o carpetas se considerarán siempre seguros y no es necesario analizarlos o supervisarlos.

Pasos para especificar los elementos que siempre serán de confianza

1. Abre el plan de protección para editarlo.
   Por ejemplo, haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del plan de protección y seleccione **Editar**.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones**.
   Se mostrará la ventana **Exclusiones de protección**.
4. En la sección **Elementos de confianza**, haga clic en **Agregar** para seleccionar entre las opciones disponibles:
   - Para añadir archivos, carpetas o procesos a los elementos de confianza, seleccione la opción **Archivo/carpeta/proceso**. Se mostrará la ventana **Añadir archivo/carpeta/proceso**.
     - En el campo **Archivo/proceso/carpeta**, escriba la ruta para cada proceso, carpeta o archivo en una nueva línea.
     - Seleccione la casilla de verificación **Añadir como archivo/carpeta** para añadir el archivo o carpeta a los elementos de confianza.
       Ejemplos de descripciones de carpetas: `D:\folder\`, `/home/Folder/folder2`, `F:\`
     - Seleccione la casilla de verificación **Añadir como proceso** para añadir el proceso a los elementos de confianza. Los procesos seleccionados se excluirán de la supervisión.
       Puede especificar la ruta completa a un proceso o usar un comodín. Por ejemplo, para excluir todos los procesos en la carpeta `Temp`, puede introducir `C:\Windows\Temp\*.exe`.
       También se admiten rutas de red local. Por ejemplo, `\\localhost\folderpath\file.exe`
   - Para añadir los hashes MD5 a la lista de elementos de confianza, seleccione la opción **Hash**. Se abrirá la ventana **Añadir hash**.

© Acronis International GmbH, 2003-2025

- Aquí puede insertar los hash MD5 en líneas separadas para que se incluyan como de confianza en la lista de exclusiones de protección. En función de estos hash, Cyber Protection excluirá los procesos descritos por los hash MD5 de la supervisión.

5. [Opcional] En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos de confianza. Por ejemplo, motivos y propósitos de la exclusión, fecha/hora, etc.

   Nota
   Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

6. Haga clic en **Agregar** y luego en **Listo**.

Pasos para especificar los elementos que siempre se bloquearán

1. Abra el plan de protección.
2. Expanda el módulo **Protección antivirus y antimalware**.
3. Seleccione la opción **Exclusiones de protección**.
   Se mostrará la ventana **Exclusiones de protección**.
4. En la sección **Elementos bloqueados**, haga clic en **Agregar** y seleccione entre las opciones disponibles:
   - Para bloquear procesos, seleccione la opción **Proceso**. Se mostrará la ventana **Añadir proceso**.
     - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea.

     Nota
     Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.

   - Para bloquear un hash, seleccione la opción **Hash**. Se abrirá la ventana **Añadir hash**.
     - En el campo **Hash**, escriba el hash de cada proceso en una nueva línea.
5. [Opcional]
   En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos bloqueados. Por ejemplo, motivos y propósitos de la exclusión, fecha/hora, etc.

   Nota
   Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

6. Haga clic en **Agregar** y luego en **Listo**.

Uso de comodines para definir exclusiones

Para definir exclusiones, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. El signo de pregunta (?) sustituye exactamente cero o un carácter. No pueden

© Acronis International GmbH, 2003-2025

usarse variables de entorno, como `%AppData%`.

Puede usar un comodín (*) para añadir elementos a las listas de exclusión.

- Los comodines se pueden usar en medio o al final de la descripción.

Ejemplos de comodines aceptados en descripciones:

C:*.pdf

D:\carpetas\archivo.*

C:\Users*\AppData\Roaming

- No se pueden utilizar caracteres comodín al principio de la descripción.

Ejemplos de comodines que no se aceptan en descripciones:

*.docx

*:\carpeta\

Uso de variables para definir exclusiones

También puede usar variables para añadir elementos a las listas de exclusiones de protección, con las siguientes limitaciones:

- Para Windows, solo se admiten las variables del SISTEMA. No se admiten las variables específicas del usuario, por ejemplo, %USERNAME% o %APPDATA%. No se admiten variables con {username}. Para obtener más información, consulte https://ss64.com/nt/syntax-variables.html.
- Para macOS, no se admiten las variables de entorno.
- Para Linux, no se admiten las variables de entorno.

Ejemplos de formatos compatibles:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Filtrado de URL

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El malware lo suelen distribuir sitios infectados o maliciosos mediante el método de infección conocido como Drive-by download.

© Acronis International GmbH, 2003-2025

La funcionalidad Filtrado de URL que le permite proteger los equipos de amenazas como el malware o suplantación de identidad que procedan Internet. Puede proteger su organización si bloquea el acceso del usuario a los sitios web en los que pueda haber contenido malicioso.

El filtrado de URL también puede controlar el uso de los sitios web para que cumplan con las regulaciones externas y las directivas internas de la empresa. Puede configurar el acceso a los sitios web en función de su categoría relacionada. En estos momentos, el filtrado de URL admite 44 categorías de sitio web y permite gestionar el acceso a ellas.

Actualmente las conexiones HTTP/HTTPS de los equipos Windows las comprueba el agente de protección.

La característica Filtrado de URL necesita conectarse a Internet para funcionar.

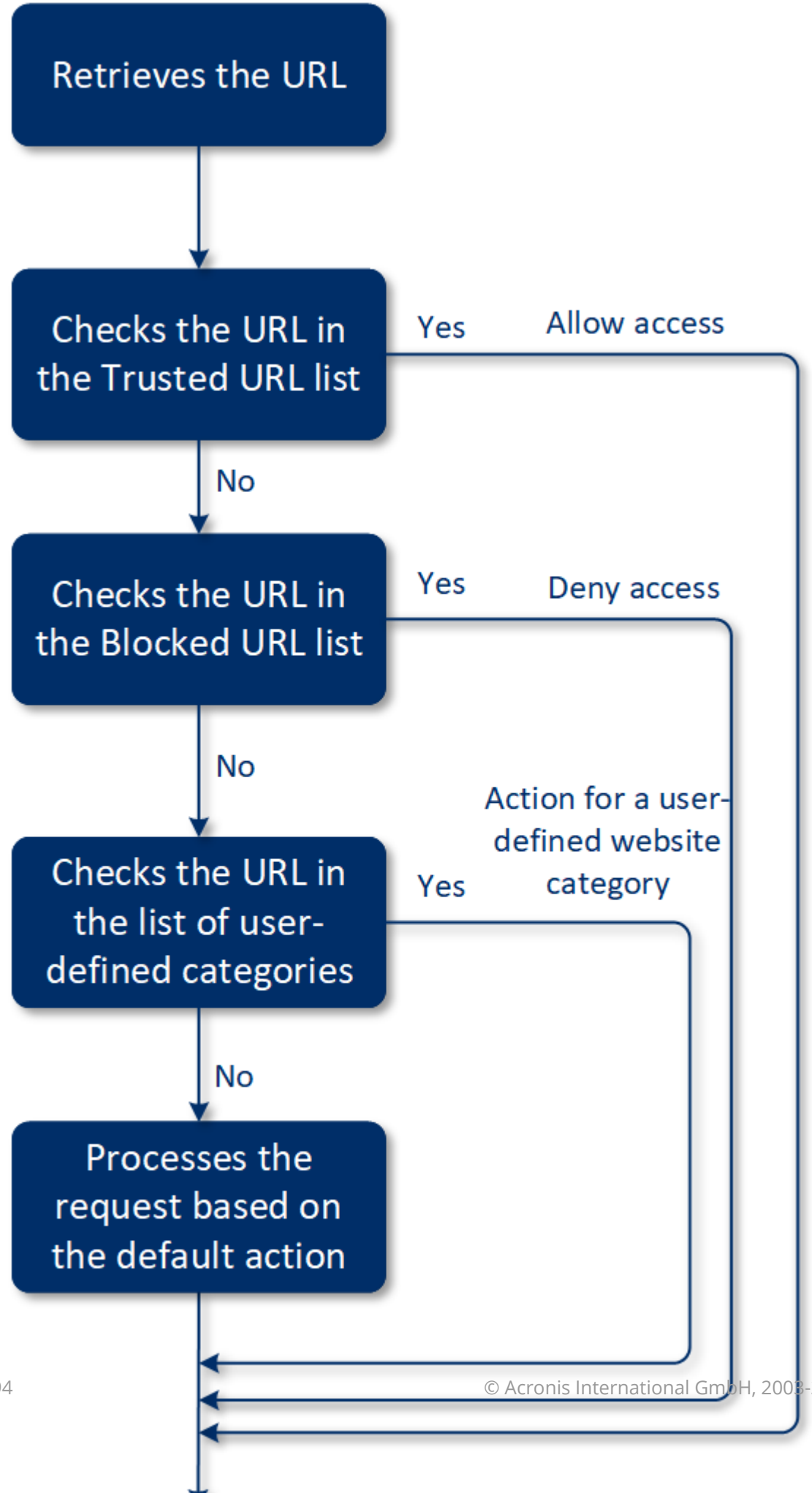
Nota
Para evitar posibles problemas de compatibilidad con compilaciones 15.0.26692 (lanzamiento C21.03 HF1) de agentes de protección y anteriores, la función del filtrado de URL se deshabilitará de forma automática si se detecta otra solución antivirus o si el servicio del Centro de seguridad de Windows no está presente en el sistema.
Para agentes de protección posteriores, los problemas de compatibilidad se resuelven para que el filtrado de URL esté siempre habilitado según la directiva.

Cómo funciona

Cuando se habilita el filtrado de URL, filtra todo el tráfico de red que entra en el equipo, incluyendo la actividad del navegador y cualquier otra actividad de red que se produzca en segundo plano.

Por ejemplo, cuando un usuario introduce una URL en un navegador, el interceptor obtiene el enlace y lo envía al agente de protección. El agente obtiene la URL, la analiza y comprueba el veredicto. El interceptor redirige al usuario a la página con el mensaje con distintas acciones para que continúe manualmente a la página solicitada.

© Acronis International GmbH, 2003-2025



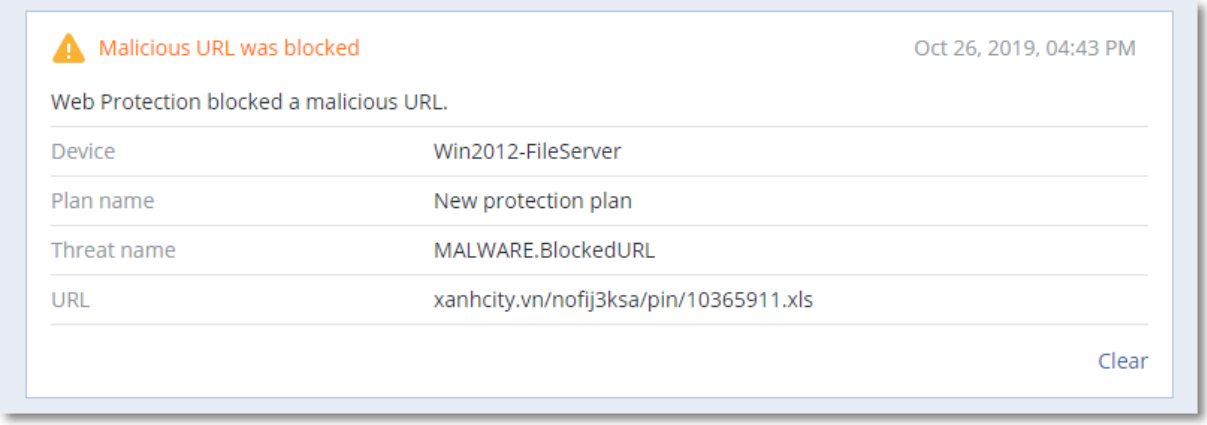
© Acronis International GmbH, 2003-2025

Flujo de trabajo de la configuración del filtrado de URL

Normalmente, la configuración del filtrado de URL está formada por los siguientes pasos:

1. Cree un plan de protección con el módulo **Filtrado de URL** habilitado.
2. Especifique los ajustes del filtrado de URL (consulte la información que aparece a continuación).
3. Asigne el plan de protección a los equipos.

Para comprobar qué direcciones URL se han bloqueado, vaya a **Supervisión** > **Alertas**.



Ajustes del filtrado de URL

Para el módulo de filtrado de URL se pueden establecer los siguientes ajustes:

Acceso a sitio web malicioso

Especifique qué acción se llevará a cabo cuando un usuario abra un sitio web malicioso:

- **Solo notificar**: el software genera una alerta sobre el proceso sospechoso de actividad de ransomware.
- **Bloquear**: bloquear el acceso al sitio web malicioso. El usuario no podrá acceder al sitio web y se generará una alerta advertencia.
- **Preguntar siempre al usuario**: preguntar al usuario si quiere continuar y acceder al sitio web o volver atrás.

Categorías que se pueden filtrar

Hay 44 categorías de sitio web cuyo acceso puede configurar:

- **Permitir**: permite el acceso a los sitios web relacionados con la categoría seleccionada.
- **Rechazar**: deniega el acceso a los sitios web relacionados con la categoría seleccionada.

De manera predeterminada, todas las categorías están permitidas.

© Acronis International GmbH, 2003-2025

Mostrar notificaciones de URL bloqueadas en la carga de trabajo protegida: si está habilitado, se mostrarán notificaciones de URL bloqueadas por categorías en el área de notificación. Si un sitio web tiene varios subdominios, el sistema genera notificaciones para ellos también, por lo que el número de notificaciones en el área de notificación puede ser elevado.

Nota
Algunas categorías bloqueadas pueden generar múltiples notificaciones

En la tabla siguiente puede encontrar la descripción de las categorías:

	Categoría del sitio web	Descripción
1	**Publicidad**	En esta categoría se incluyen aquellos dominios cuyo objetivo principal es ofrecer anuncios.
2	**Tableros de mensajes**	En esta categoría se incluyen los foros, los grupos de discusión y los sitios web de pregunta-respuesta. Esta categoría no cubre las secciones específicas de los sitios web empresariales donde los clientes hacen preguntas.
3	**Sitios web personales**	En esta categoría se incluyen los sitios web personales y todos los tipos de blogs: individuales, de varias personas e incluso de empresas. Un blog es un diario publicado en la World Wide Web. Consta de entradas (“publicaciones”) que normalmente se muestran en orden cronológico inverso, de modo que las más recientes aparecen primero.
4	**Sitios web empresariales/corporativos**	Esta categoría es amplia porque abarca los sitios web corporativos que no suelen pertenecer a ninguna otra categoría.
5	**Software**	En esta categoría se incluyen aquellos sitios web en los que se ofrece software, normalmente de código abierto, gratuito o shareware. También puede cubrir algunas tiendas de software en línea.
6	**Medicamentos**	En esta categoría se incluyen los sitios web relacionados con los medicamentos, el alcohol o los cigarros en los que se habla del uso o la venta de medicamentos (legales) o parafernalia médica, alcohol o productos con tabaco. Tenga en cuenta que las drogas ilegales quedan cubiertas en la categoría Drogas.
7	**Formación**	En esta categoría se incluyen aquellos sitios web que pertenecen a instituciones educativas oficiales, incluidos aquellos que no pertenecen al dominio .edu. También incluye los sitios web educativos, como las enciclopedias.
8	**Entretenimiento**	En esta categoría se incluyen aquellos sitios web que proporcionan información relacionada con actividades artísticas

© Acronis International GmbH, 2003-2025

		y museos, además de sitios web en los que se analiza o puntúa contenido como películas, música o arte.
9	**Uso compartido de archivos**	Esta categoría cubre los sitios web de compartición de archivos, donde un usuario puede cargar archivos y compartirlos con otros. También cubre los sitios web para compartir torrents, así como los rastreadores de torrents.
10	**Finanzas**	Esta categoría incluye todos los sitios web propiedad de bancos que proporcionan acceso en línea. También cubre algunas unidades de crédito y otras instituciones financieras. Sin embargo, las entidades bancarias locales podrían no estar cubiertas.
11	**Apuestas**	En esta categoría se incluyen los sitios web de apuestas. Son los del tipo "casino en línea " o "lotería en línea", que normalmente requieren un pago anticipado para que el usuario pueda apostar dinero en juegos de azar en línea como la ruleta, el póquer, el blackjack, etcétera. Algunos son legítimos, lo que significa que existe una posibilidad de ganar: otros son fraudulentos y no existe dicha posibilidad. También detecta los sitios web de "consejos y trucos para apostar", donde se describen modos de ganar dinero con los sitios web de juegos de azar y loterías en línea.
12	**Juegos**	En esta categoría se incluyen los sitios web que ofrecen juegos en línea, normalmente basados en applets Adobe Flash o Java. Para la detección, no importa si el juego es gratuito o si requiere una suscripción, pero los sitios web de estilo casino se integran en la categoría Apuestas. Esta categoría no cubre lo siguiente: • Sitios web oficiales de empresas que desarrollan videojuegos (salvo que produzcan juegos en línea) • Sitios web donde se conversa sobre juegos • Sitios web donde se pueden descargar juegos que no son en línea (algunos de los cuales se cubren en la categoría Ilegal) • Juegos que requieren que el usuario descargue y ejecute un archivo ejecutable, como World of Warcraft; es posible prevenirlos de distintas formas, como un cortafuegos
13	**Gobierno**	En esta categoría se incluyen los sitios web del Gobierno, incluidas las instituciones oficiales, las embajadas y los ministerios.
14	**Hackeo**	En esta categoría se incluyen los sitios web que proporcionan herramientas de hackeo, artículos y plataformas de discusión para los hackers. También cubre los sitios web que ofrecen "exploits" para plataformas comunes que facilitan el hackeo de

© Acronis International GmbH, 2003-2025

		cuentas de Facebook o Gmail.
15	**Actividades ilegales**	Esta categoría es amplia e incluye todo lo relacionado con el odio, la violencia y el racismo, y está pensada para bloquear las siguientes categorías de sitio web: • Sitios web pertenecientes a organizaciones terroristas • Sitios web con contenido racista o xenófobo • Sitios web donde se habla de deportes violentos, o que promueven la violencia
16	**Salud y bienestar**	En esta categoría se incluyen aquellos sitios web que están asociados a instituciones médicas, sitios web relacionados con la prevención de enfermedades y su tratamiento, y sitios web que ofrecen información o productos para perder peso, dietas, esteroides, anabolizantes y productos para estimular la hormona del crecimiento, así como aquellos sitios web que proporcionan información sobre cirugía plástica.
17	**Aficiones**	En esta categoría se incluyen aquellos sitios web que ofrecen recursos sobre actividades normalmente de ocio, como el coleccionismo, las manualidades y el ciclismo.
18	**Alojamiento web**	En esta categoría se incluyen los sitios web gratuitos y comerciales que alojan servicios con los que los usuarios y las organizaciones privadas pueden crear únicas páginas web.
19	**Descargas ilegales**	En esta categoría se incluyen los sitios web relacionados con la piratería de software, como los siguientes: • Sitios web de rastreadores P2P (BitTorrent, emule, DC++) conocidos por ayudar a distribuir contenido con derechos de autor sin el consentimiento de los poseedores de estos derechos • Sitios web y tableros de discusión de warez (software comercial pirateado) • Sitios web que proporcionan a los usuarios cracks, generadores de claves y números de serie para facilitar el uso ilegal del software Algunos de estos sitios web también pueden detectarse como pornografía o alcohol/tabaco, ya que a menudo utilizan publicidad de esta clase para obtener ingresos.
20	**Mensajería instantánea**	En esta categoría se incluyen los sitios web para chatear y de mensajería instantánea con los que los usuarios pueden hablar en tiempo real. También detecta yahoo.com y gmail.com, pues ambos contienen un servicio integrado de mensajería instantánea.

© Acronis International GmbH, 2003-2025

21	**Empleo**	En esta categoría se incluyen los sitios web que ofrecen bolsas de empleo, anuncios clasificados relacionados con el empleo y oportunidades de trabajo, además de agregadores de esos servicios. No cubre las agencias de reclutamiento ni las páginas de "empleos" en los sitios web oficiales de las empresas.
22	**Contenido para adultos**	En esta categoría se incluye el contenido que el creador de un sitio web ha etiquetado como dirigido a un público adulto. Cubre una amplia gama de sitios web, desde el libro Kama Sutra y las páginas de educación sexual hasta la pornografía más explícita.
23	**Drogas**	En esta categoría se incluyen los sitios web en los que se comparte información sobre drogas ilegales y recreativas. Esta categoría también cubre los sitios web sobre el desarrollo y cultivo de drogas.
24	**Noticias**	En esta categoría se incluyen los sitios web que ofrecen noticias en vídeo y texto. Intenta cubrir los sitios web de noticias tanto globales como locales, aunque algunos sitios web locales de pequeño tamaño pueden no quedar incluidos.
25	**Citas en línea**	En esta categoría se incluyen los sitios web de citas en línea, de pago y gratuitos, en los que los usuarios pueden buscar a otras personas según ciertos criterios. También pueden publicar sus perfiles para permitir que otras personas los busquen. Este categoría incluye los sitios web de citas tanto de pago como gratuitos. Como la mayoría de las redes sociales populares pueden utilizarse como sitios de citas en línea, determinados sitios populares, como Facebook, también se detectan dentro de esta categoría. Le recomendamos que utilice esta categoría con la categoría Redes sociales.
26	**Pagos en línea**	En esta categoría se incluyen los sitios web que ofrecen pagos o transferencias de dinero en línea. Detecta sitios web de pago populares como PayPal o Moneybookers. También detecta de forma heurística las páginas web que, en sitios de otra naturaleza, solicitan información de tarjetas de crédito, lo que permite detectar tiendas en línea ocultas, desconocidas o ilegales.
27	**Uso compartido de fotos**	En esta categoría se incluyen los sitios web para compartir fotos cuyo objetivo principal es que los usuarios suban y compartan imágenes.
28	**Tiendas en línea**	En esta categoría se incluyen las tiendas en línea conocidas. Un sitio web se considera una tienda en línea si vende en línea bienes o servicios.

© Acronis International GmbH, 2003-2025

29	**Pornografía**	En esta categoría se incluyen los sitios web en los que hay contenido erótico y pornografía. Incluye tanto los sitios gratuitos como los de pago. Cubre los sitios web que ofrecen imágenes, historias y vídeos, y también detecta contenido pornográfico en sitios web con contenidos mixtos.
30	**Portales**	En esta categoría se incluyen los sitios web que reúnen información de varios recursos y dominios, y que normalmente ofrecen funciones como motores de búsqueda, correo electrónico, noticias e información sobre entretenimiento.
31	**Radio**	En esta categoría se incluyen los sitios web que ofrecen servicios de reproducción de música en Internet, desde emisoras de radio en línea hasta sitios web que proporcionan contenido de audio bajo demanda, ya sea de pago o gratuito.
32	**Religión**	En esta categoría se incluyen los sitios web que promueven la religión o las sectas religiosas. También cubre los foros de discusión relacionados con una o más religiones.
33	**Motores de búsqueda**	En esta categoría se incluyen los sitios web de motores de búsqueda, como Google, Yahoo y Bing.
34	**Redes sociales**	En esta categoría se incluyen los sitios web de redes sociales, como MySpace.com, Facebook.com, Bebo.com, etc. Sin embargo, las redes sociales especializadas, como YouTube.com, se encuadran en la categoría Vídeo/Foto.
35	**Deportes**	En esta categoría se incluyen los sitios web que ofrecen información, noticias y tutoriales deportivos.
36	**Suicidio**	En esta categoría se incluyen los sitios web que promueven, ofrecen o defienden el suicidio. No cubre las clínicas de prevención del suicidio.
37	**Prensa amarilla**	Esta categoría se ha diseñado principalmente para los sitios web de porno suave y cotilleo sobre famosos. Muchos sitios web de noticias sensacionalistas pueden tener subcategorías aquí integradas. La detección de esta categoría también se basa en un mecanismo heurístico.
38	**Pérdida de tiempo**	En esta categoría se incluyen aquellos sitios web en los que las personas suelen pasar mucho tiempo. Pueden incluirse sitios web de otras categorías, como las redes sociales o el entretenimiento.
39	**Viajes**	En esta categoría se incluyen aquellos sitios web que ofrecen ofertas de viajes y equipamiento para viajar, además de reseñas y puntuaciones sobre destinos de viajes.
40	**Vídeos**	En esta categoría se incluyen aquellos sitios web en los que se

© Acronis International GmbH, 2003-2025

		alojan vídeos o fotos, ya sean subidos por los usuarios u ofrecidos por distintos proveedores de contenidos. Se incluyen sitios web como YouTube, Metacafe o Google Video, y sitios de fotos como Picasa o Flickr. También detecta vídeos incrustados en otros sitios web o blogs.
41	**Dibujos animados violentos**	En esta categoría se incluyen aquellos sitios web en los que se habla, se comparten y se proporcionan dibujos animados violentos o manga que pueden ser inapropiados para menores por su violencia, lenguaje explícito o contenido sexual. Esta categoría no cubre los sitios web que ofrecen dibujos animados generalistas como "Tom y Jerry".
42	**Armas**	En esta categoría se incluyen los sitios web de venta, intercambio, fabricación o uso de armas. También cubre los recursos de caza y el uso de armas BB y de aire comprimido, así como las armas cuerpo a cuerpo.
43	**Correo electrónico**	En esta categoría se incluyen aquellos sitios web que proporcionan funcionalidades de correo electrónico en forma de aplicación web.
44	**Proxy web**	En esta categoría se incluyen aquellos sitios web que ofrecen servicios de proxy web. Se trata de sitios web del tipo “navegador dentro de un navegador” en los que el usuario abre una página web, introduce la URL solicitada en un formulario y hace clic en “Enviar”. A continuación, el sitio de proxy web descarga la página y la muestra dentro del navegador del usuario. Estas son las razones por las que se detectan estos sitios (y por las que podría ser necesario bloquearlos): • Para navegar de forma anónima. Como las solicitudes al servidor web de destino se realizan desde el servidor web del proxy, solo la dirección IP de dicho servidor es visible. Si el administrador del servidor de destino rastrea al usuario, el rastro termina en el proxy web, que puede o no mantener registros que permitan localizar al usuario original. • Para falsificar la ubicación. La dirección IP de los usuarios se utiliza a menudo para segmentar los servicios según la ubicación de origen (algunos sitios gubernamentales solo están disponibles desde direcciones IP locales); el uso de estos servicios puede ayudar al usuario a camuflar su auténtica ubicación. • Para acceder a contenido prohibido. Si se utiliza un simple filtro de URL, solo se verán las URL del proxy web y no los servidores reales que el usuario visita.

© Acronis International GmbH, 2003-2025

		• Para evitar la supervisión de las empresas. Una directiva de empresa puede requerir que se supervise el uso que los empleados hacen de Internet. Como se accede a todo el contenido a través de un proxy web, un usuario podría evadir esta supervisión, que no obtendrá información correcta. Como el SDK analiza la página HTML (si se proporciona) y no solo las URL, en algunas categorías, el SDK podrá seguir detectando el contenido. Sin embargo, con el simple uso del SDK no pueden evitarse algunas de las razones.

Exclusiones de URL

Las direcciones URL que se sabe que son seguras se pueden añadir a la lista de dominios de confianza. Las direcciones URL que suponen una amenaza se pueden añadir a la lista de dominios bloqueadas.

Cómo especificar las URL que siempre serán de confianza

1. En la sección de filtrado de URL de un plan de protección, haga clic en **Exclusiones**.
   Se mostrará la ventana **Exclusiones de URL**.
2. En la sección **Elementos de confianza**, haga clic en **Agregar** y luego seleccione entre las opciones disponibles.
   - **Dominio**: si selecciona esta opción, se abrirá la ventana **Añadir dominio**.
     - En el campo **Dominio**, escriba cada dominio en una nueva línea.
   - **Proceso**: si selecciona esta opción, se mostrará la ventana **Añadir proceso**.
     - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea.
3. [Opcional] En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos de confianza. Por ejemplo, motivos y propósitos de la exclusión, fecha/hora, etc.

   Nota
   Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

4. Haga clic en **Agregar** y luego en **Listo**.

Cómo especificar las URL que siempre se bloquearán

1. En la sección de filtrado de URL de un plan de protección, haga clic en **Exclusiones**.
   Se mostrará la ventana **Exclusiones de URL**.
2. En la sección **Elementos bloqueados**, haga clic en **Agregar** y luego en **Dominio**.
3. En el campo **Dominio**, inserte cada dominio en una nueva línea.

   Nota
   Se admiten rutas de red local. Por ejemplo, `\\localhost\folderpath\file.exe`.

© Acronis International GmbH, 2003-2025

4. [Opcional] En el campo **Descripción**, introduzca una breve descripción para que pueda reconocer su cambio en la lista de elementos bloqueados. Por ejemplo, motivos y propósitos de la exclusión, fecha/hora, etc.

   Nota
   Si se añaden varios elementos en una única entrada, solo podrá haber un comentario para todos los elementos.

5. Haga clic en **Agregar** y luego en **Listo**.

Uso de comodines para definir exclusiones

Puede utilizar el carácter comodín asterisco (*) para añadir procesos de confianza a las listas de exclusión. El asterisco sustituye a cero o más caracteres. No se pueden utilizar variables de entorno, como %AppData%.

Los comodines se pueden usar en medio o al final de la descripción.

Ejemplos de comodines aceptados en descripciones:

- `C:\*.exe`
- `D:\folders\file.*`
- `C:\Users\*\AppData\Roaming\*.exe`

No se pueden utilizar comodines al principio de una descripción. Ejemplos de comodines no aceptados en descripciones:

- `*.exe`
- `*:\folder\process.exe`

Antivirus Microsoft Defender y Microsoft Security Essentials

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Antivirus Microsoft Defender

El antivirus Microsoft Defender es un componente antimalware integrado de Microsoft Windows que se empezó a ofrecer en Windows 8.

Con el módulo Antivirus Microsoft Defender (WDA), puede configurar la directiva de seguridad del antivirus Microsoft Defender y realizar un seguimiento de su estado a través de la consola de Cyber Protect.

© Acronis International GmbH, 2003-2025

Este módulo se aplica a cargas de trabajo en las que esté instalado el Antivirus de Microsoft Defender.

Nota
Si habilita **Antivirus Microsoft Defender** para la protección en tiempo real, el módulo **Protección en tiempo real** se desactiva automáticamente para evitar que se produzcan conflictos. Las detecciones de virus/malware y la cuarentena son gestionadas por el Antivirus Microsoft Defender y cualquier incidente de EDR relacionado con detecciones de virus/malware se crea a partir de la información proporcionada por el Antivirus Microsoft Defender. EDR incluye otros motores de detección que pueden crear otros tipos de incidentes sin la intervención del Antivirus Microsoft Defender.

De forma similar, si habilita **Protección en tiempo real**, el módulo **Antivirus Microsoft Defender** se deshabilita automáticamente.

Los ajustes de la **protección contra manipulaciones** en Windows también deben estar desactivados para garantizar que el Antivirus Microsoft Defender funcione correctamente en Cyber Protect Cloud. Para obtener más información, consulte este artículo de la base de conocimientos.

Además, si el **Motor de comportamiento** o la **Protección antivirus y antimalware** están deshabilitados en el plan de protección cuando EDR está habilitado, también estará deshabilitada la opción **Endpoint Detection and Response (EDR)**.

Microsoft Security Essentials

Microsoft Security Essentials es un componente antimalware integrado de Microsoft Windows que se empezó a ofrecer con Windows en versiones anteriores a la 8.

Con el módulo Antivirus Microsoft Security Essentials, puede configurar la directiva de seguridad de Microsoft Security Essentials y realizar un seguimiento de su estado a través de la consola de Cyber Protect.

Este módulo se aplica a cargas de trabajo en las que esté instalado Microsoft Security Essentials.

La configuración de Microsoft Security Essentials es similar a la del antivirus Microsoft Defender, pero no puede configurar la protección en tiempo real ni definir las exclusiones con la consola de Cyber Protect.

Planificar análisis

Especifique la planificación para el análisis planificado.

Modo de análisis:

- **Full**: comprobación completa de todos los archivos y las carpetas, además de los elementos analizados en el análisis rápido. Para su ejecución se necesitan más recursos del equipo que los empleados para el análisis rápido.
- **Rápido**: comprobación rápida de los procesos y las carpetas de la memoria en los que se suele encontrar malware. Para su ejecución, se requieren menos recursos del equipo.

© Acronis International GmbH, 2003-2025

Defina el día de la semana y la hora en que se llevará a cabo el análisis.

Análisis rápido diario: sirve para definir el momento en que tendrá lugar el análisis diario rápido.

Puede establecer las siguientes opciones en función de sus necesidades:

Iniciar el análisis planificado cuando el equipo está encendido, pero no en uso

Buscar las definiciones de virus y software espía más recientes antes de ejecutar un análisis planificado

Limitar el uso de la CPU durante el análisis a

Para obtener más información sobre la configuración del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/mem/configmgr/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings

Acciones predeterminadas

Defina las acciones predeterminadas que se van a llevar a cabo para las amenazas detectadas con distintos niveles de gravedad:

- **Limpiar**: limpiar el malware detectado en una carga de trabajo.
- **Cuarentena**: poner en cuarentena el malware detectado en la carpeta Cuarentena, pero no eliminarlo.
- **Eliminar**: eliminar el malware detectado de una carga de trabajo.
- **Permitir**: no eliminar ni poner en cuarentena el malware detectado.
- **Definido por el usuario**: se pedirá a un usuario que especifique la acción que se va llevar a cabo con el malware detectado.
- **Sin acción**: no se llevará a cabo ninguna acción.
- **Bloquear**: bloquear el malware detectado.

Para obtener más información sobre la configuración de las acciones por defecto del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

Protección en tiempo real

Habilite la **Protección en tiempo real** para detectar malware e impedir que se instale o se ejecute en las cargas de trabajo.

Analizar todas las descargas: si esta opción está seleccionada, se analizan todos los adjuntos y archivos descargados.

Habilitar supervisión del comportamiento: si esta opción está seleccionada, se habilitará la supervisión del comportamiento.

Analizar archivos de red: si esta opción está seleccionada, se analizarán los archivos de red.

© Acronis International GmbH, 2003-2025

Permitir análisis completo de los dispositivos de red asignados: si esta opción está seleccionada, se analizarán por completo los dispositivos de red asignados.

Permitir análisis del correo electrónico: si esta opción está habilitada, el motor analizará los archivos del correo y de los buzones de correo en función de su formato específico con el fin de analizar los archivos adjuntos y el cuerpo de los correos.

Para obtener más información sobre la configuración de la protección en tiempo real del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings

Avanzado

Especifique la configuración de análisis avanzado:

- **Analizar archivos del archivo comprimido**: incluye archivos comprimidos como archivos .zip o .rar en el análisis.
- **Analizar unidades extraíbles**: analiza unidades extraíbles durante los análisis completos.
- **Crear un punto de restauración del sistema**: hay ocasiones en las que una entrada de registro o un archivo importante se elimina como "falso positivo". Con esta opción podrá restaurar el sistema desde un punto de recuperación.
- **Eliminar archivos en cuarentena después de**: define el periodo tras el que se eliminarán los archivos que están puestos en cuarentena.
- **Enviar muestras de archivos automáticamente cuando se requiere un análisis más detallado:**
  - **Indicar siempre**: se le pedirá su confirmación antes de enviar un archivo.
  - **Enviar muestras seguras automáticamente**: se enviarán automáticamente la mayoría de las muestras, excepto los archivos que puedan contener información personal. Esos archivos requerirán una confirmación adicional.
  - **Enviar todas las muestras automáticamente**: se enviarán todas las muestras automáticamente.
- **Deshabilitar interfaz del antivirus Windows Defender**: si se selecciona esta opción, no estará disponible la interfaz de usuario del antivirus Windows defender para un usuario. Puede gestionar las directivas del antivirus Windows Defender a través de la consola de Cyber Protect.
- **MAPS (Microsoft Active Protection Service)**: comunidad en línea que la ayuda a decidir cómo responder a posibles amenazas.
  - **No quiero unirme a MAPS**: no se enviará ninguna información a Microsoft sobre el software que se haya detectado.
  - **Afiliación básica**: se enviará información básica a Microsoft sobre el software que se haya detectado.
  - **Afiliación avanzada**: se enviará información más detallada a Microsoft sobre el software que se haya detectado.

© Acronis International GmbH, 2003-2025

Para obtener más información, consulte https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/ (en inglés).

Para obtener más información sobre la configuración avanzada del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

Exclusiones

Puede definir que se excluyan del análisis los siguientes archivos y carpetas:

- **Procesos**: cuando añade un proceso, cualquier archivo en que el proceso lea o escriba quedará excluido del análisis. Tiene que definir una ruta completa al archivo ejecutable del proceso.
- **Archivos y carpetas**: los archivos y las carpetas especificados excederán del análisis. Tiene que definir una ruta completa a una carpeta o un archivo, o bien definir la extensión del archivo.

Para obtener más información sobre la configuración de exclusiones del antivirus Microsoft Defender, consulte https://docs.microsoft.com/es-es/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

Gestión del cortafuegos

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La gestión del cortafuegos le permite ajustar fácilmente la configuración del cortafuegos en las cargas de trabajo protegidas.

Esta funcionalidad en Cyber Protect se proporciona a través de un componente integrado del cortafuegos de Microsoft Defender de Microsoft Windows. El cortafuegos de Microsoft Defender bloquea el tráfico de red no autorizado que entra o sale en las cargas de trabajo.

Esta gestión del cortafuegos se aplica a cargas de trabajo en las que esté instalado el cortafuegos de Microsoft Defender.

Sistemas operativos Windows compatibles

Los siguientes sistemas operativos Windows son compatibles para la gestión del cortafuegos:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

© Acronis International GmbH, 2003-2025

Windows Server no es compatible.

Habilitar y deshabilitar la gestión del cortafuegos

Puede habilitar la gestión del cortafuegos al crear un plan de protección. Puede cambiar un plan de protección existente para habilitar o deshabilitar la gestión del cortafuegos.

Pasos para habilitar o deshabilitar la gestión del cortafuegos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Realice uno de los siguientes procedimientos para abrir el panel del plan de protección:
   - Si va a crear un nuevo plan de protección, seleccione un equipo para proteger, haga clic en **Proteger** y, a continuación, haga clic en **Crear plan**.
   - Si va a cambiar un plan de protección existente, seleccione un equipo protegido, haga clic en **Proteger**, haga clic en el icono de puntos suspensivos (...) junto al nombre del plan de protección y, a continuación, haga clic en **Editar**.
3. En el panel del plan de protección, vaya al área de **gestión del cortafuegos** y habilite o deshabilite la **gestión del cortafuegos**.
4. Realice uno de los siguientes procedimientos para aplicar los cambios:
   - Para crear un plan de protección, haga clic en **Crear**.
   - Para editar un plan de protección, haga clic en **Guardar**.

El **estado del cortafuegos de Microsoft Defender** en el área de **gestión del cortafuegos** del panel del plan de protección aparece como **activado** o **desactivado**, en función de si ha habilitado o deshabilitado la gestión del cortafuegos.

También puede acceder al plan de protección desde la pestaña Administración. Sin embargo, esta opción no está disponible en todas las ediciones del servicio Cyber Protection.

Cuarentena

`Cuarentena` es una carpeta especial y aislada en el disco duro de un dispositivo protegido. Si la protección antivirus y antimalware detecta algún archivo sospechoso, se mueve a esta carpeta para evitar la propagación de amenazas.

En la pestaña **Cuarentena** de la consola de Cyber Protection puede revisar los archivos sospechosos y potencialmente peligrosos de todos los dispositivos protegidos y decidir si eliminarlos o restaurarlos.

Nota
Los archivos que estén en cuarentena se borran automáticamente si el dispositivo se ha eliminado del entorno.

© Acronis International GmbH, 2003-2025

¿Cómo llegan los archivos a la carpeta de cuarentena?

1. En el plan de protección, seleccione **Cuarentena** como la acción predeterminada para los archivos infectados o sospechosos.
   Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 250).
2. Mientras se realiza el análisis, el módulo de protección antivirus y antimalware detecta los archivos malintencionados y los mueve a la carpeta segura de `Cuarentena`.
3. El módulo actualiza la lista de cuarentena para añadir información sobre los archivos que se movieron a esta carpeta de cuarentena.

Nota
Los archivos se borran automáticamente de la carpeta `Cuarentena` cuando pasa el periodo de tiempo definido en el parámetro **Eliminar archivos en cuarentena después de** del plan de protección. Consulte "Configuración de cuarentena" (p. 1172).

Gestión de los archivos que están en cuarentena

Para gestionar los archivos en cuarentena, vaya a **Protección** > **Cuarentena**. La lista de archivos en cuarentena de todos los dispositivos protegidos contiene la siguiente información.

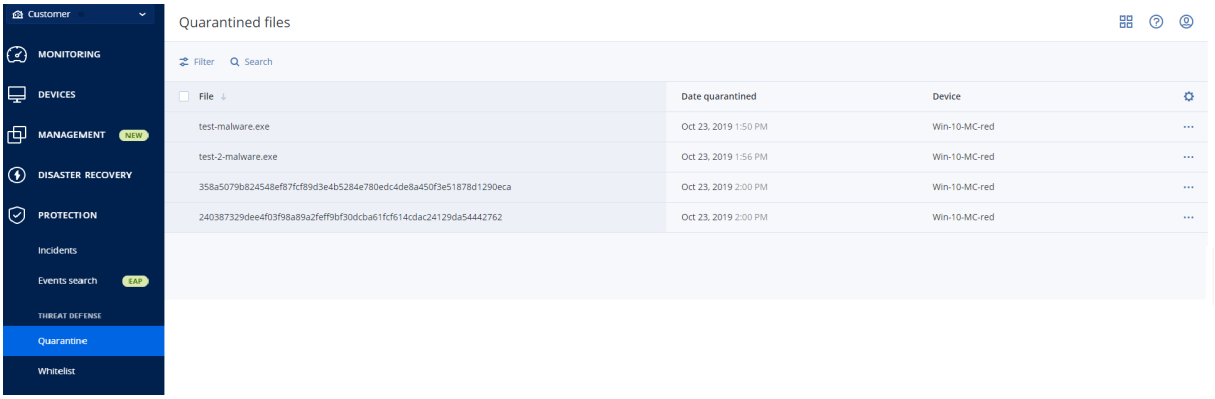
Nombre	Descripción
Archivo	El nombre del archivo en cuarentena.
Fecha de puesta en cuarentena	Fecha y hora en que el archivo se puso en cuarentena.
Dispositivo	Dispositivo en que se encuentra el archivo infectado.
Nombre de la amenaza	El nombre de la amenaza.
Plan de protección	El plan de protección según el cual el archivo sospechoso se puso en cuarentena.

Puede llevar a cabo las siguientes acciones en los archivos en cuarentena:

- **Eliminar**: Eliminar permanentemente un archivo en cuarentena de todos los equipos. Puede eliminar todos los archivos con el mismo hash de archivo. Puede restaurar todos los archivos con el mismo hash de archivo. Agrupe los archivos por hash, seleccione los que necesite y después, elimínelos.
- **Restaurar**: Restaurar un archivo en cuarentena a su ubicación original sin ninguna modificación. Si ya hay un archivo con el mismo nombre en la ubicación original, se sobrescribirá con el archivo restaurado.

© Acronis International GmbH, 2003-2025

Nota
El archivo restaurado se añadirá a la lista de permitidos y se omitirá cuando se realicen otros análisis antimalware.



Ubicación de la carpeta Cuarentena en los equipos

A continuación, se muestra una lista de ubicaciones predeterminadas para los archivos en cuarentena por sistema operativo.

- Para equipos Windows: `%programdata%\Acronis\NGMP\quarantine`
- Para equipos Mac: `/Library/Application Support/Acronis/NGMP/quarantine`
- Para equipos Linux: `/var/lib/Acronis/NGMP/quarantine`

El almacenamiento para poner los archivos en cuarentena se encuentra en la protección de autodefensa del proveedor de servicios.

Carpeta personalizada de autoservicio bajo demanda

Puede seleccionar carpetas personalizadas de la carga de trabajo y analizarlas directamente desde el menú contextual.

Para acceder a la opción Análisis con Cyber Protect de menú contextual

Para las cargas de trabajo con protección antivirus y antimalware habilitada en el plan de protección, haga clic con el botón derecho en la carpeta o carpetas en las que quiera realizar el análisis.

Nota
Esta opción solo está disponible para los administradores de la carga de trabajo.

Lista de permitidos corporativa

Una solución antivirus puede identificar aplicaciones legítimas específicas de la empresa como sospechosas. Para evitar estas detecciones de falsos positivos, las aplicaciones de confianza deben

© Acronis International GmbH, 2003-2025

agregarse manualmente a una lista blanca.

Nota
La lista blanca corporativa no afecta a los análisis antimalware de las copias de seguridad.

Cyber Protection puede automatizar este proceso: el módulo de protección antivirus y antimalware analiza las copias de seguridad y los datos escaneados, lo que permite que dichas aplicaciones se incorporen a la lista de permitidos y se eviten detecciones de falsos positivos. Además, la lista blanca para toda la empresa mejora el rendimiento del análisis antimalware.

La lista blanca se crea para cada cliente basándose en sus datos.

La lista blanca se puede activar y desactivar. Cuando está desactivada, sus archivos añadidos se ocultan temporalmente.

Nota
Solo las cuentas con rol de administrador (por ejemplo, administrador de Cyber Protection, administrador de la empresa, administrador de un partner que opera en nombre del administrador de una empresa, administrador de la unidad) pueden configurar y gestionar la lista de permitidos.

Esta función no está disponible para una cuenta de administrador de solo lectura ni para una cuenta de usuario.

Inclusión automática de aplicaciones en la lista blanca

1. Ejecutar un análisis en la nube de las copias de seguridad en al menos dos equipos. Para hacerlo, utilice los planes de análisis de copia de seguridad.
2. En la configuración de las listas de permitidos, habilite el conmutador **Generación automática de listas de permitidos**.

Inclusión manual de aplicaciones en la lista blanca

Cuando el conmutador **Generación automática de listas de permitidos** esté deshabilitado, podrá añadir archivos a la lista de permitidos de forma manual.

1. En la consola de Cyber Protect, vaya a **Protección** > **Lista de permitidos**.
2. Haga clic en **Añadir archivo**.
3. Especifique la ruta del archivo y haga clic en **Agregar**.

Añadir archivos en cuarentena a la lista blanca

Puede añadir archivos en cuarentena a la lista blanca.

1. En la consola de Cyber Protect, vaya a **Protección** > **Cuarentena**.
2. Seleccione un archivo en cuarentena y haga clic en **Añadir a la lista blanca**.

© Acronis International GmbH, 2003-2025

Configuración de la lista blanca

Cuando habilite el conmutador **Generación automática de listas de permitidos**, debe especificar uno de los siguientes niveles de protección heurística:

- **Bajo**
  Las aplicaciones empresariales se añadirán a la lista de permitidos solo después de un tiempo significativo y varias comprobaciones. Tales aplicaciones ofrecen mayor confianza. Sin embargo, este enfoque aumenta la posibilidad de que se detecten falsos positivos. Los criterios para considerar que un archivo está limpio y es de confianza son muy elevados.
- **Predeterminado**
  Las aplicaciones empresariales se añadirán a la lista de permitidos en función del nivel de protección recomendado para reducir la detección de posibles falsos positivos. Los criterios para considerar que un archivo está limpio y es de confianza son intermedios.
- **Alto**
  Las aplicaciones empresariales se añadirán a la lista de permitidos más rápido para reducir la detección de posibles falsos positivos. Sin embargo, así no se garantiza que el software esté limpio y más adelante podría reconocerse como sospechoso o malware. Los criterios para considerar que un archivo está limpio y es de confianza son bajos.

Visualización de detalles sobre elementos de la lista blanca

Puede hacer clic en un elemento para ver más información sobre este y analizarlo en línea.

Si tiene dudas sobre un elemento que añadió, puede comprobarlo en el analizador de VirusTotal. Al hacer clic en **Comprobar en VirusTotal**, el sitio analiza archivos y URL sospechosos para detectar tipos de malware mediante el hash del archivo del elemento que añadió. Puede ver el hash en la cadena **Hash del archivo (MD5)**.

El valor **Equipos** representa el número de equipos en los que se ha encontrado ese hash durante el análisis de copias de seguridad. Este valor se completa solo si un elemento proviene del análisis de copias de seguridad o de la cuarentena. El campo se queda vacío si se ha añadido el archivo manualmente a la lista blanca.

Análisis antimalware de copias de seguridad

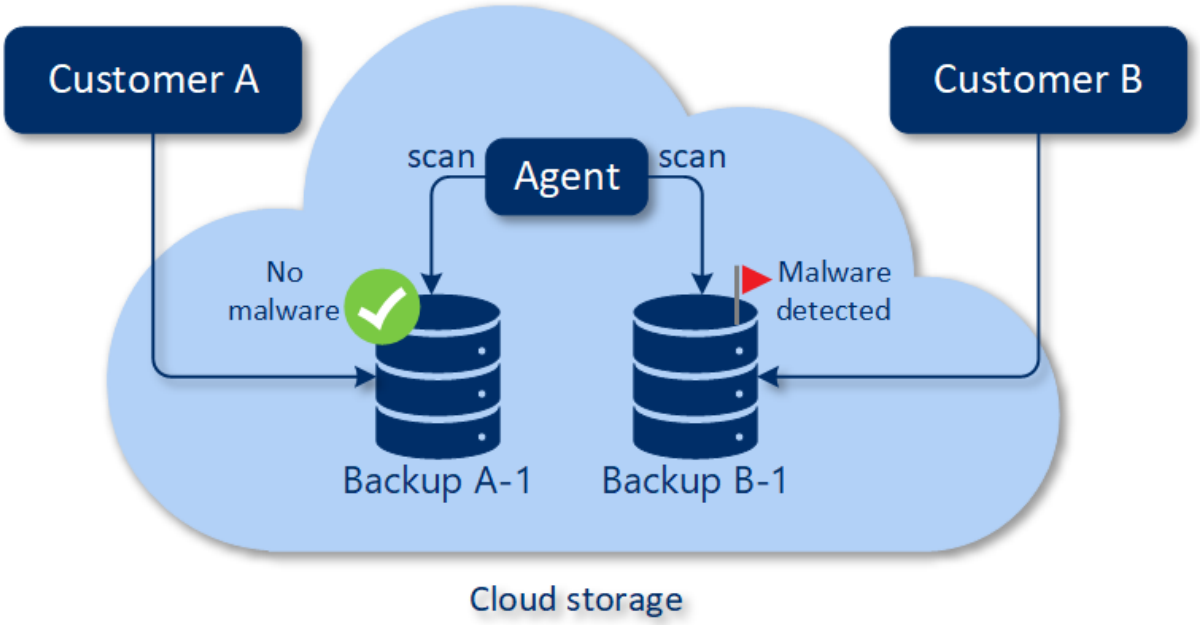
Nota
Esta descripción se aplica a una función que no está disponible para las copias de seguridad de la nube a la nube. Para obtener más información sobre una función similar, el análisis antimalware de buzones de correo de Microsoft 365, consulte "Análisis antimalware de buzones de correo" (p. 857).

Con un análisis antimalware de las copias de seguridad puede evitar la recuperación de archivos ejecutables infectados, ya que comprueba si sus copias de seguridad están libres de malware. Los

© Acronis International GmbH, 2003-2025

análisis antimalware los realiza un agente de la nube que reside en el centro de datos de Cyber Protection y no se utilizan recursos informáticos locales.

Nota
Solo se escanean los archivos ejecutables (*.exe) en busca de malware.



Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para realizar un análisis antimalware, debe configurar un plan de análisis de copias de seguridad. Para obtener más información, consulte "Planes de análisis de copia de seguridad" (p. 277).

Cada plan de análisis de copias de seguridad crea una tarea de análisis para el agente de la nube y agrega esta tarea a una cola, que es una por centro de datos. Las tareas de análisis se procesan de acuerdo con su orden en la cola.

El tiempo de análisis depende del tamaño de la copia de seguridad. Por eso, hay un retraso entre la creación de un plan de análisis de copias de seguridad y la finalización del mismo.

Las copias de seguridad que seleccionó para llevar a cabo el análisis pueden encontrarse en uno de los siguientes estados:

- No analizado
- Sin malware
- Malware detectado

© Acronis International GmbH, 2003-2025

Puede comprobar los resultados del análisis de una copia de seguridad en el widget de **Detalles del análisis de copias de seguridad (amenazas)**. Puede encontrarlo en la consola de Cyber Protect, en la pestaña **Supervisión** > **Información general**.

Limitaciones

- El análisis antimalware solo es compatible con las copias de seguridad de **Todo el equipo** o **Discos/volúmenes** de las siguientes cargas de trabajo:
  - Equipos Windows en los que hay instalado un agente de protección.
  - Máquinas virtuales de Windows de las que se hace una copia de seguridad a nivel del hipervisor (copia de seguridad sin agente) por un Agente para Hyper-V y Agente para VMware (Windows).

  El análisis antimalware no es compatible con copias de seguridad creadas por dispositivos virtuales, como el agente para VMware (dispositivo virtual), el agente para Virtuozzo, agente para Scale Computing HC3, agente para Azure y agente para oVirt.
- Solo se pueden escanear los volúmenes con el sistema de archivos NTFS con partición GPT y MBR.
- El análisis antimalware solo se admite en el almacenamiento en la nube predeterminado. No se admite en los almacenamientos locales, los almacenamientos alojados por partners ni los almacenamientos en la nube pública.
- El análisis antimalware no es compatible con los inquilinos en el modo Cumplimiento.
- El análisis antimalware no es compatible con los siguientes tipos de archivos:
  - RAR
  - 7z
  - ISO
- Si una tarea de análisis falla, se volverá a intentar en un día.
- Cuando seleccione las copias de seguridad para analizar, puede seleccionar conjuntos de copias de seguridad que incluyan una copia de protección continua de datos (CDP). No obstante, solo se analizarán las copias de seguridad de este conjunto que no sean de CDP. Para obtener más información sobre las copias de seguridad CDP, consulte "Protección continua de datos (CDP)" (p. 552).
- Cuando ejecute la recuperación segura de un equipo completo, puede seleccionar un conjunto de copias de seguridad que incluya una copia de seguridad CDP. Sin embargo, esta operación de recuperación no utilizará los datos en la copia de seguridad de la CDP. Para recuperar los datos de la CDP, ejecute una operación de recuperación de **Archivos/carpetas**.

© Acronis International GmbH, 2003-2025

Trabajar con funciones de protección avanzada

De forma predeterminada, Cyber Protect incluye características que abarcan la mayoría de amenazas de ciberseguridad. Puede utilizar estas características sin coste adicional. Asimismo, puede habilitar funciones avanzadas para mejorar la protección de sus cargas de trabajo.

- Si tiene disponible alguna función de protección avanzada, se mostrará en el plan de protección marcada con el icono  de función avanzada.
- Si no tiene disponible una función de protección avanzada, contacte con su administrador para habilitar el paquete de protección avanzada requerido.
- Si el administrador le autoriza a comprar paquetes de seguridad adicionales, puede habilitar las funciones avanzadas. Aparecerá un mensaje en la pantalla para informarle de que se aplican cargos adicionales.

Nota
Si se habilita al menos una función, deberá comprar el paquete de protección avanzada correspondiente.

Nota
Si se deshabilitan todas las funciones avanzadas de su plan de protección, se deshabilitará el paquete de protección avanzada correspondiente.

Paquete de protección avanzada	Funciones de protección avanzada
Advanced Backup	Protege sus recursos informáticos continuamente y garantiza que incluso los cambios de última hora en su trabajo no se pierdan. Las funciones incluyen: • Recuperación con un clic • Protección continua de datos • Soporte de copia de seguridad para los clústeres de Microsoft SQL Server y Microsoft Exchange: Grupos de disponibilidad Always On (AAG) y Grupos de disponibilidad de base de datos (DAG) • Soporte de copia de seguridad para MariaDB, MySQL, Oracle DB y SAP HANA • Mapa de protección de datos e informes de cumplimiento normativo • Procesamiento de datos fuera del host • Frecuencia de las copias de seguridad para cargas de trabajo de Microsoft 365 y Google Workspace • Operaciones remotas con soportes de arranque • Copia de seguridad directa a Microsoft Azure, Amazon S3 y almacenamiento en la nube pública de Wasabi
Advanced Security +	El paquete Advanced Security + XDR está compuesto por "Extended Detection and Response (XDR)" (p. 1339), "Endpoint Detection and Response (EDR)" (p. 1250) y Managed

© Acronis International GmbH, 2003-2025

XDR	Detection and Response (MDR), y protege sus recursos informáticos de forma continuada de todas las amenazas de malware. Entre las funciones, se encuentran las siguientes: • Integraciones con soluciones de terceros, incluidas Perception Point, aplicaciones de colaboración de Microsoft 365 y Microsoft Entra ID • Gestionar incidentes en una página de incidentes centralizada • Visualizar el ámbito y el impacto de los incidentes • Recomendaciones y medidas de corrección • Comprobar si hay ataques de dominio público en sus cargas de trabajo utilizando las fuentes de información sobre amenazas • Almacenar los eventos de seguridad durante 180 días • Protección contra ransomware: Active Protection • Protección antivirus y antimalware con detección basada en firmas locales (con protección en tiempo real) • Prevención de vulnerabilidades • Filtrado de URL • Gestión del cortafuegos de endpoint • Copia de seguridad forense, análisis de copias de seguridad en busca de malware, recuperación segura, lista blanca corporativa • Planes de protección inteligentes (integración con alertas del CPOC) • Análisis de copia de seguridad centralizado para malware • Borrado remoto • Antivirus Microsoft Defender • Microsoft Security Essentials • Análisis de copias de seguridad en busca de malware de buzones de correo de Microsoft 365
RMM	Proporciona un nivel avanzado de supervisión y gestión de los endpoints y las licencias de Microsoft 365. Las funciones incluyen: Para los endpoints: • Gestión de parches • Estado del disco • Inventario de software • Evaluación de vulnerabilidades de terceros compatibles con sistemas operativos Windows • Correcciones a prueba de fallos • Secuencia de comandos cibernética • Asistencia remota • Transferencia y uso compartido de archivos • Selección de una sesión para conectarse • Observar las cargas de trabajo en la vista múltiple • Modos de conexión: control, solo visualización y cortina • Conexión mediante la aplicación Asistencia rápida

© Acronis International GmbH, 2003-2025

	• Protocolos de conexión remota: NEAR y el uso compartido de pantalla de Apple • Grabación de la sesión para conexiones NEAR • Transmisión de captura de pantalla • Informe de historial de sesiones • 24 monitores • Supervisión basada en umbrales • Supervisión basada en anomalías • Despliegue remoto de software mediante DeployPilot • Evaluaciones de vulnerabilidad para aplicaciones Windows de terceros • Seguimiento de geolocalización • Chat de asistencia Para licencias de Microsoft 365: • Corrección automática y manual de desviaciones de línea base y baja de usuarios
Advanced Data Loss Prevention	Impide la fuga de información confidencial de las cargas de trabajo protegidas. Las funciones incluyen: • Prevención consciente del contenido de la pérdida de datos de cargas de trabajo a través de dispositivos periféricos y comunicación de red • Detección automática prediseñada de la información de identificación personal (PII), la información de salud protegida (PHI) y los datos del Estándar de Seguridad de los Datos para la Industria de Tarjetas de Pago (PCI DSS), así como de los documentos de la categoría "Marcado como confidencial" • Creación de la directiva de prevención de pérdida de datos automática con asistencia del usuario final opcional • Aplicación de la prevención de pérdida de datos adaptada con ajuste automático de directivas basado en el aprendizaje • Registro de auditoría centralizado basado en la nube, alertas y notificaciones de usuario final

Advanced Data Loss Prevention

El módulo Advanced Data Loss Prevention analiza el contenido y el contexto de las transferencias de datos en las cargas de trabajo protegidas y previene la filtración de datos confidenciales a través de dispositivos periféricos o transferencias de redes en y fuera de la red de la empresa según la directiva de flujo de datos.

Las características de Advanced Data Loss Prevention pueden incluirse en cualquier plan de protección para un inquilino cliente si el servicio de protección y el paquete de Advanced Data Loss Prevention están habilitados para ese cliente.

Antes de empezar a utilizar el módulo de Advanced Data Loss Prevention, compruebe que lee y entiende los conceptos básicos y la lógica de la gestión de Advanced DLP descritos en la Guía de fundamentos.

Puede que también desee revisar el documento de Especificaciones técnicas.

© Acronis International GmbH, 2003-2025

Creación de la directiva de flujo de datos y reglas de la directiva

El principio clave de la prevención de pérdida de datos exige que se permita a los usuarios de un sistema de TI corporativo administrar los datos confidenciales solo en la medida de lo necesario para ejecutar sus obligaciones laborales. Cualquier otra transferencia de datos confidenciales: irrelevante para los procesos comerciales, deben bloquearse. Por ello, es fundamental distinguir entre transferencias o flujos de datos relacionados con el negocio y no autorizados.

La directiva de flujo de datos contiene reglas que especifican qué flujos de datos están permitidos y cuáles prohibidos, con el fin de evitar transferencias no autorizadas de información confidencial cuando el módulo de prevención de pérdida de datos está activado en un plan de protección y se ejecuta en el modo de aplicación.

Cada categoría de confidencialidad de la directiva contiene una regla predeterminada, marcada con un asterisco (*) y una o más reglas explícitas (no predeterminadas) que definen los flujos de datos para usuarios o grupos específicos. Obtenga más información sobre los tipos de reglas de directiva en la Guía de fundamentos.

La directiva de flujo de datos suele crearse automáticamente mientras se ejecuta Advanced Data Loss Prevention en el Modo de observación. El tiempo requerido para crear una directiva de flujo de datos representativa es de aproximadamente un mes, pero puede variar según los procesos comerciales de su organización. La directiva de flujo de datos también puede crearla, configurarla y editarla manualmente un administrador de la empresa o de la unidad.

Para iniciar la creación automática de la directiva de flujo de datos

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Gestión** > **Planes de protección**.
3. Haga clic en **Crear plan**.
4. Expanda la sección **Prevención de pérdida de datos** y haga clic en la fila **Modo**.
5. En el cuadro de diálogo Modo, seleccione **Modo de observación** y cómo procesar las transferencias de datos:

Opción	Descripción
Permitir todo	Todas las transferencias de datos confidenciales de las cargas de trabajo de los usuarios se tratan como necesarias para el proceso empresarial y seguras. Se crea una nueva regla para cada flujo de datos detectado que no coincide con una regla ya definida en la directiva.
Justificar todo	Todas las transferencias de datos confidenciales de las cargas de trabajo de los usuarios se tratan como necesarias para el proceso empresarial, pero con riesgos. Por ella, para cada transferencia de salida de datos confidenciales interceptada a cualquier destinatario o destino dentro y fuera de la organización que no coincida con una regla de flujo de datos previamente creada, el usuario debe facilitar una justificación empresarial única. Cuando se presenta la justificación, se crea una nueva

© Acronis International GmbH, 2003-2025

Opción	Descripción
	regla de flujo de datos en la directiva de flujo de datos.
Combinada	La lógica Permitir todo se aplica a todos los flujos de datos confidenciales internos, y la lógica Justificar todo se aplica a todos los flujos de datos externos. **Nota** Para obtener más información acerca de datos internos y externos, consulte Detección automatizada de destino

6. Guarde el plan de protección y aplíquelo a las cargas de trabajo de las que quiera recopilar datos para crear la directiva.

Nota
La filtración de datos no se evita durante el modo de observación.

Para configurar la directiva de flujo de datos de forma manual

1. En la consola de Cyber Protect, vaya a **Protección** > **Directiva de flujo de datos**.
2. Haga clic en **Nueva regla de flujo de datos**.
   El panel de la nueva regla de flujo de datos se expande a la derecha.
3. Seleccione una categoría de confidencialidad, añada un remitente y un destinatario y defina el permiso para las transferencias de datos de la categoría, el remitente y el destinatario seleccionados.

Opción	Descripción
Permitir	Permita a este remitente transferir datos de esta categoría de confidencialidad a este destinatario.
Excepción	No permita a este remitente transferir datos de esta categoría de confidencialidad a este destinatario, pero permita que el remitente envíe una excepción a la regla para una transferencia específica. Cuando este remitente intente transferir datos de esta categoría de confidencialidad a este destinatario, bloquee la transferencia y pida al remitente que envíe una excepción para permitir esta transferencia. Cuando envíe la excepción, se permitirá que se lleve a cabo la transferencia de datos. **Importante** Se permitirán todas las posteriores transferencias de datos entre el remitente y el destinatario para esta categoría de confidencialidad durante cinco minutos después de que se envíe la excepción.
Rechazar	No permita a este remitente transferir datos de esta categoría de confidencialidad a este destinatario y no permita que el remitente solicite una excepción a la regla.

© Acronis International GmbH, 2003-2025

4. (Opcional) Seleccione una acción que debe ejecutarse cuando la regla se active.

Acción	Descripción
Escribir en registro	Almacenar un registro de eventos en el registro de auditoría cuando se active la regla. Se recomienda seleccionar esta acción para las reglas con el permiso **Excepción**.
Generar una alerta	Genere una alerta en la pestaña **Alertas** de Cyber Protect cuando se active la regla. Si se habilitan las notificaciones para el administrador, se enviará también una notificación por correo electrónico.
Notificar al usuario final cuando se deniega una transferencia de datos	Notifique al usuario en tiempo real con un aviso en la pantalla cuando active la regla.

5. Haga clic en **Guardar**.
6. Repita los pasos 2 a 5 para crear varias reglas de categorías y opciones de confidencialidad diferentes y verifique que las reglas resultantes corresponden con las opciones que seleccionó.

Estructura de la directiva de flujo de datos

En la vista **Directiva de flujo de datos**, las reglas de la directiva se agrupan según la categoría de datos confidenciales que controlan. El identificador de la categoría de confidencialidad se muestra a la derecha sobre las reglas de la directiva del grupo.

- Confidencial
  - Información de salud protegida (PHI)
  - Información de identificación personal (PII)
  - Estándar de Seguridad de los Datos para la Industria de Tarjetas de Pago (PCI DSS),
  - Marcado como confidencial
- No confidencial

Para obtener más información sobre el concepto y las características de la directiva de flujo de datos, consulta la Guía de fundamentos.

Estructura de la regla

Cada regla de la directiva consta de los siguientes elementos:

- **Categoría de confidencialidad**
  - **Información de salud protegida (PHI)**
  - **Información de identificación personal (PII)**
  - **Estándar de Seguridad de los Datos para la Industria de Tarjetas de Pago (PCI DSS)**
  - **Marcado como confidencial**

    Consulte "Definiciones de datos confidenciales" (p. 1232)

© Acronis International GmbH, 2003-2025

- **Remitente**: especifica quién inicia una transferencia de datos controlada por esta regla. Puede ser un usuario único, una lista de usuarios o un grupo de usuarios.
  - **Cualquier interno**: un grupo de usuarios que incluye todos los usuarios internos de la organización.
  - **Contacto/Desde la organización**: una cuenta de Windows de la organización reconocida por Advanced Data Loss Prevention, así como el resto de cuentas (incluidas las que utilizan las aplicaciones de comunicación de terceros) que una cuenta específica de Windows haya utilizado antes.
  - **Contacto/Identidad personalizada**: identificador de un usuario interno especificado en uno de los siguientes formatos: correo electrónico, ID de Skype, identificador de ICQ, identificador de IRC, correo electrónico de Jabber, correo electrónico del agente de Mail.ru, número de teléfono de Viber y correo electrónico de Zoom.
    Se pueden utilizar los siguientes comodines para especificar un grupo de contactos:
    - *****: cualquier número de símbolos
    - **?**: cualquier símbolo único
- **Destinatario**: especifica el destino de una transferencia de datos controlada por esta regla. Puede ser un usuario único, una lista de usuarios o un grupo de usuarios, así como otros tipos de destino especificados a continuación.
  - **Cualquiera**: cualquier tipo de destinatario compatible con Advanced DLP.
  - **Contacto/Cualquier contacto**: cualquier contacto interno o externo.
  - **Contacto/Cualquier contacto interno**: cualquier contacto de un usuario interno (consulte "Detección automatizada de destino" (p. 1231)).
  - **Contacto/Cualquier contacto externo**: cualquier contacto de una persona o entidad externa.
  - **Contacto/Desde la organización**: el mismo principio descrito en el campo Remitente.
  - **Contacto/Identidad personalizada**: el mismo principio descrito en el campo Remitente.
  - **Servicios de archivos compartidos**: el identificador de un servicio de archivos compartidos controlado.
  - **Red social**: el identificador de un servicio de red social controlado.
  - **Servidor/Cualquier servidor**: cualquier ordenador reconocido por Advanced DLP como interno o externo.
  - **Servidor/Cualquier servidor interno**: cualquier ordenador reconocido por Advanced DLP como interno.
  - **Servidor/Cualquier servidor externo**: cualquier ordenador reconocido por Advanced DLP como externo.
  - **Servidor/Servidor específico:** un identificador de ordenador especificado como un nombre de servidor (p. ej.,FQDN) o dirección IP (IPv4 o IPv6).
  - **Dispositivo/Cualquier dispositivo**: cualquier dispositivo periférico conectado a la carga de trabajo.

© Acronis International GmbH, 2003-2025

  - **Dispositivo/Almacenamiento externo**: un almacenamiento extraíble o una unidad asignada redirigida conectada a la carga de trabajo.
  - **Dispositivo/Dispositivo extraíble cifrado**: un dispositivo de almacenamiento extraíble cifrado con BitLocker To Go.
  - **Dispositivo/Portapapeles redirigido**: un portapapeles redirigido conectado a la carga de trabajo.
  - **Impresoras**: cualquier impresora local o de red conectada a la carga de trabajo.
- **Permiso**: un control preventivo aplicado a una transferencia de datos controlada por esta regla. Se describe de forma más detallada en el tema Permisos en las reglas de la directiva de flujo de datos.
- **Acción**: una acción no preventiva se ejecuta cuando se activa esta regla. De forma predeterminada, este campo se establece en "Ninguna acción". Las opciones son:
  - **Escribir en registro**: almacene un registro de eventos en el registro de auditoría cuando se active la regla.
  - **Notificar al usuario final cuando se deniega una transferencia de datos**: notifique al usuario con un aviso en pantalla en tiempo real cuando active la regla.
  - **Generar una alerta**: avisar al administrador cuando se active la regla.

Advertencia.
Cuando la opción **Sin acción** está seleccionada y se activa la regla:
- no se añade ningún registro de evento al registro de auditoría;
- no se envía ninguna alerta al administrador;
- no se muestra ninguna notificación en pantalla al usuario final.

¿Qué activa una regla de directiva?

Una transferencia de datos coincide con una regla de directiva de flujo de datos si se cumplen todas las condiciones siguientes:

- Todos los remitentes de esta transferencia de datos se enumeran o pertenecen a un grupo de usuarios especificado en el campo **Remitente** de la regla.
- Todos los destinatarios de esta transferencia de datos se enumeran o pertenecen a un grupo de usuarios especificado en el campo **Destinatario** de la regla.
- Los datos transferidos coinciden con la regla **Categoría de confidencialidad**.

Ajuste de los permisos en las reglas de la directiva de flujo de datos

Advanced Data Loss Prevention admite tres tipos de permisos de las reglas de la directiva de flujo de datos. Los permisos se configuran de manera individual para cada regla de la directiva.

Permitir (permisivo)	Se permiten las transferencias de datos que coinciden con la combinación de categoría de confidencialidad, remitente y destinatario definida en la regla.

© Acronis International GmbH, 2003-2025

Excepción (prohibitivo)	No se permiten las transferencias de datos que coinciden con la combinación de categoría de confidencialidad, remitente y destinatario definida en la regla, pero el remitente puede enviar una excepción a la regla para permitir una transferencia específica. **Importante** Se permitirán todas las posteriores transferencias de datos entre el remitente y el destinatario para esta categoría de confidencialidad durante cinco minutos después de que se envíe la excepción.
Rechazar (prohibitivo)	No se permiten las transferencias de datos que coinciden con la combinación de categoría de confidencialidad, remitente y destinatario definida en la regla, y el remitente no tiene la opción de enviar una excepción.

Además, se puede asignar una etiqueta de prioridad a los permisos **Permitir** y **Excepción** para aumentar la flexibilidad de la gestión de la política. Con esta configuración, puede sobrescribir los permisos establecidos para grupos específicos en otras reglas de flujos de datos de la directiva. Puede utilizarla para aplicar una regla de flujo de datos de grupo solo a algunos de sus miembros. Para lograr esto, tiene que crear una regla de flujo de datos para usuarios específicos que quiera excluir de las reglas de grupo y, a continuación, priorizar sus permisos sobre las restricciones de flujo de datos configurados en las reglas para el grupo al que pertenecen estos usuarios. Para obtener información sobre las prioridades de los permisos al combinar reglas, consulte "Combinación de las reglas de la directiva de flujo de datos" (p. 1224).

Importante
Antes de cambiar una empresa o directiva de la unidad del modo de observación al de aplicación, es fundamental ajustar las reglas predeterminadas para cada categoría de datos confidenciales del estado permisivo al prohibitivo. Las reglas predeterminadas están marcadas con un asterisco (*) en la vista **Directiva de flujo de datos**. Obtenga más información sobre los tipos de reglas de directiva en la Guía de fundamentos.

Pasos para editar permisos en las reglas de la directiva

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Directiva de flujo de datos**.
3. Seleccione la regla de la directiva que desea editar y haga clic en **Editar** encima de la lista de las reglas.
   Se abre la ventana **Editar regla de flujo de datos**.
4. En la sección **Permiso**, seleccione **Permitir**, **Excepción**, o **Rechazar**.
5. (Opcional) Para priorizar el permiso **Permitir** o **Excepción** de esta regla con respecto del permiso de otras reglas, seleccione la casilla de verificación **Priorizar**.
   No necesita utilizar esta casilla de verificación para priorizar una regla de flujo de datos sobre la regla predeterminada Cualquiera > Otra porque tiene la menor prioridad en una directiva de forma predeterminada.

© Acronis International GmbH, 2003-2025

Para obtener información sobre las prioridades de los permisos al combinar reglas, consulte "Combinación de las reglas de la directiva de flujo de datos" (p. 1224).

6. (Opcional) Seleccione una acción para ejecutar cuando la regla se active.
7. Guarde los cambios de la regla de la directiva.

Combinación de las reglas de la directiva de flujo de datos

Cuando una transferencia de datos coincide con más de una regla, se combinan los permisos y acciones de todas las reglas y se aplican del siguiente modo:

Permisos

Si una transferencia de datos coincide con más de una regla y estas reglas tienen diferentes permisos para la misma categoría de datos, la regla predominante es la que tiene un permiso de mayor prioridad, de acuerdo con la siguiente lista de prioridad de permisos (en orden descendente):

1. Excepción con la etiqueta **Priorizado**
2. Permitir con la etiqueta **Priorizado**
3. Rechazar
4. Excepción
5. Permitir

Si una transferencia de datos coincide con más de una regla y estas reglas tienen diferentes permisos para diferentes categorías de datos, se aplica la siguiente lógica para la anulación:

1. El permiso de regla más restrictivo se define para cada una de las categorías de confidencialidad con las que coincide la transferencia de datos.
2. Se aplica el permiso más restrictivo de las reglas que se definen en el punto 1.

Ejemplo

Una transferencia de archivos coincide con tres reglas en las diferentes categorías de confidencialidad como sigue:

Categoría de confidencialidad	Permiso
PII	Permitir: Priorizado
PHI	Excepción: Priorizado
PCI	Rechazar

El permiso que se aplicará es Rechazar.

Acciones

Si una transferencia de datos coincide con más de una regla y estas reglas tienen diferentes opciones configuradas en el campo **Acción**, se llevarán a cabo todas las acciones configuradas en

© Acronis International GmbH, 2003-2025

todas las reglas activadas.

Revisión y gestión de directivas

Antes de que se aplique la política de flujo de datos de referencia creada automáticamente, el cliente debe revisarla, validarla y aprobarla, ya que es el cliente quien conoce inherentemente todos los detalles de sus procesos comerciales y puede evaluar si se interpretan de manera consistente en la directiva de referencia. Asimismo, el cliente puede identificar inexactitudes, que luego corrige el administrador de partners.

Durante la revisión de la directiva, el administrador de partners presenta la directiva de flujo de datos de referencia al cliente, que revisa cada flujo de datos de la directiva y valida su consistencia con los procesos comerciales. La validación no requiere ninguna habilidad técnica, porque la representación de las reglas de la directiva de la consola de Cyber Protect es intuitivamente clara: cada regla describe quién es el remitente y el destinatario de un flujo de datos confidenciales.

Según las instrucciones del cliente, el administrador del partner ajusta manualmente la política de referencia editando, eliminando y creando reglas de directiva de flujo de datos. Tras la aprobación del cliente, se aplica la directiva revisada en las cargas de trabajo protegidos cambiando el plan de protección aplicado a estas cargas de trabajo en el modo de aplicación.

Antes de aplicar una directiva revisada, es importante cambiar el permiso **Permitir** de todas las reglas de directiva predeterminadas creadas automáticamente para las categorías de datos confidenciales a **Rechazar** o **Excepción**. Los usuarios no pueden sobrescribir el permiso **Rechazar**, mientras que el permiso **Excepción** bloquea una transferencia que coincide con la regla, pero permite a los usuarios sobrescribir el bloque en una situación de emergencia al enviar una excepción relacionada con la empresa.

Renovación de la directiva de flujo de datos

Cuando el proceso comercial de la empresa o su unidad ha cambiado de forma importante, sus directivas DLP tienen que renovarse para hacerlas más consistentes con los cambios de los flujos de datos confidenciales del proceso comercial actualizado. La renovación de una directiva también es necesaria si el rol de un empleado cambia. En este caso, también debe renovarse la parte de la directiva de la unidad utilizada para proteger la carga de trabajo del empleado.

El flujo de trabajo de administración de directivas de Advanced DLP permite a los administradores automatizar las renovaciones de directivas para toda la empresa, una unidad, un usuario o una parte de los usuarios de una unidad.

Renovación de la directiva de una empresa o unidad

Todas las opciones del Modo de observación pueden utilizarse para renovar la directiva de toda la empresa o unidad, además de como parte de una directiva de unidad para uno o más usuarios de la unidad.

Pasos para renovar la directiva de una empresa o unidad

© Acronis International GmbH, 2003-2025

El proceso de renovación consta de los siguientes pasos que debe ejecutar un administrador o partner de la empresa que gestiona las cargas de trabajo de esta.

1. Elimine todas las reglas no predeterminadas de la directiva aplicada.
2. Para iniciar la renovación, cambie el plan de protección con Advanced DLP aplicado a la empresa o unidad a una de las opciones del modo de observación, según la que sea adecuada para esa empresa o unidad específica, y aplique el plan a todas las cargas de trabajo de la empresa o la unidad.
3. Cuando el periodo de renovación termine, revise la nueva directiva de la empresa o la unidad con el cliente, ajústela si es necesario y obtenga la aprobación del cliente.
4. Cambie el plan de protección aplicado a las cargas de trabajo de la empresa o la unidad a una opción de modo de aplicación adecuada que el cliente considere óptima para evitar la filtración de datos de las cargas de trabajo de la unidad.

Renovación de la directiva de uno o más usuarios de la empresa o unidad

Las directivas a nivel de usuario pueden renovarse utilizando cualquier opción del Modo de observación, así como el modo de aplicación adaptable.

Uso del Modo de observación para renovar una directiva de usuario

El uso del Modo de observación para renovar una directiva para un usuario o un grupo de usuarios de la empresa (o unidad) tiene los siguientes detalles específicos: la directiva de flujo de datos aplicada para toda la empresa (o unidad) no se aplica a las transferencias de datos de usuarios durante el periodo de renovación. Como resultado, pueden crearse nuevas reglas individuales para el usuario durante la renovación que podrían contradecirse o coincidir con las reglas del grupo existentes de la directiva aplicada para la empresa (o unidad). Cuando se complete la renovación y se vuelva a aplicar la directiva a las transferencias de datos del usuario, si las nuevas reglas individuales creadas para el usuario se aplican en realidad o no a las transferencias de datos del usuario depende de sus prioridades en comparación con otras reglas de la directiva con las que coincidan tales transferencias de datos.

Pasos para renovar la directiva de un usuario a través del Modo de observación

El proceso de renovación consta de los siguientes pasos que debe ejecutar un administrador o partner de la empresa que gestiona las cargas de trabajo de esta.

1. Elimine todas las reglas de la directiva que no sean predeterminadas y se apliquen a la empresa (o unidad) que tengan al usuario como remitente único.
2. Elimine al usuario de las listas de remitentes de las reglas de flujos de datos no predeterminadas de la directiva aplicada.
3. Cree un nuevo plan de protección con Advanced DLP en el Modo de observación y aplíquelo a la carga de trabajo del usuario para comenzar el periodo de renovación (observación).
   La duración del periodo de renovación depende de cuánto tarde el usuario en realizar la totalidad o el 90-95 % de sus actividades comerciales regulares que implican la transferencia de datos confidenciales de sus cargas de trabajo.

© Acronis International GmbH, 2003-2025

4. Cuando el periodo de renovación termine, revise la nuevas reglas relacionadas con este usuario que se hayan añadido a la directiva aplicada, ajústelas si es necesario y obtenga la aprobación del cliente.
5. Cambie el plan de protección aplicado a la carga de trabajo el usuario al modo **Aplicación estricta** o al modo **Aplicación adaptada**, según la opción que el cliente considere óptima para evitar la filtración de datos de la carga de trabajo del usuario.
   De manera alternativa, puede volver a aplicar a la carga de trabajo del usuario el plan de protección aplicado a la empresa (o unidad).

Uso del modo de aplicación adaptada para renovar una directiva de usuario

La renovación de la política para un solo usuario o una parte de todos los usuarios de la empresa (o unidad) se puede llevar a cabo mediante el modo de aplicación adaptada de un plan de protección con Advanced DLP aplicado a la carga de trabajo del usuario.

Nota
Este método de renovación de la política tiene los siguientes detalles: las reglas de la directiva de la empresa (unidad) aplicadas para los grupos de remitentes con la membresía del usuario (es decir, cualquier interno) también se aplican a las transferencias de datos de este usuario durante la renovación. Como resultado, la renovación no creará nuevas reglas individuales para el usuario que podrían contradecirse o coincidir con las reglas de las directivas existentes para los grupos de remitentes. Cuál de estos dos métodos es más efectivo para las renovaciones de directivas de usuario para un cliente en particular depende de sus requisitos de seguridad de TI específicos

Pasos para renovar la directiva de un usuario a través del modo de aplicación adaptada

El proceso de renovación consta de los siguientes pasos que debe ejecutar un administrador o partner de la empresa que gestiona las cargas de trabajo de esta.

1. Elimine todas las reglas de la directiva que no sean predeterminadas y se apliquen a la empresa (unidad) que tengan al usuario como remitente único.
2. Elimine al usuario de las listas de remitentes de las reglas de flujos de datos no predeterminadas de la directiva aplicada.
3. Para todas las reglas de la directiva que no sean predeterminadas y se apliquen a la empresa (o unidad), establezca el permiso en **Excepción** y seleccione la acción **Escribir en registro** en el campo **Acción**.
4. Si el plan de protección aplicado actualmente a la carga de trabajo del usuario se configura en el modo **Aplicación estricta**, cree un nuevo plan de protección con Advanced DLP y aplíquelo a la carga de trabajo del usuario en el modo **Aplicación adaptada** para comenzar el periodo de renovación.
   La duración del periodo de renovación depende de cuánto tarde el usuario en realizar la totalidad o el 90-95 % de sus actividades comerciales regulares que implican la transferencia de datos confidenciales de sus cargas de trabajo.

© Acronis International GmbH, 2003-2025

5. Cuando el periodo de renovación termine, revise la nuevas reglas relacionadas con este usuario que se hayan añadido a la directiva aplicada, ajústelas si es necesario y obtenga la aprobación del cliente.
6. Cambie el plan de protección aplicado a la carga de trabajo el usuario al modo **Aplicación estricta** o déjelo en el modo **Aplicación adaptada**, según la opción que el cliente considere óptima para evitar la filtración de datos de la carga de trabajo del usuario.
   De manera alternativa, puede volver a aplicar a la carga de trabajo del usuario el plan de protección aplicado a la empresa (o unidad).

Habilitar Advanced Data Loss Prevention en los planes de protección

Las características de Advanced Data Loss Prevention pueden incluirse en cualquier plan de protección para un inquilino cliente si el servicio de protección y el paquete de Advanced Data Loss Prevention están habilitados para ese cliente.

Advanced DLP es el módulo avanzado del grupo de funciones de prevención de pérdida de datos. Las funciones de Advanced DLP y el control del dispositivo pueden usarse de forma independiente o conjunta (en un solo plan de protección o en dos planes que protejan el mismo recurso informático). Si se utilizan juntos, sus capacidades funcionales se coordinan como se indica a continuación.

- El control del dispositivo deja de controlar el acceso del usuario a esos canales locales en los que Advanced DLP inspecciona el contenido de los datos transferidos. Sin embargo, el control del dispositivo mantiene el control sobre los tipos de dispositivos siguientes si están configurados para acceso de solo lectura o acceso denegado:
  - Extraíble
  - Extraíble cifrada
  - Unidad asignada

  Por ejemplo, si tiene habilitados tanto el control de dispositivos como el Advanced DLP en un solo plan de protección o en dos planes que protegen el mismo recurso informático y tiene configurado el acceso de solo lectura para los dispositivos USB en el control de dispositivos, el acceso de solo lectura se aplicará a todos los dispositivos USB, excepto a los que están en la lista de permitidos, independientemente de las configuraciones de acceso en el módulo Advanced DLP. Si la opción predeterminada, Habilitar acceso, está configurada en el control de dispositivos, se aplicará la configuración de acceso en Advanced DLP.
- El control de dispositivos impone el acceso del usuario a los siguientes canales locales y periféricos en la lista de permitidos:
  - Unidades ópticas
  - Unidades de disquetes
  - Dispositivos móviles conectados por MTP
  - Adaptadores Bluetooth
  - Portapapeles de Windows

© Acronis International GmbH, 2003-2025

- Capturas de pantalla
- Dispositivos USB y tipos de dispositivo (excepto para el almacenamiento extraíble y cifrado)

Pasos para crear un plan de protección con Advanced DLP

1. Vaya a **Gestión** > **Planes de protección**.
2. Haga clic en **Crear plan**.
3. Expanda la sección **Prevención de pérdida de datos** y haga clic en la fila **Modo**.
   Se abre el cuadro de diálogo **Modo**.
   - Para comenzar con la creación o renovación de la directiva de flujo de datos, seleccione **Modo de observación** y cómo procesar las transferencias de datos:

Opción	Descripción
Permitir todo	Todas las transferencias de datos confidenciales de las cargas de trabajo de los usuarios se tratan como necesarias para el proceso empresarial y seguras. Se crea una nueva regla para cada flujo de datos detectado que no coincide con una regla ya definida en la directiva.
Justificar todo	Todas las transferencias de datos confidenciales de las cargas de trabajo de los usuarios se tratan como necesarias para el proceso empresarial, pero con riesgos. Por ella, para cada transferencia de salida de datos confidenciales interceptada a cualquier destinatario o destino dentro y fuera de la organización que no coincida con una regla de flujo de datos previamente creada, el usuario debe facilitar una justificación empresarial única. Cuando se presenta la justificación, se crea una nueva regla de flujo de datos en la directiva de flujo de datos.
Combinada	La lógica Permitir todo se aplica a todas las transferencias internas de datos confidenciales, y la lógica Justificar todo se aplica a todas las transferencias externas de datos confidenciales. Para ver la definición de destinos internos, consulte "Detección automatizada de destino" (p. 1231)

Advertencia.
- Seleccione el **Modo de observación** solo si no ha creado una directiva de flujo de datos antes o si la está renovando. Antes de empezar la renovación de la directiva, consulte "Renovación de la directiva de flujo de datos" (p. 1225).
- La filtración de datos no se evita durante el Modo de observación. Consulte Modo de observación en la Guía de fundamentos.

   - Para aplicar la directiva de flujo de datos existente, seleccione **Modo de aplicación** y cómo de estricta es la aplicación de las reglas de la directiva de flujo de datos:

Opción	Descripción
Aplicación estricta	La directiva de flujo de datos se aplica tal cual y no se ampliará con nuevas reglas de directivas permisivas cuando se detecten flujos de datos confidenciales no

© Acronis International GmbH, 2003-2025

Opción	Descripción
	observados anteriormente. Consulte Aplicación estricta en la Guía de fundamentos.
Aplicación adaptativa (aplicación con aprendizaje)	La política vigente continúa su adaptación automática a aquellas operaciones comerciales que no se realizaron durante el período de observación o los cambios de los procesos comerciales. Este modo permite que la directiva de flujo de datos aplicada se amplíe en función de los nuevos flujos de datos aprendidos detectados en las cargas de trabajo. Consulte Aplicación adaptada en la Guía de fundamentos.

Importante
Antes de cambiar una empresa o directiva de la unidad del Modo de observación al de aplicación, es fundamental ajustar las reglas predeterminadas para cada categoría de datos confidenciales del estado permisivo al prohibitivo. Las reglas predeterminadas están marcadas con un asterisco (*) en la vista **Directiva de flujo de datos**. Obtenga más información sobre los tipos de reglas de directiva en la Guía de fundamentos.

4. Haga clic en **Listo** para cerrar el cuadro de diálogo Modo.
5. (Opcional) Para configurar el reconocimiento óptico de caracteres, las listas de permitidos y más opciones de protección, haga clic en **Configuraciones Avanzadas**.
   Para obtener más información sobre las opciones disponibles, consulte "Configuraciones avanzadas" (p. 1230).
6. Guarde el plan de protección y aplíquelo a las cargas de trabajo que desee proteger.

Configuraciones avanzadas

Puede usar las configuraciones avanzadas de los planes de protección con Advanced Data Loss Prevention para aumentar la calidad de la inspección del contenido de datos de los canales controlados por Advanced Data Loss Prevention, y excluir de cualquier control preventivo las transferencias de datos a tipos de dispositivos periféricos en la lista de permitidos, categorías de comunicaciones de red, servidores de destino, así como las transferencias de datos iniciadas por aplicaciones en la lista de permitidos. Puede configurar las siguientes configuraciones avanzadas:

- **Reconocimiento óptico de caracteres**
  Esta configuración activa o desactiva el reconocimiento óptico de caracteres OCR para extraer partes de texto en 31 idiomas para una posterior inspección del contenido a partir de archivos gráficos e imágenes de documentos, mensajes, escaneos, capturas de pantalla y otros objetos.
- **Transferencia de datos protegidos por contraseña**
  El contenido de los archivos y documentos protegidos por contraseña no se puede inspeccionar. Con esta configuración, Advanced DLP permite al administrador seleccionar si se deben permitir o bloquear las transferencias de salida de datos protegidos por contraseña.

© Acronis International GmbH, 2003-2025

- **Evitar la transferencia de datos en caso de error**
  A veces, el análisis del contenido que se envía puede fallar o puede producirse otro error de control en las operaciones del agente de DLP. Si esta opción está habilitada, se bloqueará la transferencia. Si la opción está deshabilitada, se permitirá la transferencia a pesar del error.
- **Lista de permitidos para tipos de dispositivos y comunicaciones de red**
  Las transferencias de datos a los tipos de dispositivos periféricos y en las comunicaciones de red marcadas en esta lista están permitidas independientemente de su confidencialidad de datos y de la directiva de flujo de datos aplicada.

  Advertencia.
  Esta opción se usa si hay problemas con un tipo de dispositivo o protocolo específico. No la habilite a menos que se lo indique un representante del soporte técnico.

- **Lista de permitidos para servidores remotos**
  Las transferencias de datos a los servidores de destino especificados en esta lista se permiten independientemente de la sensibilidad de los datos y de la directiva de flujo de datos aplicada.
- **Lista de permitidos para aplicaciones**
  Las transferencias de datos realizadas por aplicaciones especificadas en esta lista se permiten independientemente de la sensibilidad de los datos y de la directiva de flujo de datos aplicada.

El indicador **Nivel de seguridad** de las configuraciones avanzadas que se muestra en la vista **Crear plan de protección** y en la vista "Detalles" de un plan de protección tiene la siguiente lógica de indicación de nivel:

- **Básica** indica que ninguna de las configuraciones avanzadas está activada.
- **Moderada** indica que una o más configuraciones están activadas, pero la combinación de **OCR**, **Transferencia de datos protegidos por contraseña** y **Evitar la transferencia de datos en caso de error** no está activada.
- **Estricta** indica que al menos la combinación de configuraciones de **OCR**, **Transferencia de datos protegidos por contraseña** y **Evitar la transferencia de datos en caso de error** está activada.

Detección automatizada de destino

En el Modo de observación combinada, Advanced Data Loss Prevention aplica diferentes reglas dependiendo de si el destino de la transferencia de datos detectado es interno o externo. La lógica para determinar que un destino es interno se describe a continuación. El resto de destinos se consideran externos.

Para cada transferencia de datos interceptada, Advanced Data Loss Prevention detecta automáticamente si el servidor de destino HTTP, FTP o SMB es interno al ejecutar una solicitud DNS y comprar los nombres FQDN de la máquina en la que se ejecutan el agente de Data Loss Prevention y el servidor remoto. Si la solicitud DNS falla, también se comprueba si la carga de trabajo protegida y el servidor remoto están en la misma red. Los servidores que tienen el mismo

© Acronis International GmbH, 2003-2025

nombre de dominio (o están en la misma subred) que el equipo en el que se ejecuta el agente de Data Loss Prevention se consideran internos.

Para la comunicación por correo electrónico, Advanced Data Loss Prevention trata como internas las transferencias de todos los correos electrónicos enviados desde una dirección de correo electrónico corporativa al utilizar el servidor de correo corporativo si el destinatario del correo electrónico está en el mismo dominio que el remitente y el nombre del servidor del correo electrónico del recipiente es el mismo.

Los correos electrónicos se tratan como comunicaciones externas a menos que se conozca la cuenta del destinatario. Las direcciones de correo electrónico conocidas se actualizan a medida que Data Loss Prevention supervisa la actividad del usuario en la red y actualiza la base de datos del servidor interno con los datos de las direcciones de correo electrónico asociadas con el usuario.

Las comunicaciones a través de correos se tratan como comunicaciones externas a menos que se conozca la cuenta del destinatario. Las cuentas conocidas se actualizan a medida que Data Loss Prevention supervisa la actividad del usuario en la red y actualiza la base de datos del servidor interno con los datos de las cuentas asociadas con el usuario.

Definiciones de datos confidenciales

Este tema describe la lógica de identificar datos confidenciales durante el análisis de contenido.

Para reducir el número de falsos positivos, se cuentan las coincidencias idénticas como una coincidencia para todos los grupos de las expresiones lógicas descritas.

Importante
Las expresiones lógicas utilizadas para identificar contenido se facilitan solo a título informativo y no describen la solución de forma detallada.

Información de salud protegida (PHI)

Idiomas admitidos

- US, UK, inglés internacional
- Finlandés
- Italiano
- Francés
- Polaco
- Ruso
- Húngaro
- Noruego
- Español

© Acronis International GmbH, 2003-2025

Datos considerados Información de Salud Protegida

Los siguientes datos se consideran información de salud protegida:

- Nombres y apellidos
- Dirección (calle, ciudad, condado, distrito, código postal y sus geocódigos equivalentes)
- Números de teléfono
- Direcciones de correo electrónico
- Números de la seguridad social
- Números de beneficiario de los planes de salud
- Números de cuentas bancarias
- URL
- Números de direcciones IP
- Códigos ICD-10-CM
- ICD-10-PCS-and-GEMs
- HIPAA
- Otros relacionados con la asistencia sanitaria
- Números de tarjeta de crédito

Expresión lógica utilizada para la detección de contenido

La expresión lógica está compuesta de las siguientes cadenas unidas por el operador lógico OR. El operador OR se utiliza para unir diferentes grupos de datos de la lista anterior y no se especifica el operador lógico AND de forma explícita. Los números de los paréntesis representan el número de instancias detectadas que podrían devolver un resultado de detección positivo.

- **Números de la seguridad social** (5)
- (Nombres y apellidos (3) OR Dirección (3) OR Números de teléfono (3) OR Dirección de correo electrónico (3) OR Números de cuentas bancarias (3) OR Números de tarjetas de crédito(3)) AND (Números de la seguridad social (3) OR Números de beneficiario de los planes de salud (3) * OR Códigos ICD-10-CM (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR *Otros relacionados con la asistencia sanitaria (3))

Información de identificación personal (PII)

Idiomas admitidos

- US, UK, inglés internacional
- Búlgaro
- Chino

© Acronis International GmbH, 2003-2025

- Checo
- Danés
- Neerlandés
- Finlandés
- Francés
- Alemán
- Húngaro
- Indonesio
- Italiano
- Coreano
- Malayo
- Noruego
- Polaco
- Portugués (Brasil)
- Portugués (Portugal)
- Rumano
- Ruso
- Serbio
- Singapur
- Español
- Sueco
- Taiwán
- Turco
- Thai
- Japonés

Datos considerados información de identificación personal (PII)

- Nombres y apellidos
- Dirección (calle, ciudad, condado, código postal)
- Números de cuentas bancarias
- Números de identificación personal y fiscal
- Números de pasaporte
- Números de la seguridad social
- Números de teléfono

© Acronis International GmbH, 2003-2025

- Números de matrícula
- Números de permiso de conducir
- Identificadores y números de serie
- Direcciones IP
- Direcciones de correo electrónico
- Números de tarjeta de crédito

Expresión lógica utilizada para la detección de contenido

Expresión lógica para todos los idiomas admitidos menos el japonés

La expresión lógica está compuesta de las siguientes cadenas unidas por el operador lógico OR o AND. Los números de los paréntesis representan el número de instancias detectadas que podrían devolver un resultado de detección positivo.

- Números de identificación personal y fiscal (5)
- Nombres y apellidos (3) AND **(**Número de tarjeta de crédito (3) OR Número de la seguridad social (3) OR Número de cuenta bancaria (3) OR Números de identificación personal y fiscal (3) OR Números de permiso de conducir (3) OR Números de pasaporte (3) OR Números de la seguridad social (3) OR Direcciones IP (3) OR Números de matrícula (3) OR Identificadores y números de serie**)**
- Números de teléfono (3) AND **(**Número de tarjeta de crédito (3) OR Número de la seguridad social (3) OR Número de cuenta bancaria (3) OR Dirección (3) OR Números de identificación personal y fiscal (3) OR Números de permiso de conducir (3) OR Números de pasaporte (3) OR Números de la seguridad social (3) OR Números de matrícula (3) OR Identificadores y números de serie (3)**)**
- **(**Nombres y apellidos (30) OR Dirección (30)**)** AND **(**Dirección de correo electrónico (30) OR Números de teléfono (30) OR Direcciones IP (30)**)**
- Direcciones de correo electrónico (3) AND **(**Número de tarjeta de crédito (3) OR Número de la seguridad social (3) OR Número de cuenta bancaria (3) OR Números de identificación personal y fiscal (3) OR Números de permiso de conducir (3) OR Números de pasaporte (3) OR Números de la seguridad social (3) OR Números de matrícula (3) OR Identificadores y números de serie (3)**)**
- Dirección de correo electrónico (30) AND **(**Direcciones (30) OR Números de teléfono (30)**)**
- Nombres y apellidos (30) AND Dirección (30)
- Números de teléfono (30) AND Dirección (30)
- Nombres y apellidos (3) AND Números de cuentas bancarias (3)
- Números de teléfono (3) AND **(**Número de tarjeta de crédito (3) OR Número de cuenta bancaria (3) OR Números de la seguridad social (3) OR Números de identificación personal y fiscal (3) OR Números de permiso de conducir (3) OR Números de pasaporte (3)**)**

© Acronis International GmbH, 2003-2025

Expresión lógica para el idioma japonés

Nota
La detección de contenido solo cuenta las coincidencias únicas.

La expresión lógica está compuesta de las siguientes cadenas unidas por el operador lógico OR. El operador OR se utiliza para unir diferentes grupos si no se especifica el operador AND de forma explícita.

- Números de la seguridad social (5)
- Nombres y apellidos (3) AND **(**Número de tarjeta de crédito (3) OR Número de cuenta bancaria (3) OR Números de permiso de conducir (3) OR Números de pasaporte (3) OR Números de la seguridad social (3)**)**
- Nombres y apellidos (30) AND **(**Dirección de correo electrónico (30) OR Números de teléfono (30) OR Direcciones IP (30) OR Dirección (30)**)**
- Dirección (3) AND **(**Número de tarjeta de crédito (3) OR Número de cuenta bancaria (3) OR Números de permiso de conducir (3) OR Números de pasaporte (3) OR Números de la seguridad social (3)**)**
- Dirección de correo electrónico (3) AND **(**Número de tarjeta de crédito (3) OR Número de cuenta bancaria (3) OR Números de la seguridad social (3) OR Números de permiso de conducir (3)**)**
- Dirección (5) AND **(**Dirección de correo electrónico (5) OR Nombres y apellidos (5) OR Números de teléfono (5) OR Direcciones IP (5)**)**
- Nombres y apellidos (3) AND Números de cuentas bancarias (3)
- Números de teléfono (3) AND **(**Número de tarjeta de crédito (3) OR Número de cuenta bancaria (3) OR Dirección (3) OR Números de la seguridad social (3) OR Números de permiso de conducir (3)**)**

Estándar de Seguridad de los Datos para la Industria de Tarjetas de Pago (PCI DSS)

Idiomas admitidos

Este grupo de confidencialidad es independiente del idioma. Los datos PCI DSS están en inglés en todos los países.

Datos considerados PCI DSS

- Datos del titular de la tarjeta
  - Número de cuenta principal (PAN)
  - Nombre del titular de la tarjeta
  - Fecha de caducidad
  - Código del servicio

© Acronis International GmbH, 2003-2025

- Datos de autenticación confidenciales
  - Datos completos de la pista (datos de banda magnética o equivalente en un chip)
  - CAV2/CVC2/CVV2/CID
  - Bloques de PIN

Expresión lógica utilizada para la detección de contenido

La expresión lógica está compuesta de las siguientes cadenas unidas por el operador lógico OR. Los números de los paréntesis representan el número de instancias detectadas que podrían devolver un resultado de detección positivo.

- Número de tarjeta de crédito (5)
- Número de tarjeta de crédito (3) AND (Nombre americano (Ex) (3) OR Nombre Americano (3) OR Palabras clave PCI DSS (3) OR Fecha (mes/año) (3))
- Volcado de tarjeta de crédito (5)

Marcado como confidencial

Los datos marcados como confidenciales se detectan a través del grupo de palabras clave.

La condición de coincidencia se basa en el peso y el peso de cada palabra es == 1. La detección del contenido se considera positiva cuando coincide si el peso es > 3.

Idiomas admitidos

- Inglés
- Búlgaro
- Chino simplificado
- Chino tradicional
- Checo
- Danés
- Neerlandés
- Finlandés
- Francés
- Alemán
- Húngaro
- Indonesio
- Italiano
- Japonés
- Coreano

© Acronis International GmbH, 2003-2025

- Malayo
- Noruego
- Polaco
- Portugués: Brasil
- Portugués: Portugal
- Ruso
- Serbio
- Español
- Sueco
- Turco

Grupos de palabras clave

El grupo de palabras clave para cada idioma contiene equivalentes específicos del país para las palabras clave utilizadas en inglés (no distingue entre mayúsculas y minúsculas).

- confidencial
- distribución interna
- no apto para su distribución
- no distribuir
- no es para uso público
- no apto para distribución externa
- solo para uso interno
- documentación altamente confidencial
- privada
- información privilegiada
- solo para uso interno
- solo para uso oficial

Eventos para la prevención de pérdida de datos

Advanced Data Loss Prevention genera eventos en la vista de eventos de DLP de la siguiente forma:

- Durante el modo de observación, se generan eventos para todas las transferencias de datos justificadas.
- Durante el modo de aplicación, se generan eventos según la acción **Escribir en registro** configurada para cada regla de la directiva que se activa.

Pasos para ver los eventos de una regla de la directiva de flujo de datos

© Acronis International GmbH, 2003-2025

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Directiva de flujo de datos**.
3. Localice la regla para la que desea ver los eventos y haga clic en los puntos suspensivos al final de la línea de la regla.
4. Seleccione **Ver los eventos**.

Pasos para ver la información sobre el evento en la vista de eventos de DLP

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Eventos de DLP**.
3. Haga clic en un evento de la lista para ver más información sobre él.
   El panel de detalles del evento se expande a la derecha.
4. Desplácese hacia abajo y hacia arriba en el panel de detalles del evento para ver la información disponible.
   Los detalles que se muestran en el panel dependen del tipo y los ajustes de la regla que activó el evento.

Pasos para filtrar eventos en la lista de eventos de DLP

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Eventos de DLP**.
3. Haga clic en **Filtro** en la parte superior izquierda.
4. Seleccione la categoría de confidencialidad, carga de trabajo, tipo de acción, usuario y canal desde los menús desplegables.
   Puede seleccionar más de un elemento en los menús desplegables. El filtrado aplica el operador lógico OR entre los elementos del mismo menú, pero utiliza el operador lógico AND entre los elementos de diferentes menús.
   Por ejemplo, si selecciona la categoría de confidencialidad **PHI** y **PII**, el resultado devolverá todos los eventos que contengan PHI, PII o ambas. Si selecciona la categoría de confidencialidad **PHI** y la acción **Acceso de escritura**, solo aparecerán eventos que coincidan con ambas categorías en el resultado filtrado.
5. Haga clic en **Aplicar**.
6. Para ver todos los eventos de nuevo, haga clic en **Filtro**, luego en **Restablecer a los valores predeterminados** y, por último, haga clic en **Aplicar**.

Pasos para buscar eventos en la lista de eventos de DLP

1. Repita los pasos 1 a 2 del procedimiento anterior.
2. Seleccione una categoría de la lista desplegable a la derecha del Filtro en la que desee buscar: **Remitente**, **Destino**, **Proceso**, **Asunto del mensaje** o **Motivo**.
3. En el cuadro de texto, introduzca la frase que le interesa y confírmela presionando Intro en el teclado.
   En la lista solo aparecen los eventos que coinciden con la frase que ha introducido.

© Acronis International GmbH, 2003-2025

4. Para restablecer la lista de eventos, haga clic en el signo **X** en el cuadro del texto de búsqueda y presione Intro.

Pasos para ver la lista de eventos relacionada con las reglas específicas de la directiva de flujo de datos

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Directiva de flujo de datos**.
3. Seleccione la casilla de verificación que hay frente al nombre de la regla de la directiva que le interesa.
   Puede seleccionar varias reglas de la directiva si es necesario.
4. Haga clic en **Ver los eventos**.
   La vista cambia a **Protección** > **Eventos de DLP** y los eventos relacionados con las reglas de la directiva que ha seleccionado aparecen en la lista.

Widgets de Advanced Data Loss Prevention en el panel de control Información general

El panel de control **Información general** proporciona una serie de widgets personalizables que dan una imagen general de las operaciones relacionadas con el servicio Cyber Protection, incluido Advanced Data Loss Prevention. Puede encontrar los siguientes widgets de Advanced Data Loss Prevention en el panel de control **Información general** de **Supervisión**.

- **Transferencias de datos confidenciales**: muestra el número total de las operaciones de transferencia de datos confidenciales a destinatarios internos y externos. La tabla se divide por el tipo de permisos aplicados: permitidas, justificadas o bloqueadas. Puede personalizar este widget seleccionando el intervalo de tiempo deseado (1 día, 7 días, 30 días o este mes).
- **Categorías de datos confidenciales salientes**: muestra el número total de transferencias de datos confidenciales a destinatarios externos. La tabla se divide por categorías de información confidencial: Información de salud protegida (PHI), Información de identificación personal (PII), PCI DSS and Marcada como confidencial (Confidencial).
- **Remitentes principales de datos confidenciales salientes**: muestra el número total de transferencias de datos confidenciales de la organización a destinatarios externos y una lista de los cinco principales usuarios con el mayor número de transferencias (junto con esos números). Esta estadística incluye las transferencias permitidas y las justificadas. Puede personalizar este widget seleccionando el intervalo de tiempo deseado (1 día, 7 días, 30 días o este mes).
- **Remitentes principales de transferencias de datos confidenciales bloqueadas**: muestra el número total de transferencias de datos confidenciales bloqueados y una lista de los cinco principales usuarios con el mayor número de intentos de transferencia (junto con esos números). Puede personalizar este widget seleccionando el intervalo de tiempo deseado (1 día, 7 días, 30 días o este mes).
- **Eventos de prevención de pérdida de datos recientes**: muestra los detalles de los eventos de prevención de pérdida de datos recientes del rango de tiempo seleccionado. Puede personalizar este widget con las siguientes opciones:

© Acronis International GmbH, 2003-2025

- **Intervalo (fecha de publicación)** (1 día, 7 días, 30 días o este mes).
- Nombre de la **carga de trabajo**
- **Estado de la operación** (permitida, justificada o bloqueada)
- **Confidencialidad** (PHI, PII, Confidencial, PCI DSS)
- **Tipo de destino** (externo, interno)
- **Agrupación** (carga de trabajo, usuario, canal, tipo de destino)

Los widgets se actualizan cada cinco minutos. Los widgets tienen elementos interactivos que le permiten investigar y solucionar problemas. Puede descargar el estado actual del panel de información o bien enviarlo por correo electrónico en formato .pdf y/o .xls.

Categorías de confidencialidad personalizadas

Las categorías de datos confidenciales personalizadas pueden ayudar a una organización a proteger la propiedad intelectual y los datos confidenciales específicos de esa organización mediante la ampliación del catálogo integrado DLP de definiciones de contenido relacionado para su cumplimiento.

Para crear una categoría de confidencialidad personalizada

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Prevención de pérdida de datos** > **Clasificadores de datos**.
3. Seleccione **Categoría de confidencialidad**.
   Se muestra la lista de categorías de confidencialidad.
4. Haga clic en **Agregar** en la esquina superior derecha de la ventana.
5. En la ventana que se abre, introduzca un nombre para la nueva categoría de confidencialidad y haga clic en **Crear**.
   Por defecto, las categorías recién creadas o clonadas están deshabilitadas. Puede habilitarlas una vez que haya configurado todos sus parámetros.
6. En la lista desplegable a la derecha de la fila, haga clic en **Editar**.
7. En el cuadro de diálogo **Editar confidencialidad**, haga clic en **Añadir línea** para expandir la lista de detectores de contenido.
8. Seleccione los detectores de contenido que desea añadir.
   - Para añadir detectores de contenido existentes, seleccione las casillas de verificación junto a sus nombres y, a continuación, haga clic en **Agregar** en la esquina inferior derecha.
   - Para definir un nuevo detector de contenido, haga clic en **Agregar** y configure el detector que necesite.
     En lugar de empezar desde cero, puede clonar un detector de contenido existente y editarlo.
9. Verifique que ha añadido todos los detectores de contenido que necesita y haga clic en **Listo** en la esquina inferior derecha.
10. Active su categoría de confidencialidad personalizada.

© Acronis International GmbH, 2003-2025

En lugar de crear una nueva categoría de confidencialidad desde cero, también puede clonar una (ya sea una confidencialidad personalizada integrada o existente) y ajustar sus parámetros.

1. Para clonar una confidencialidad existente, seleccione **Clonar** en la lista desplegable al final de su fila.
2. Edite la categoría clonada para añadir o eliminar detectores de contenido según sea necesario y haga clic en **Listo** para guardar los cambios.

Nota
La clonación de una categoría de confidencialidad integrada dentro de un inquilino crea una nueva confidencialidad que contiene los mismos detectores que se convierten en personalizados una vez copiados.

Consulte "Detectores de contenido personalizados" (p. 1242).

Detectores de contenido personalizados

Los detectores de contenido permiten definir de forma centralizada los tipos de contenido para los que se desea el control de acceso. Los detectores de contenido especifican los criterios de filtrado de contenido para identificar los datos a los que se deben aplicar las reglas con conocimiento del contenido.

Tipo de archivo

Para crear un detector de contenido de tipo de archivo

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Prevención de pérdida de datos** > **Clasificadores de datos**.
3. Haga clic en **Detectores de contenido**.
   Se abre la lista de detectores de contenido.
4. En la esquina superior derecha de la ventana, haga clic en **Agregar**.
5. En la lista desplegable, seleccione **Tipo de archivo**.
6. Configure el detector de contenido.
   a. Especifique un nombre y una descripción para el detector de contenido.
   b. [Opcional] Seleccione una categoría de sensibilidad de la lista.
   c. En la lista **Tipos de archivos compatibles**, haga clic en el icono «más» para mover el tipo seleccionado a la lista **Tipos de archivos seleccionados**. Al hacer clic en el icono «más» a la derecha del tipo de archivo compatible, lo moverá a la lista Tipos de archivos seleccionados. También puede seleccionar varios tipos de archivos compatibles. Para ello, haga clic en las marcas de verificación junto a los nombres y utilice el botón **Agregar seleccionados** de la esquina superior derecha.
   d. Para eliminar un tipo de archivo de la lista **Tipos de archivos seleccionados**, haga clic en el icono de papelera a la derecha del nombre. También puede eliminar varios tipos de archivos a la vez con las casillas de verificación y el botón **Eliminar seleccionado**.

© Acronis International GmbH, 2003-2025

7. En la esquina inferior derecha, haga clic en **Guardar**.

Palabras clave

Para crear un detector de contenido con palabras clave

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Prevención de pérdida de datos** > **Clasificadores de datos**.
3. Haga clic en **Detectores de contenido**.
   Se abre la lista de detectores de contenido.
4. En la esquina superior derecha de la ventana, haga clic en **Agregar**.
5. En la lista desplegable, haga clic en **Palabras clave**.
6. Configure el detector de contenido.
   a. Introduzca las palabras clave manualmente, una a la vez, o impórtelas desde un archivo CSV o TXT.

      Nota
      Cada palabra clave o frase en el archivo debe especificarse en una nueva línea.

      Después de importar las palabras clave correctamente, puede fusionar las nuevas palabras clave con la lista de existentes o reemplazar las palabras clave existentes con las importadas.
   b. Configure si el detector de contenido debería coincidir con todas las palabras clave de la lista, con cualquier palabra clave de la lista o con un número personalizado de palabras clave.
7. En la esquina inferior derecha, haga clic en **Guardar**.

Patrón

Para crear un detector de contenido con un patrón

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Prevención de pérdida de datos** > **Clasificadores de datos**.
3. Haga clic en **Detectores de contenido**.
   Se abre la lista de detectores de contenido.
4. En la esquina superior derecha de la ventana, haga clic en **Agregar**.
5. En la lista desplegable, haga clic en **Patrón**.
6. Configure el detector de contenido.
   a. **Nombre**: especifique el nombre del grupo.
   b. **Descripción**: especifique una descripción para el grupo.
   c. **Expresión regular**: introduzca una expresión regular.
   d. **Validar**: comprobar la sintaxis de la expresión regular.
   e. **Comprobar ahora**: introduzca cadenas de prueba y vea el resultado. DLP admite la coloración en tiempo real de los resultados de la prueba. Se resaltan todas las coincidencias.

© Acronis International GmbH, 2003-2025

f. **Validación**: cuando se configura para realizar la validación, el grupo detecta una coincidencia solo en caso de que coincida con el tipo de validación seleccionado además de la expresión especificada. Para que coincida con el grupo, los datos deben coincidir con la expresión y además pasar la validación.
Si en este campo se selecciona **Sin validación**, el grupo no realiza la validación. Para que coincida el grupo en este caso, solo es necesario que los datos coincidan con la expresión especificada.
Para configurar la validación, seleccione el tipo deseado de la lista desplegable en este campo.

g. **Número mínimo de coincidencias**: introduzca el número de coincidencias que activarán la regla de inspección de contenido.

Importante
El detector comprueba si hay una coincidencia exacta no más allá del primer megabyte del contenido proporcionado para su inspección. Si el contenido supera 1 MB, la regla con la condición **Coincidencia exacta** no se activa incluso si el primer megabyte del contenido coincide con la expresión regular del detector.

h. **Distinguir mayúsculas y minúsculas**: cuando esta casilla de verificación está seleccionada, el grupo distingue entre caracteres en minúsculas y mayúsculas. Por ejemplo, las palabras `Term` y `term` se tratarán de forma diferente, por lo que se puede configurar el grupo para que coincida con la palabra `Term` pero no con `term`.
Cuando esta casilla de verificación está desactivada, el grupo no diferencia entre caracteres en mayúsculas y minúsculas. Por ejemplo, si `Term` coincide con el grupo, entonces `term` o incluso `tErM` también coincidirán.

i. **Contar coincidencias idénticas como una sola coincidencia**: combina las coincidencias duplicadas devueltas por la expresión regular en una sola coincidencia. Para ello, seleccione la casilla de verificación **Contar coincidencias idénticas como una sola coincidencia**.

7. En la esquina inferior derecha, haga clic en **Guardar**.

Complejo

Pasos para crear un detector de contenido complejo

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Protección** > **Prevención de pérdida de datos** > **Clasificadores de datos**.
3. Haga clic en **Detectores de contenido**.
Se abre la lista de detectores de contenido.
4. En la esquina superior derecha de la ventana, haga clic en **Agregar**.
5. En la lista desplegable, haga clic en **Complejo**.
6. Configure el detector de contenido.

© Acronis International GmbH, 2003-2025

El detector de contenido complejo le permite crear combinaciones lógicas de dos o más detectores de contenido. Puede examinar la base de datos de los detectores disponibles y combinarlos con los operadores lógicos AND, OR y NOT.

7. En la esquina inferior derecha, haga clic en **Guardar**.

En lugar de crear un nuevo detector de contenido desde cero, también puede clonar un detector de contenido integrado o personalizado existente y ajustar sus parámetros.

Para clonar un detector de contenido existente

1. En la lista de detectores de contenido, seleccione el que desea clonar y haga clic en **Clonar** en la lista desplegable al final de su fila.
2. Edite el detector de contenido clonado para añadir o eliminar parámetros según sea necesario y haga clic en **Listo** para guardar los cambios.

Nota
La clonación de un detector de contenido integrado crea un detector de contenido personalizado.

Mapa de la organización

Nota
Esta funcionalidad solo es accesible para los usuarios administradores de la empresa.

El mapa de la organización es una base de datos que contiene información para los usuarios y todas sus cuentas utilizadas para la transferencia de datos a través de mensajería instantánea, correo electrónico, u otros medios, que han sido interceptados por Advanced DLP.

El mapa de la organización proporciona medios para crear y gestionar grupos de usuarios en Advanced DLP, y para gestionar usuarios y cuentas asociadas a usuarios en Advanced DLP. Los grupos de usuarios pueden utilizarse entonces para la gestión de directivas de DLP basadas en grupos.

Para localizar el mapa de la Organización

- En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.

¿Cómo funciona?

Nota
El mapa de la organización se llena mientras el módulo Advanced DLP opera en modo de Observación.

Para cada transferencia de datos interceptada por el agente DLP, se recogen los siguientes atributos en el back-end.

© Acronis International GmbH, 2003-2025

Atributo	Descripción	Etiqueta en la interfaz de usuario
Unidad organizativa	Un grupo creado manualmente. La Unidad organizativa puede tener una o más Unidades organizativas anidadas.	Nombre del grupo, según se define
ID de seguridad	Un identificador de seguridad único.	En la página de detalles del usuario > **SID**
	Un nombre que se muestra fácil de usar derivado de los nombres de cuenta del usuario. Este nombre no siempre está disponible en el mapa de la organización.	**Nombre**
PC\NombreUsuario	El nombre del usuario del endpoint (recurso informático). Un nombre de usuario solo puede ser asignarse a una Unidad organizativa.	**Nombre de usuario**
Dispositivo (recurso informático)	El nombre del endpoint (recurso informático).	**Carga de trabajo**
Cuenta	Cuentas que fueron utilizadas por un usuario para la comunicación a través de mensajería instantánea y correo electrónico, y que han sido interceptadas por el agente DLP. Por ejemplo, si el agente detecta que el nombre de usuario "PC\John" usa john@gmail.com para enviar un correo electrónico, esta cuenta se vincula al nombre de usuario PC\John.	**Cuentas**

En el mapa de la organización, puede ver y buscar cuentas, usuarios y grupos, y crear, editar y eliminar grupos.

Para buscar cuentas específicas

Como parte de la investigación de un incidente, los usuarios administradores podrían tener que encontrar el propietario de una cuenta específica que estuvo involucrada en una posible violación de datos.

1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.
2. En el cuadro de texto **Buscar** que figura antes de la lista de usuarios, comience a escribir o pegue la cuenta.
   La lista se filtra a medida que se escribe.

Para buscar un nombre de usuario específico

© Acronis International GmbH, 2003-2025

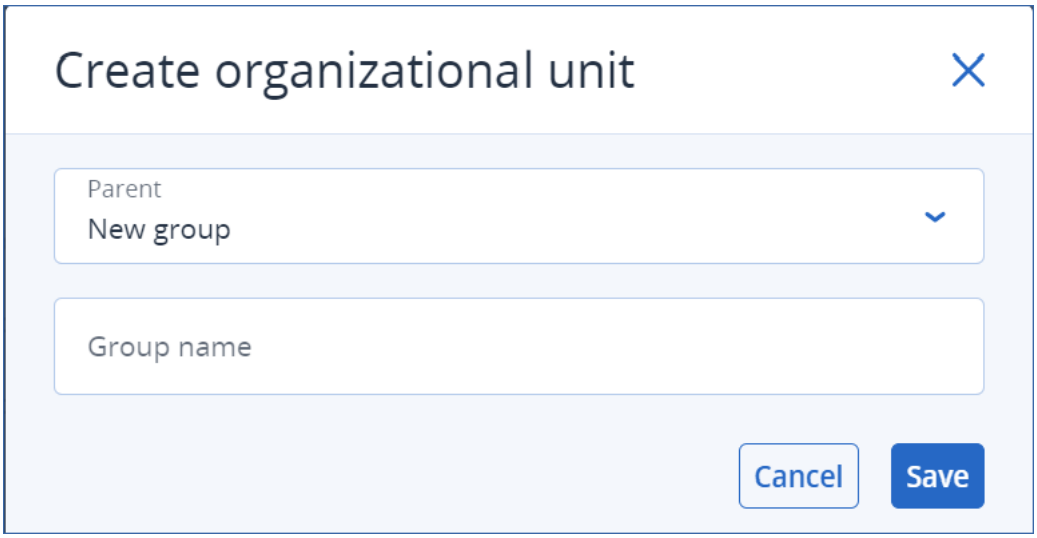
1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.
2. Para realizar una búsqueda en un grupo específico, haga clic en el nombre del grupo en la lista.
3. En el cuadro de texto **Buscar** que figura antes de la lista de usuarios, comience a escribir o pegue un nombre de usuario.
   La lista se filtra a medida que se escribe.

Para ver las cuentas utilizadas por un nombre de usuario en particular

1. Localice el usuario en la lista de usuarios.
2. Haga clic en los tres puntos al final de la fila del usuario y seleccione **Ver**.
3. En el diálogo de detalles del usuario, busque la sección **Cuentas asociadas**.
4. Puede añadir comentarios en el cuadro de texto de Descripción.

Para crear un grupo de usuarios

1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.
2. En la sección inferior izquierda de la lista de grupos, haga clic en **Crear grupo**.
   Se abre el diálogo para crear una unidad organizativa.



3. En el menú desplegable Principal, seleccione el contexto para el nuevo grupo.

   Nota
   No se puede cambiar la entidad principal más adelante. El grupo permanecerá anidado en este contexto.

4. Introduzca un nombre de grupo y haga clic en **Guardar**.

Para añadir un usuario a un grupo

1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.

© Acronis International GmbH, 2003-2025

2. En la lista de usuarios, localice el usuario que quiera añadir y seleccione la casilla de verificación al inicio de la fila del usuario.
   Los botones **Mover selección** y **Eliminar selección** aparecen sobre la lista de usuarios.

3. Haga clic en **Mover selección**.
   Se abre el cuadro de diálogo Mover usuario.
4. Seleccione la nueva entidad principal para el usuario seleccionado y haga clic en **Guardar**.

Nota
Un usuario solo puede pertenecer a un grupo.

Para eliminar una cuenta asociada a un usuario

1. Localice el usuario en la lista de usuarios.
2. Haga clic en los tres puntos al final de la fila del usuario y seleccione **Ver**.
3. En el diálogo de detalles del usuario, busque la sección **Cuentas asociadas**.
4. Localice la cuenta que quiera eliminar y haga clic en los tres puntos junto a ella.
5. En la lista desplegable, seleccione **Eliminar**.

Para cambiar el nombre de un grupo de usuarios

1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.
2. Haga clic en los tres puntos junto al nombre del grupo y haga clic en **Cambiar nombre**.

Pasos para eliminar un grupo de usuarios

1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.
2. Haga clic en los tres puntos junto al nombre del grupo y haga clic en **Eliminar**.
   Todos los usuarios del grupo se trasladan a la entidad principal.

Problemas conocidos y limitaciones

- [DEVLOCK-4028] No hay ningún control para los chats de grupo del agente de escritorio de Zoom.
- [DEVLOCK-4016] El nombre descriptivo y el ID del remitente no se capturan para GMX Web Mail y Web.de Mail cuando se crea el borrador.
- [DEVLOCK-4447] No hay ningún diálogo de Justificación para naver.com WebMail cuando se crea el borrador.
- [DEVLOCK-1033] DeviceLockDriver: posible comprobación de errores DRIVER_POWER_STATE_FAILURE causada por un interbloqueo durante el procesamiento de IRP_MN_QUERY_DEVICE_RELATIONS.

© Acronis International GmbH, 2003-2025

RMM

RMM es una colección de funciones que proporcionan un nivel avanzado de supervisión y administración para endpoints y licencias de Microsoft 365. Puede obtener más información, probar o solicitar una demostración aquí.

Para comprobar los requisitos de software de cada función, consulte la sección correspondiente.

- Para los endpoints, Acronis RMM proporciona las siguientes funciones:
  - **Inventario de software**: puede ver la lista completa del software que utilizan los clientes y ahorrar tiempo y esfuerzo en la preparación, la planificación y el seguimiento de las actualizaciones. Consulte "Gestión del inventario de software" (p. 1374).
  - **Despliegue de software mediante DeployPilot**: despliegue software de forma remota en sus recursos informáticos gestionados. Utilice planes de despliegue de software para automatizar el proceso de despliegue y garantizar que la distribución de software en las cargas de trabajo sea uniforme. Consulte "Gestión de software" (p. 1374).
  - **Administración de parches automatizada**: corrija las vulnerabilidades antes que las exploten. Consulte "Gestión de parches" (p. 1390).
  - **Aplicación de parches a prueba de fallos**: recupere las cargas de trabajo de los parches con errores de forma rápida y fácil realizando copias de seguridad del sistema automáticas antes de aplicar los parches. Consulte "Configuración de gestión de parches en el plan de protección" (p. 1391).
  - **Supervisión y alertas inteligentes basadas en el aprendizaje automático**: mitigue los riesgos operativos y optimice las tareas de supervisión con alertas y supervisión predictiva. Consulte "Supervisión de alertas" (p. 1555).
  - **Programación cibernética lista para su uso**: automatice y agilice las tareas rutinarias. Consulte "Secuencia de comandos cibernética" (p. 474).
  - **Supervisión del estado de la unidad**: utilice las alertas y la supervisión predictiva para reducir de forma proactiva el tiempo de inactividad que causan los fallos en las unidades. Consulte "Supervisión del estado del disco" (p. 336).
  - **Escritorio remoto y asistencia remota**: acceda a cargas de trabajo remotas y resuelva los problemas técnicos rápidamente. Ahorre tiempo y proporcione un soporte fiable con un rendimiento excelente, incluso con un ancho de banda limitado. La función incluye una mejor cobertura de plataformas (Windows, macOS y Linux) y funcionalidades ampliadas para grabaciones de sesiones, acciones remotas, transferencia de archivos, supervisión, generación de informes y observación de cargas de trabajo en vista múltiple. Consulte "Conexión a cargas de trabajo para asistencia o escritorio remotos" (p. 1441).
  - **Evaluación de vulnerabilidades de aplicaciones de Windows de terceros**: mejore la posición de seguridad de las aplicaciones de terceros de Windows al detectar y gestionar vulnerabilidades en 314 aplicaciones críticas, compatibles con una base de datos mantenida internamente por Acronis. Consulte "Productos de Microsoft y de terceros compatibles con la evaluación de vulnerabilidades" (p. 1380).

© Acronis International GmbH, 2003-2025

  - **Seguimiento de geolocalización**: vea la ubicación física en tiempo real de sus cargas de trabajo gestionadas. Consulte "Seguimiento de geolocalización" (p. 1495).
  - **Chat de asistencia**: utilice la herramienta de comunicación en tiempo real entre técnicos y usuarios remotos de cargas de trabajo en Windows y macOS gestionados para proporcionar una resolución de problemas más rápida y un mejor servicio de atención al cliente. Consulte "Chat de asistencia" (p. 1498).
- Para las licencias de Microsoft 365, Acronis RMM proporciona una auditoría continua de la posición de seguridad de Microsoft 365, con líneas base de las mejores prácticas y la corrección de las desviaciones de línea base. Dos modos de producto están disponibles cuando habilita el servicio de gestión de Microsoft 365:
  - **Gratuito**: permite la auditoría de la posición de seguridad de Microsoft 365 con líneas base de las mejores prácticas y la incorporación de usuarios. El modo gratuito está disponible en el conjunto de funciones de protección estándar.
  - **Avanzado**: incluye todas las funciones del modo gratuito y también permite la corrección automática de desviaciones de línea base de la posición de seguridad y la baja de usuarios.

Endpoint Detection and Response (EDR)

Nota
Esta funcionalidad forma parte del paquete de protección de Advanced Security + XDR, que a su vez forma parte del servicio de ciberprotección. Tenga en cuenta que, cuando añade la funcionalidad EDR a un plan de protección, puede estar sujeta a cargos adicionales.

La EDR detecta actividad sospechosa en la carga de trabajo, incluidos los ataques que han pasado desapercibidos. La EDR genera incidentes que proporcionan información general paso a paso de cada ataque, lo que le ayuda a entender cómo ocurrió un ataque y cómo impedir que vuelva a ocurrir. Gracias a las interpretaciones fáciles de entender de cada fase del ataque, el tiempo invertido en investigar ataques puede reducirse a unos pocos minutos.

A partir de C24.05, puede ampliar la funcionalidad de EDR con Extended Detection and Response (XDR). Utilice el gráfico XDR para obtener una perspectiva adicional y enriquecida de los incidentes de EDR al correlacionar las detecciones con los eventos de las fuentes de datos de XDR, que incluyen metadatos de correo electrónico y gestión de identidades. Para obtener más información, consulte "Extended Detection and Response (XDR)" (p. 1339).

Por qué necesita Endpoint Detection and Response (EDR)

En el actual mundo de las ciberamenazas y los ataques maliciosos en continua expansión, la prevención ya no garantiza el 100 % de la protección. Algunos ataques pueden producirse a través de capas de prevención y entrar con éxito en la red. Las soluciones convencionales no ven cuándo ocurre esto, lo que da a los atacantes manga ancha para profundizar en su entorno durante días, semanas o meses.

© Acronis International GmbH, 2003-2025

Las soluciones de EDR existentes le ayudan a prevenir estos «fallos silenciosos» al encontrar y eliminar a los atacantes rápidamente. Sin embargo, por lo general requieren un alto nivel de experiencia en seguridad o costosos analistas del Centro de operaciones de seguridad (SOC), y el análisis de incidentes puede llevar mucho tiempo.

La funcionalidad Advanced Security + EDR de Acronis supera estas limitaciones mediante la detección de ataques que no se han detectado, lo que le ayuda a entender cómo ocurrió un ataque y cómo impedir que vuelva a ocurrir. A cambio, se reduce el tiempo invertido en investigar ataques.

Estos son los motivos por los que necesita EDR:

- **Visibilidad completa**: Entienda qué ha ocurrido y cómo, incluso en el caso de ataques que hayan pasado desapercibidos. La evolución de cada ataque también se asigna de forma visual, paso por paso (desde el punto de entrada inicial hasta la visualización de los datos seleccionados o filtrados), lo que le permite comprender rápidamente el alcance y el impacto de un incidente. Para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285).
- **Minimice el tiempo de investigación**: Reduzca el tiempo de investigación de incidentes de horas a cuestión de minutos. La EDR detalla cada paso del ataque en un lenguaje humano claro y fácil de entender, lo que a su vez ayuda a reducir la necesidad de expertos costosos o personal adicional. Para obtener más información, consulte "Investigación de incidentes" (p. 1284)
- **Compruebe si hay amenazas conocidas en sus cargas de trabajo**: Puede buscar automáticamente en sus cargas de trabajo si hay amenazas de malware, vulnerabilidades y otros tipos de acontecimientos globales que puedan afectar a la protección de sus datos. A estas amenazas se las conoce como incidentes de compromiso (IOC), y se basan en los datos de amenazas recibidos del centro de operaciones de ciberprotección (CPOC). Para obtener más información, consulte "Busque indicadores de compromiso (IOC) de ataques conocidos públicamente en sus cargas de trabajo" (p. 1298).
- **Responda más rápido a incidentes**: Gracias al acceso a todas las actividades posteriores a la infracción y a un desglose de cada paso de la kill chain, puede ejecutar una serie de acciones para solucionar cada punto de ataque. Entre otros aspectos, puede investigar el uso del control remoto y la copia de seguridad forense (esta función no está disponible en la versión de acceso temprano), poner en cuarentena cargas de trabajo y acabar con procesos de malware. También puede recuperar operaciones comerciales con Disaster Recovery. Para obtener más información, consulte "Solución de incidentes" (p. 1302).
- **Informe de su postura de seguridad con confianza**: Con la EDR habilitada, podrá eliminar gran parte de la inseguridad y el miedo a las consecuencias que los ciberataques pueden tener en su empresa. Asimismo, la información relacionada con incidentes se almacena durante 180 días, lo que puede utilizarse con fines de auditoría.

Funciones

Endpoint Detection and Response (EDR) incluye las siguientes características:

© Acronis International GmbH, 2003-2025

- Recibir notificaciones de alerta cuando ocurra una infracción
- Gestionar los incidentes en la página Incidentes
- Visualización fácil de entender de la historia del ataque
- Recomendaciones y medidas de corrección
- Comprobar si hay ataques de dominio público en sus cargas de trabajo utilizando las fuentes de información sobre amenazas
- Información general a simple vista en el panel de control
- Almacenar los eventos de seguridad durante 180 días

Recibir notificaciones de alerta cuando ocurra una infracción

La EDR ofrece notificaciones de alerta cada vez que ocurre un incidente. Estas alertas están destacadas en el menú principal de la consola de Cyber Protect. Podrá investigar una alerta haciendo clic en el botón **Investigar incidente**, que le redirigirá a la pantalla de investigación del incidente (también conocida como cyber kill chain).

Para obtener más información, consulte "Revisar incidentes" (p. 1258).

Gestionar los incidentes en la página Incidentes

La EDR le permite gestionar todos los incidentes en la página Incidentes (se accede desde el menú **Protección** de la consola de Cyber Protect). Puede filtrar la información de la página **Incidentes** según sus requisito para entender rápido y fácilmente el estado actual de los incidentes, incluida la gravedad, la carga de trabajo afectada y el nivel de positividad. También puede ir directamente a la cyber kill chain para ver la historia del ataque, nodo a nodo.

Para obtener más información acerca de la página Incidentes, consulte "Revisar incidentes" (p. 1258).

Visualización fácil de entender de la historia del ataque

La EDR proporciona una representación visual de un ataque en un formato fácil de leer. Esto garantiza que incluso el personal que no sea de seguridad puede digerir los objetivos y la gravedad de cualquier ataque. En realidad, no es necesario ningún servicio del centro de operaciones de seguridad (SOC) ni contratar expertos de seguridad. La EDR le informa exactamente de cómo ha ocurrido un ataque, incluido:

- Cómo entró el atacante
- Cómo ocultó sus huellas el atacante
- Qué daño causó
- Cómo se propagó el ataque

Para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285).

© Acronis International GmbH, 2003-2025

Recomendaciones y medidas de corrección

La EDR proporciona recomendaciones claras y fáciles de implementar para resolver ataques en una carga de trabajo. Para resolver un ataque rápidamente, haga clic en el botón **Solucionar todo el incidente** para ver y seguir los pasos de las recomendaciones con el fin de mitigar el incidente. Estos pasos recomendados le permiten reanudar rápidamente las operaciones afectadas por un ataque. Sin embargo, si desea llevar a cabo más pasos para una solución granular, puede ir a cada nodo y solucionarlo con la acción que corresponda.

También puede hacer clic en **Copilot** para iniciar la herramienta de chat asistida por IA Copilot y enviar varias solicitudes y recibir acciones de respuesta sugeridas para el incidente seleccionado.

Para obtener más información, consulte "Solución de incidentes" (p. 1302).

Comprobar si hay ataques de dominio público en sus cargas de trabajo utilizando las fuentes de información sobre amenazas

La EDR incluye la capacidad de revisar los ataques conocidos existentes en las fuentes de información sobre amenazas de sus cargas de trabajo. Estas fuentes de información sobre amenazas se generan automáticamente según los datos sobre amenazas recibidos del centro de operaciones de ciberprotección (CPOC); la EDR le permite comprobar si una amenaza ha afectado a su carga de trabajo o no y llevar a cabo los pasos necesarios para anular la amenaza.

Para obtener más información, consulte "Busque indicadores de compromiso (IOC) de ataques conocidos públicamente en sus cargas de trabajo" (p. 1298).

Información general a simple vista en el panel de control

La EDR ofrece una serie de estadísticas en el panel de control de la consola de Cyber Protect. Puede ver:

- El estado actual de las amenazas, incluido el número de incidentes que deben investigarse.
- La evolución de los ataques por gravedad, indicando las posibles campañas de ataques.
- La tasa de eficiencia de cierre de incidentes.
- Las tácticas más específicas utilizadas para atacar a sus clientes.
- El estado de la red de la carga de trabajo, que indica si es aislada o conectada.

Almacenar los eventos de seguridad durante 180 días

La EDR recopila eventos de cargas de trabajo y aplicaciones y los almacena durante 180 días. Los eventos anteriores al período de 180 días se eliminan (la eliminación de eventos se basa en la antigüedad y no en el espacio de almacenamiento). Tenga en cuenta que aunque la EDR esté apagada, todos los eventos recopilados previamente para una carga de trabajo se conservan y estarán disponibles para la investigación de incidentes.

© Acronis International GmbH, 2003-2025

Requisitos de software para Endpoint Detection and Response

Endpoint Detection and Response (EDR) es compatible con los siguientes sistemas operativos:

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 y posterior
- Versiones 13, 14, 15 y 26 de macOS
- Versiones de SO Linux:
  - CentOS 7.x
  - Debian 10.x, 11.x
  - CloudLinux 7.x, 8.x
  - Ubuntu 16.04, 18.04, 20.04 y 22.04

Nota
Esta funcionalidad solo es compatible con las siguientes CPU, que soportan el conjunto de instrucciones de CPU SSE4.2:

- CPU de Intel después de 2011
- CPU de AMD después de 2012

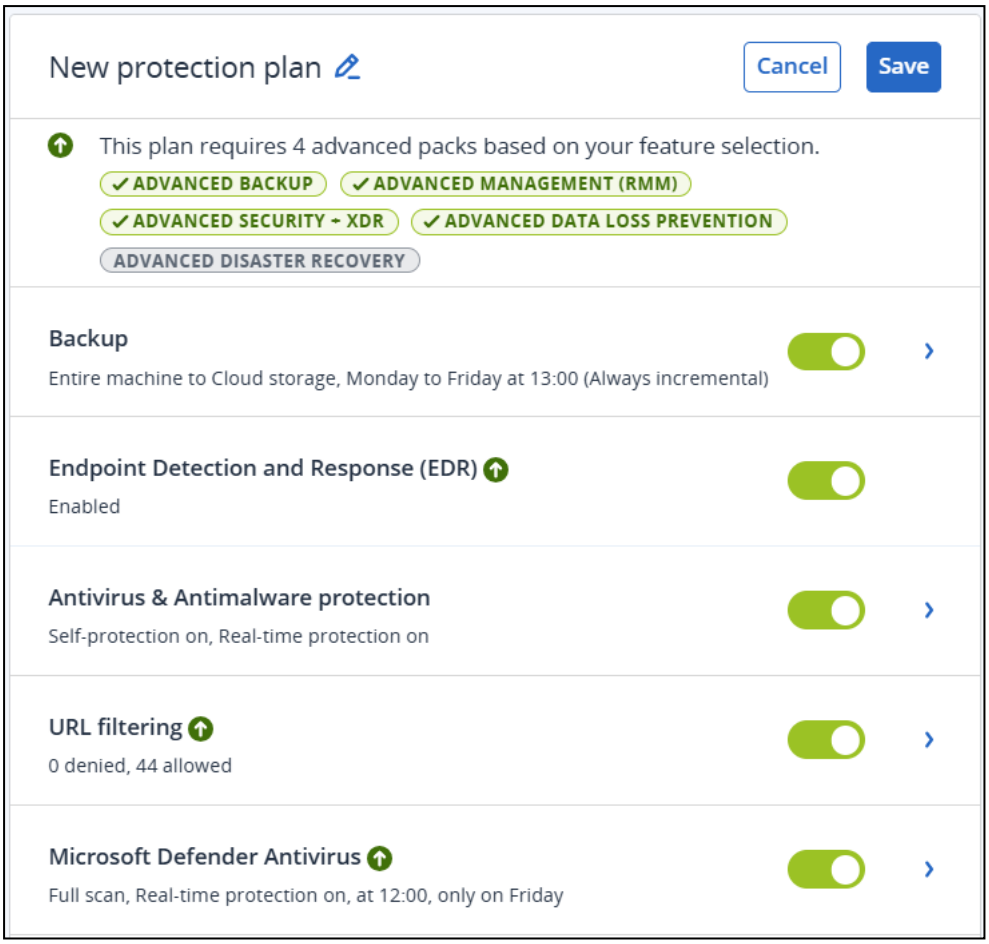
Habilitación de la funcionalidad Endpoint Detection and Response (EDR)

Puede habilitar la EDR en cualquier plan de protección.

Pasos para habilitar la EDR

1. En la consola de Cyber Protect, vaya a **Administración > Planes de protección**.
2. Seleccione el plan de protección correspondiente en la lista que se muestra y, en la barra lateral derecha, haga clic en **Editar**.
   De manera alternativa, puede crear un nuevo plan de protección y seguir con el siguiente paso.
   Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 249).
3. En la barra lateral del plan de protección, haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo de **Endpoint Detection and Response (EDR)**.

© Acronis International GmbH, 2003-2025



Tal y como se muestra a continuación, el icono del paquete **Advanced Security + XDR** se añadirá a la lista de paquetes de protección necesarios para la implementación del plan de protección, según los paquetes adicionales que seleccione.

✓ ADVANCED SECURITY + XDR

4. En el diálogo que se muestra, haga clic en **Habilitar**. Tenga en cuenta que puede habilitar EDR y, al mismo tiempo, deshabilitar cualquiera de las funciones antivirus y antimalware, Active Protection y filtrado de URL en el plan de protección.

© Acronis International GmbH, 2003-2025



© Acronis International GmbH, 2003-2025

Nota

Si habilita **Antivirus Microsoft Defender** para la protección en tiempo real, el módulo **Protección en tiempo real** se desactiva automáticamente para evitar que se produzcan conflictos. Las detecciones de virus/malware y la cuarentena son gestionadas por el Antivirus Microsoft Defender y cualquier incidente de EDR relacionado con detecciones de virus/malware se crea a partir de la información proporcionada por el Antivirus Microsoft Defender. EDR incluye otros motores de detección que pueden crear otros tipos de incidentes sin la intervención del Antivirus Microsoft Defender.

De forma similar, si habilita **Protección en tiempo real**, el módulo **Antivirus Microsoft Defender** se deshabilita automáticamente.

También se deben desactivar los ajustes de protección contra manipulaciones en Windows para garantizar que el Antivirus Microsoft Defender funcione correctamente en Cyber Protect Cloud. Para obtener más información, consulte este artículo de la base de conocimiento.

Además, si el **Motor de comportamiento** o la **Protección antivirus y antimalware** están deshabilitados en el plan de protección cuando EDR está habilitado, también estará deshabilitada la opción **Endpoint Detection and Response (EDR)**.

Cómo se utiliza Endpoint Detection and Response (EDR)

La EDR permite detectar ataques que no se han detectado, lo que le ayuda a entender cómo ocurrió un ataque y cómo prevenir que vuelva a ocurrir. Gracias a las interpretaciones fáciles de entender de cada fase del ataque, el tiempo invertido en investigar ataques puede reducirse a unos pocos minutos.

La siguiente tabla describe el flujo de trabajo general al trabajar con la EDR. De manera inicial, revisará y dará propiedad a cualquier incidente nuevo, los investigará más a fondo en la cyber kill chain y tomará las acciones de solución que correspondan.

Paso	Cómo usar la EDR
PASO 1: Revisar incidentes	En la lista de incidentes de la EDR: • Entender la postura en temas de seguridad de una organización: ¿cuántos incidentes deben investigarse? • Entender cuáles son los incidentes más graves y dar prioridad a su investigación según la gravedad. • Entender qué incidentes son nuevos y cuáles continúan.
PASO 2: Investigar incidentes	En la cyber kill chain de la EDR: • Entender los objetivos del atacante y ver las técnicas de ataque utilizadas. • Comprobar la probabilidad de que un incidente sea un ataque malicioso de verdad. • Comprobar si una fuente de información sobre amenazas está afectando a su carga de trabajo o no. • Ver qué acciones de respuesta se han aplicado ya a un incidente.

© Acronis International GmbH, 2003-2025

Paso	Cómo usar la EDR
PASO 3: Solucionar incidentes	En las secciones de solución pertinentes de la EDR: • Solucione fácil y rápidamente un incidente completo mediante la aplicación de acciones de respuesta globales. • Solucione los puntos de ataque individuales de un incidente. • Aplique acciones para evitar que el ataque (o los futuros ataques) se propague o afecte a cargas de trabajo que todavía no son objetivo del atacante.

Revisar incidentes

Endpoint Detection and Response (EDR) ofrece una lista de incidentes que incluye tanto la prevención (o malware) como detecciones sospechosas en una carga de trabajo. La lista de incidentes le ofrece información general en un vistazo rápido de los ataques o amenazas que afectan a sus cargas de trabajo, incluidas las amenazas que ya se han mitigado.

Desde la lista de incidentes, puede determinar rápidamente:

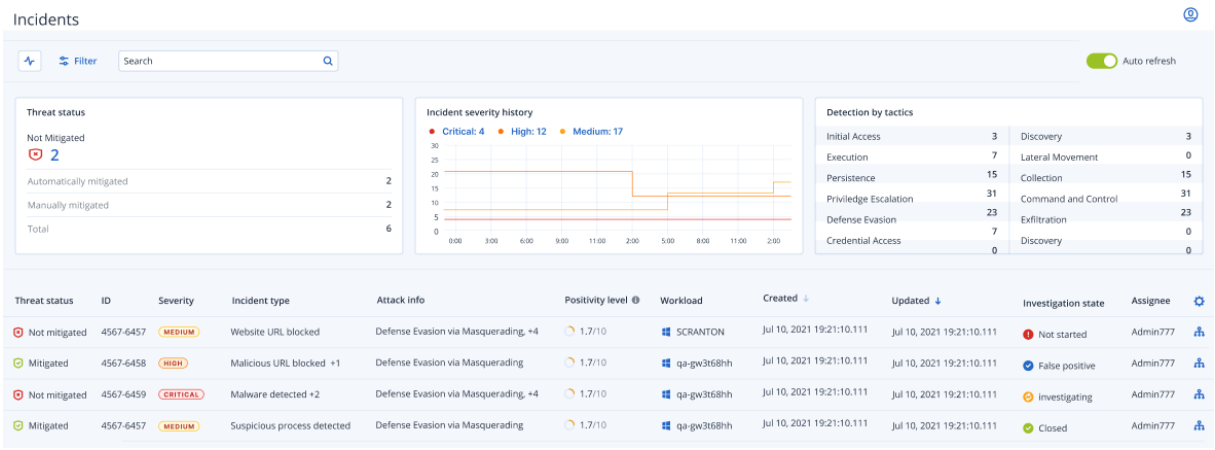
- La postura en temas de seguridad de una organización: ¿cuántos incidentes deben investigarse?
- Cuáles son los incidentes más graves y dar prioridad a su investigación según la gravedad.
- Qué incidentes son nuevos o están en curso.

Nota
Cuando inicia sesión como administrador de partners, puede ver todos los incidentes de EDR en una sola pantalla que consolida los incidentes de todos sus clientes, sin la necesidad de acceder a la vista de incidentes individuales de cada cliente. Se muestra una columna adicional de **Clientes**, que incluye el nombre del cliente al que pertenece cada incidente. Además, los widgets que se muestran en el panel de **Información general** muestran datos de métricas agregados de todos los clientes.

Según se muestra a continuación, se accede a la lista de incidentes desde el menú **Protección** de la consola de Cyber Protect. Para obtener más información sobre la revisión de incidentes en la lista, consulte " Ver qué incidentes no se han mitigado actualmente" (p. 1261) Para obtener más información acerca de cuándo se ha creado un incidente, consulte ¿Qué son exactamente los incidentes?

Nota
Si la detección y respuesta gestionadas (MDR) están habilitadas en sus cargas de trabajo, se muestra una columna adicional de **Ticket MDR**. Esta columna muestra el número de ticket proporcionado por el proveedor de MDR.

© Acronis International GmbH, 2003-2025



Nota
La consola de Cyber Protect debe estar abierta para que pueda recibir notificaciones sobre incidentes.

¿Qué son exactamente los incidentes?

Los incidentes, o los incidentes de seguridad, se pueden considerar *contenedores* de al menos un punto de prevención o detección sospechoso (o una mezcla), e incluyen todos los eventos y detecciones relacionados de un solo ataque. Estos incidentes de seguridad también pueden incluir eventos benignos adicionales que den más contexto a lo que ha pasado.

Esto le permite ver los eventos de ataque en un solo incidente y comprender los pasos lógicos que ha llevado a cabo el atacante. Asimismo, ayuda a acelerar el tiempo de investigación de un ataque.

Cuando la está habilitada en el plan de protección, se crean incidentes de seguridad cuando:

- **Una capa de prevención detiene algo:** El sistema cierra estos incidentes automáticamente, según la configuración del plan de protección. Sin embargo, puede investigar lo que hizo el malware exactamente antes de que se detuviese. Por ejemplo, el ransomware se detiene cuando empieza a cifrar archivos, pero, antes de eso, podría haber robado credenciales o instalado un servicio.
- **Actividad sospechosa detectada por la EDR:** Se trata de detecciones que deberían investigarse y solucionarse. Al revisar la cyber kill chain mejorada visualmente (para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285)), puede aplicar las soluciones pertinentes fácilmente.

Priorice qué incidentes necesitan atención inmediata

Se puede acceder a la lista de incidentes de la consola de Cyber Protect en cualquier momento desde el menú **Protección** de la consola de Cyber Protect. La lista de incidentes le ofrece información general en un vistazo rápido de los ataques o amenazas, lo que le permite priorizar los incidentes que requieren atención.

© Acronis International GmbH, 2003-2025

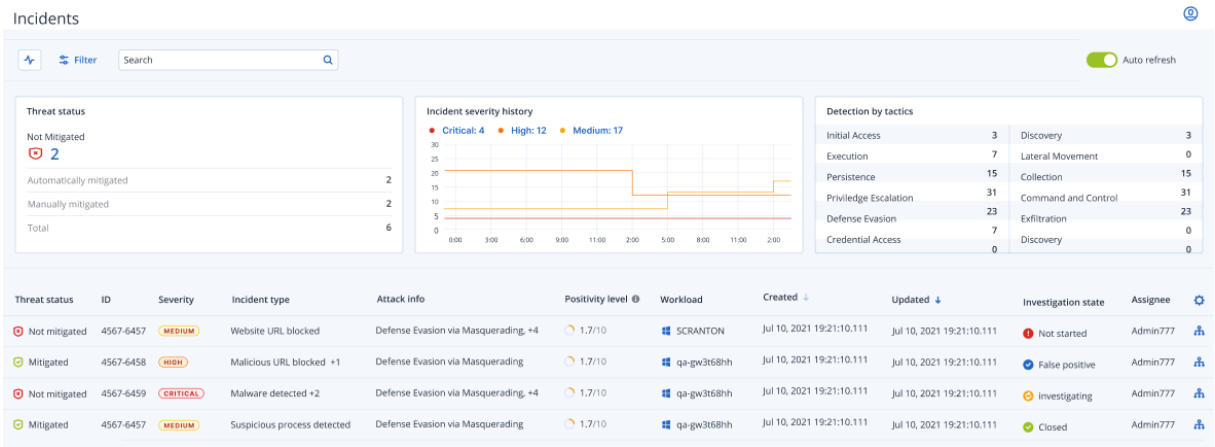
Importante
Para garantizar que sus cargas de trabajo siguen siendo seguras, analice y dé prioridad *siempre* los incidentes que están en progreso o no se han mitigado.

Cómo analizar qué incidentes de seguridad necesitan atención inmediata

La lista de incidentes le permite analizar y dar prioridad a los incidentes de la lista que requieren atención. Puede:

- Ver qué incidentes no se han mitigado actualmente: Conozca rápidamente a partir de la lista de incidentes si los ataques están en progreso actualmente. Los incidentes que no se hayan mitigado, según se indique en la columna **Estado de la amenaza**, deberían revisarse inmediatamente (de forma predeterminada, la lista de incidentes se filtra para mostrar dichos incidentes).
- Entienda el ámbito y el impacto de los incidentes: En función de su filtrado de ataques nuevos o en curso, entienda la gravedad de los incidentes filtrados, así como el impacto en su negocio.

Una vez que tenga una lista refinada de los incidentes más importantes, puede analizar la información de los incidentes para entender mejor un incidente específico, así como las técnicas utilizadas por el atacante para conseguir su objetivo. Para obtener más información, consulte "Analice la información sobre el incidente" (p. 1263).

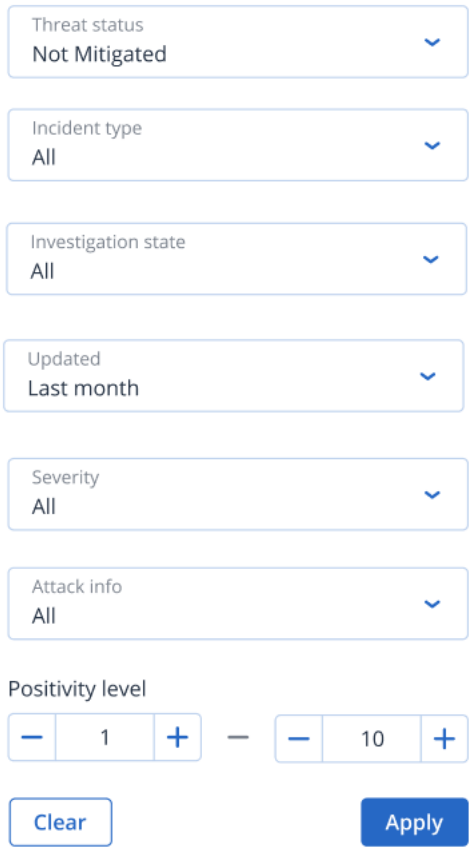


Nota
De forma predeterminada, la lista de incidentes se ordena según la columna **Actualizado**, que indica la fecha y hora en las que el incidente se actualizó por última vez con nuevas detecciones registradas dentro del incidente. Tenga en cuenta que los incidentes existentes se pueden actualizar en cualquier momento, incluso aunque se hayan cerrado previamente. También puede filtrar la lista para mostrar ataques recién abiertos o en curso según sus requisitos, tal y como se describe en el siguiente procedimiento.

Pasos para filtrar la lista de incidentes

© Acronis International GmbH, 2003-2025

1. Al principio de la lista de incidentes, haga clic en **Filtro** para filtrar la lista de incidentes que se muestra. Por ejemplo, si selecciona una fecha de inicio y finalización en el campo **Creado**, la lista de incidentes y los widgets mostrarán los incidentes que correspondan creados durante el periodo de tiempo definido.



2. Haga clic en **Aplicar** cuando haya finalizado.

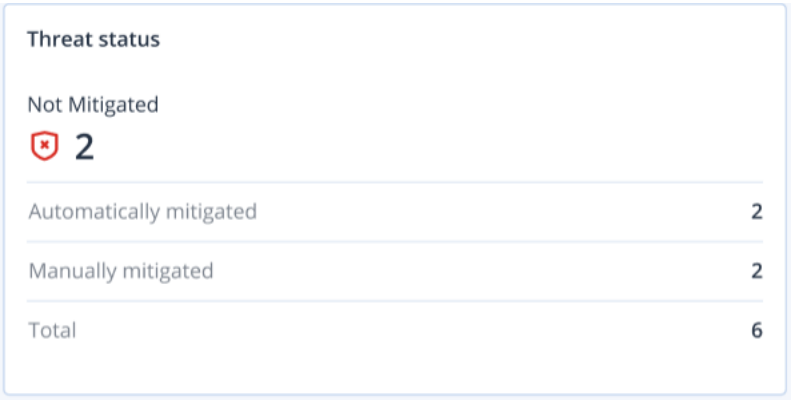
Ver qué incidentes no se han mitigado actualmente

Puede ver el actual estado de la amenaza para los incidentes en la columna **Estado de la amenaza**, que muestra si el incidente está **Mitigado** o **No mitigado**. La EDR define automáticamente el estado de la amenaza. Los incidentes con el estado No mitigado deben investigarse lo antes posible.

Puede refinar más la lista de incidentes mostrados mediante la aplicación de filtros. Por ejemplo, si desea filtrar la lista según el estado de la amenaza *y* un nivel de gravedad específico, seleccione las opciones de filtro que apliquen. Cuando haya filtrado los incidentes que le interesen, puede investigarlos, según se describe en "Investigación de incidentes" (p. 1284).

También puede utilizar el widget **Estado de la amenaza**, como se muestra a continuación, para ver un resumen rápido a simple vista del estado actual de las amenazas. Tenga en cuenta que los datos que se muestran en este widget reflejan los filtros que ha aplicado; consulte " Pasos para filtrar la lista de incidentes" (p. 1260).

© Acronis International GmbH, 2003-2025



Entender el ámbito y el impacto de los incidentes

Puede entender rápidamente el ámbito y el impacto de los incidentes mediante la revisión de las columnas **Gravedad**, **Información del ataque** y **Nivel de positividad**. Como se menciona más arriba, después de determinar qué incidentes se encuentran en progreso actualmente, puede filtrarlos por estas columnas adicionales para hacer lo siguiente:

- Revisar qué incidentes son más graves en la columna **Gravedad**. La gravedad se un incidente puede ser **Crítica**, **Alta** o **Media**.
  - **Crítico**: Existe un grave riesgo de actividad cibernética maliciosa con el riesgo de comprometer hosts críticos en su entorno.
  - **Alto**: Existe un alto riesgo de actividad cibernética maliciosa con el riesgo de daño grave a su entorno.
  - **Medio**: Existe un mayor riesgo de actividad cibernética maliciosa.

  Nota
  Al determinar la gravedad, el algoritmo de la EDR tiene en cuenta el tipo de carga de trabajo, así como el ámbito de cada paso del ataque. Por ejemplo, un incidente que incluye pasos relacionados con el robo de credenciales se establece como **Crítico**.

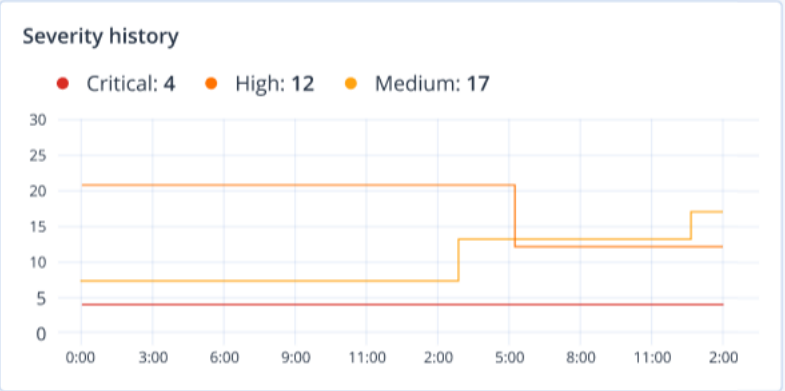
- Obtenga información sobre por qué se creó un incidente en la columna **Tipo de incidente**. El tipo de incidente puede incluir uno o más de los siguientes:
  - **Ransomware detectado**
  - **Malware detectado**
  - **Proceso sospechoso detectado**
  - **Proceso malicioso detectado**
  - **URL sospechosa bloqueada**
  - **URL maliciosa bloqueada**
- Determine qué técnicas de ataque se utilizan en la columna **Información del ataque** y conozca si hay un tema o modelo común para los ataques.

© Acronis International GmbH, 2003-2025

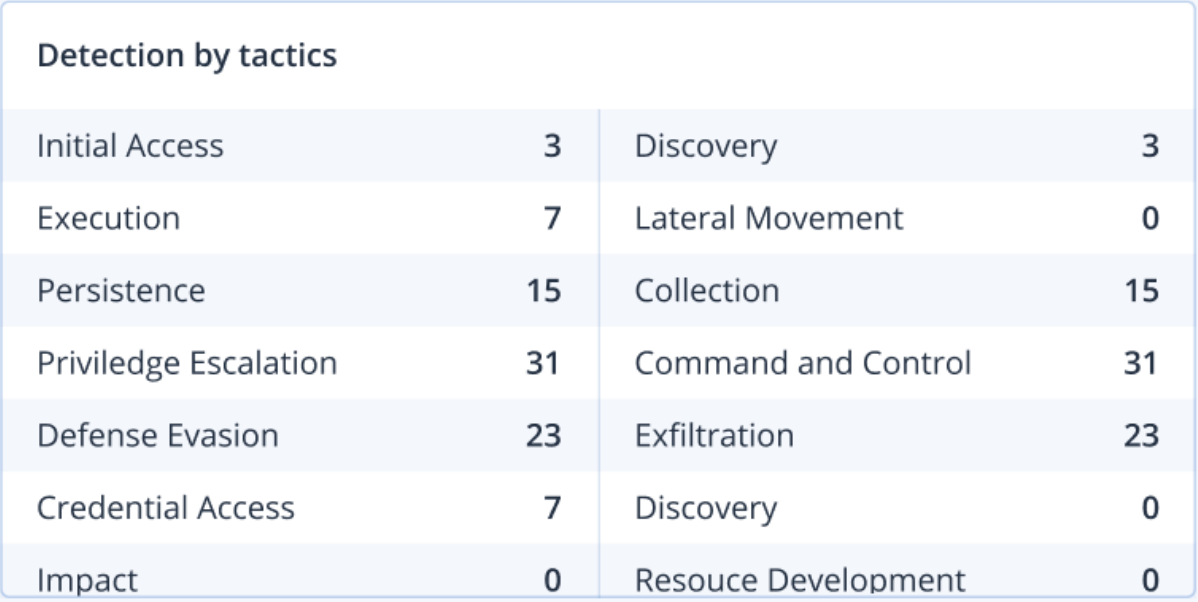
- Confirme la probabilidad de que un incidente sea un ataque malicioso de verdad. La columna **Nivel de positividad** incluye una puntuación del 1 al 10 (cuanto más alta es la puntuación, más probable es que el ataque sea malicioso de verdad).

Cuando haya encontrado los incidentes que necesiten atención inmediata, puede investigarlos, según se describe en "Investigación de incidentes" (p. 1284)

También puede utilizar los widgets **Historial de gravedad** y **Detección por tácticas** para ver un resumen rápido a simple vista de la gravedad y de las técnicas de ataque.



El widget **Detección por tácticas** muestra las distintas técnicas de ataque utilizadas, con valores en verde o rojo que indica el aumento o la disminución con respecto al rango de tiempo especificado anteriormente. Este widget ofrece una visión agregada de todos los objetivos de los incidentes filtrados, lo que le proporciona un resumen rápido del impacto en sus clientes.



Analice la información sobre el incidente

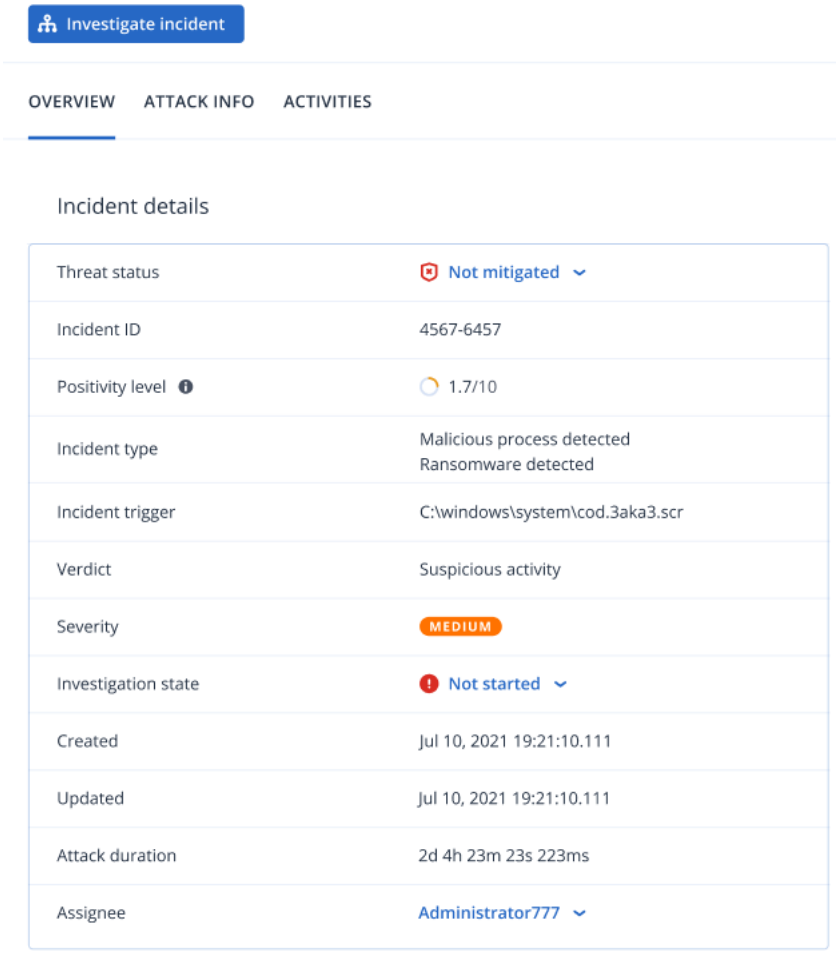
Durante la fase de revisión del incidente, también puede analizar la información de dicho incidente desde la lista de incidentes de Endpoint Detection and Response (EDR). Esta información le permite

© Acronis International GmbH, 2003-2025

profundizar en todo el incidente y entender cómo y cuándo ocurrió. Además, puede asignar un incidente a usuarios específicos para investigarlo y establecer el estado de la investigación.

Pasos para analizar la información sobre el incidente

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**. Se mostrará la lista del incidente.
2. Haga clic en el incidente que desea revisar. Se mostrarán los detalles para el incidente seleccionado.
3. En la pestaña **Información general**, puede revisar la información del incidente y la carga de trabajo, incluido el estado actual de la amenaza y la gravedad. También puede definir el **Estado de la investigación** (seleccionar entre **Investigando**, **Sin iniciar** (el estado predeterminado), **Falso positivo** o **Cerrada**) y seleccionar un usuario al que asignar el incidente (en la lista desplegable **Cesionario**, seleccione el usuario que corresponda).



4. Haga clic en la pestaña **Información del ataque** para revisar la información del ataque y las técnicas utilizadas en este. Haga clic junto a cada técnica de ataque que aparezca en la lista para revisar más información sobre la técnica en MITRE.org.
5. Haga clic en la pestaña **Actividades** para revisar las acciones llevadas a cabo en la cyber kill chain con el fin de mitigar un incidente. Para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285).

© Acronis International GmbH, 2003-2025

Por ejemplo, si se ha ejecutado un parche en la carga de trabajo, puede ver quién inició el parché, cuánto tardó y los errores que ocurrieron durante la implementación del mismo.

6. Haga clic en **Investigar incidente** para acceder a la cyber kill chain e investigar el incidente nodo por nodo. Para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285).

Buscar indicadores de compromiso (IoC) y actividades sospechosas

Nota
Esta función es parte del programa de acceso anticipado. Algunas de las funcionalidades y descripciones pueden estar incompletas.

Para detectar y mitigar amenazas antes de que se conviertan en incidentes de alto impacto, utilice la función **Búsqueda de eventos**. Esta función le permite buscar IoC y actividades sospechosas en todas las cargas de trabajo habilitadas con Endpoint Detection and Response (EDR).

Utilice la función **Búsqueda de eventos** para:

- Ejecutar consultas personalizadas en los datos de eventos recopilados de todas las cargas de trabajo para buscar hashes. Como alternativa, puede obtener métricas para responder a determinadas preguntas (por ejemplo, mostrar cargas de trabajo con un número inusualmente alto de procesos).
- Filtrar consultas mediante atributos proporcionados por los endpoints EDR y datos de otras integraciones, como actividades del sistema operativo, actividades del usuario y actividades de la red.
- Vea un resumen intuitivo de los datos basado en sus consultas para ayudarle en la investigación de incidentes o en la búsqueda de amenazas.
- Guarde y comparta consultas con usuarios de la misma organización.

La función **búsqueda de eventos** se accede desde el menú **Protección** en la consola de Cyber Protect.

Nota
El período de retención predeterminado para los resultados de búsqueda de eventos EDR es de siete días.

Búsqueda de eventos

Nota
Esta función es parte del programa de acceso anticipado. Algunas de las funcionalidades y descripciones pueden estar incompletas.

Puede buscar eventos de Endpoint Detection and Response (EDR) en todas las cargas de trabajo protegidas por EDR.

© Acronis International GmbH, 2003-2025

Tenga en cuenta que, cuando utiliza la consola de Cyber Protect en el nivel del inquilino de partner **(todos los clientes)**, puede buscar eventos de todos sus clientes gestionados. Si está trabajando en el nivel del inquilino del cliente, puede buscar eventos específicos del cliente seleccionado.

Para buscar eventos

1. En la consola de Cyber Protect, vaya a **Protección** > **Búsqueda de eventos**.
2. Indique su consulta de búsqueda utilizando el lenguaje de consulta XDR de Acronis (XQL), y defina un intervalo de tiempo.

   Tenga en cuenta que XQL utiliza el autocompletado para ayudarlo a crear una consulta. Para obtener más información sobre la sintaxis y las opciones de consulta disponibles, consulte "Sintaxis" (p. 1271).

   Al crear la consulta, también están disponibles las siguientes operaciones de teclado:

   - Presione **Intro** para enviar el cursor a la siguiente línea. El carácter "|" también se añade al inicio de la nueva línea (lo que ayuda al escribir consultas en varias etapas).
   - Pulse **Mayús + Intro** para enviar el cursor a la siguiente línea.

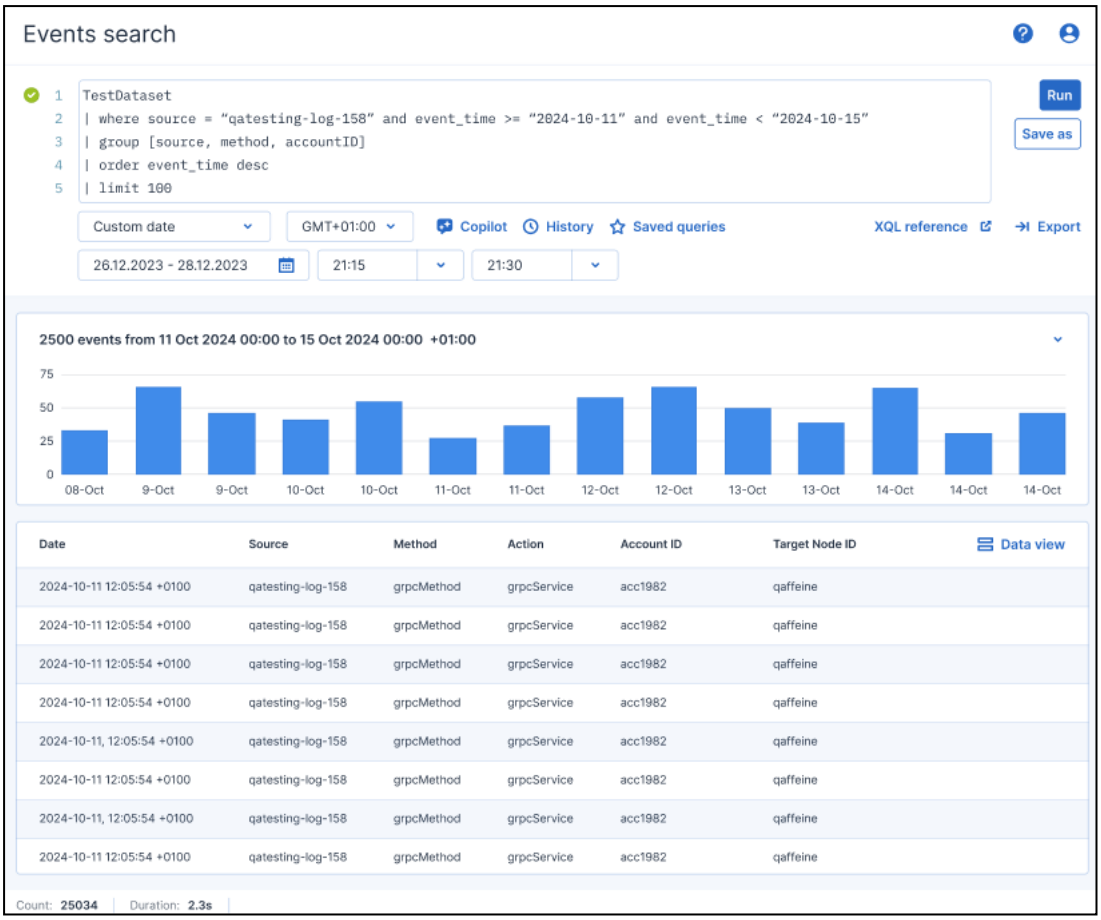
   Nota
   Para utilizar una de las últimas diez consultas ejecutadas, haga clic en **Historial** y seleccione la consulta correspondiente. El campo de consulta de búsqueda se rellenará automáticamente con la consulta. Para obtener más información, consulte "Cómo trabajar con consultas guardadas" (p. 1269).

3. Haga clic en **Ejecutar** para ejecutar la consulta.

   También puede pulsar **Ctrl+Intro** para ejecutar la consulta.

   Se muestran los resultados de la consulta. Para obtener más información, consulte "Cómo agregar o quitar columnas en la vista de diseño de tabla" (p. 1268).

© Acronis International GmbH, 2003-2025



4. Afine su consulta de búsqueda según sea necesario. Por ejemplo, elija mostrar campos o eventos específicos que contengan un determinado nombre de archivo.
5. [Opcional] Para guardar la consulta actual, haga clic en **Guardar como**. Para obtener más información, consulte "Cómo trabajar con consultas guardadas" (p. 1269).

Visualización y comprensión de los resultados de la consulta

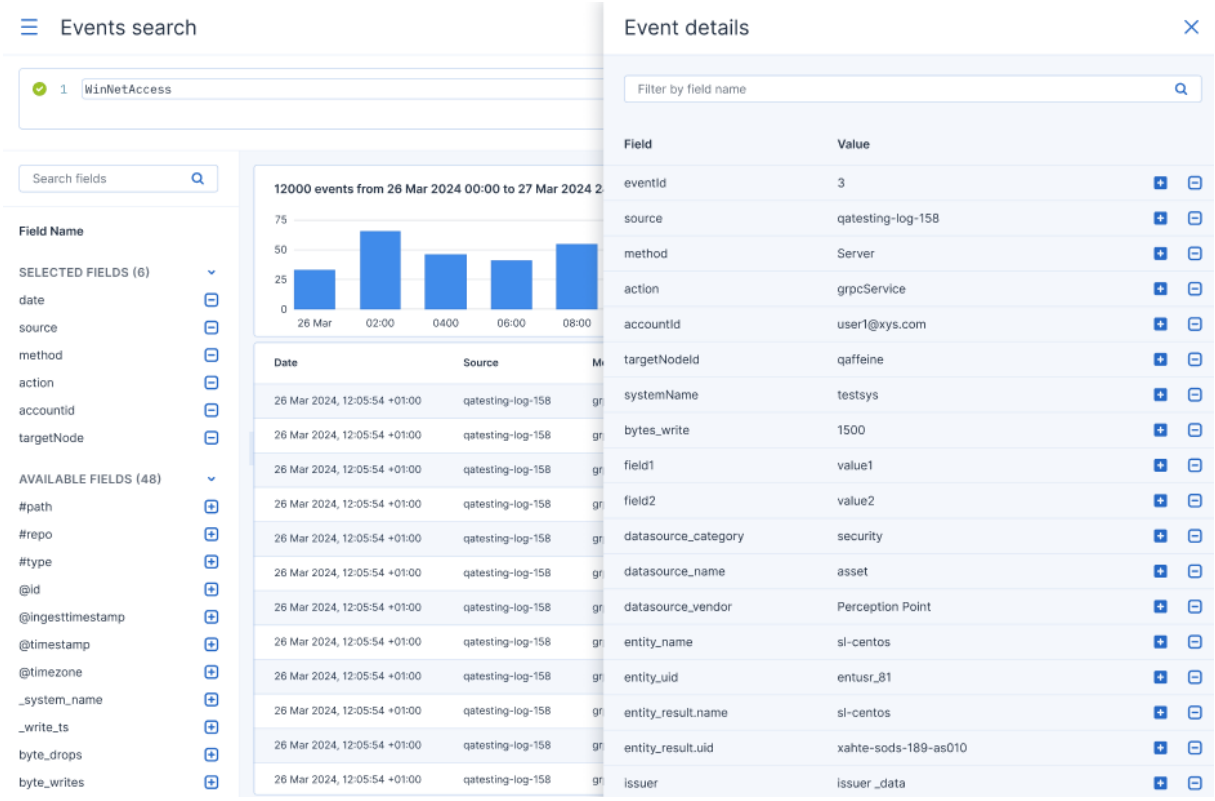
Nota
Esta función es parte del programa de acceso anticipado. Algunas de las funcionalidades y descripciones pueden estar incompletas.

Cuando haya definido y ejecutado su consulta de búsqueda (consulte "Búsqueda de eventos" (p. 1265)), los resultados se mostrarán debajo del cuadro de consulta de búsqueda en una vista de diseño de tabla. Desde esta vista, puede:

- Ver todos los eventos del período seleccionado.
- Hacer clic en una fila de evento para ver los detalles de un evento en concreto.
- Agregar o quitar columnas que se muestran en los resultados de la consulta. Consulte "Cómo agregar o quitar columnas en la vista de diseño de tabla" (p. 1268).
- Cambiar a la **Vista de datos**, que muestra todos los datos del evento en formato JSON.

© Acronis International GmbH, 2003-2025

- Pase el ratón por encima de una columna en el gráfico de barras para ver la fecha, la zona horaria, el recuento y la duración de los eventos.



Cómo agregar o quitar columnas en la vista de diseño de tabla

En la vista de diseño de tabla, hay tres maneras de añadir o eliminar las columnas que se muestran en los resultados de la consulta:

- En el panel **Nombre del campo**, haga clic en junto al nombre del campo correspondiente (en la sección **Campos disponibles**) para agregar ese campo como columna en los resultados de la consulta.

  Para eliminar una columna, haga clic en junto al nombre del campo correspondiente (en la sección **Campos seleccionados**).
- Haga clic en un evento para mostrar el panel **Detalles del evento** y, a continuación, haga clic en o para añadir o eliminar el campo correspondiente de los resultados de la consulta de búsqueda.
- Pase el ratón sobre una columna para mostrar un icono en forma de X. Haga clic en el icono para eliminar la columna.

Si incluye el operador `Column` en la consulta, solo se muestran los campos especificados por el operador `Column` en la vista de diseño de la tabla. Puede seguir añadiendo o eliminando campos a través del panel **Campos**.

© Acronis International GmbH, 2003-2025

Si la consulta no incluye el operador `Column`, los resultados se muestran de forma predeterminada en el diseño de **Vista de datos** (en formato JSON). Sin embargo, puede hacer clic en **Vista de tabla** para cambiar de vista o agregar campos a través del panel **Campos** para cambiar automáticamente a la **Vista de tabla** y que solo se muestren los campos seleccionados.

Para obtener más información sobre el operador `Column` y otros elementos XQL, consulte "Sintaxis" (p. 1271).

Nota
Después de agregar o eliminar columnas a través del panel **Detalles del evento** o el panel **Campos**, la consulta se ejecuta automáticamente de nuevo.

Cómo trabajar con consultas guardadas

Nota
Esta función es parte del programa de acceso anticipado. Algunas de las funcionalidades y descripciones pueden estar incompletas.

La función de **Búsqueda de eventos** le permite guardar, reutilizar y actualizar las consultas según sea necesario. Puede:

- Guardar una nueva consulta
- Ejecutar una consulta guardada previamente
- Actualizar una consulta guardada
- Eliminar una consulta

Pasos para guardar una nueva consulta

1. En la consola de Cyber Protect, vaya a **Protección** > **Búsqueda de eventos**.
2. Defina su consulta en el cuadro de consulta de búsqueda. Para obtener más información sobre la sintaxis y las opciones de consulta disponibles, consulte "Sintaxis" (p. 1271).
3. Haga clic en **Guardar como**.
4. En el diálogo **Guardar nueva consulta**, defina lo siguiente:
   - Introduzca un nombre de la consulta único y (de forma opcional) añada una descripción.
   - Seleccione la casilla de verificación **Guardar filtro de tiempo** para asegurarse de que el filtro de tiempo definido se incluya en la consulta.
   - Seleccione la casilla de verificación **Permitir que otros usuarios utilicen esta consulta** para asegurarse de que otros usuarios dentro del mismo inquilino de cliente puedan utilizar la consulta. Si esta casilla de verificación no está seleccionada, solo el administrador, el administrador de la empresa y el usuario que creó la consulta pueden utilizarla.
5. Haga clic en **Guardar**.

   Cuando guarde una consulta, se guardará únicamente la parte de texto de la consulta y el rango de tiempo seleccionado.

© Acronis International GmbH, 2003-2025

Nota
Se pueden guardar un máximo de 300 consultas por cuenta de inquilino de cliente. Cuando se alcanza este límite, la próxima vez que guarde una consulta, se le pedirá que elimine una ya guardada antes de almacenar la nueva.

Pasos para ejecutar una consulta guardada previamente

1. En el cuadro de búsqueda de consultas, haga clic en **Consultas guardadas**.
2. En la lista de consultas guardadas que se muestra, haga clic en la consulta correspondiente.
   La consulta se agrega al cuadro de consulta de búsqueda y se ejecuta automáticamente.

Pasos para actualizar una consulta guardada

1. En el cuadro de búsqueda de consultas, haga clic en **Consultas guardadas**.
2. En la lista de consultas guardadas que se muestra, pase el ratón sobre la consulta que desea actualizar y haga clic en el icono del lápiz.
3. Realice los cambios necesarios en la consulta y luego haga clic en **Guardar**.
   Para obtener más información sobre los campos editables, consulte Guardar una nueva consulta.
4. [Opcional] Haga clic en la consulta guardada para ejecutarla.

Pasos para eliminar una consulta

1. En el cuadro de búsqueda de consultas, haga clic en **Consultas guardadas**.
2. En la lista de consultas guardadas, pase el ratón sobre la consulta que desea eliminar y haga clic en el icono de la papelera.
3. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

Lenguaje de consulta XDR de Acronis (XQL)

Nota
Esta función es parte del programa de acceso anticipado. Algunas de las funcionalidades y descripciones pueden estar incompletas.

Utilice XQL para buscar eventos de Endpoint Detection and Response (EDR) y luego profundice en los eventos que está buscando. Esta sección enumera los diversos elementos de XQL con los que debería estar familiarizado al buscar eventos EDR:

- Sintaxis (incluyendo consultas de muestra)
- Tipos de eventos y campos

Para obtener más información sobre cómo usar la función de **Búsqueda de eventos**, consulte "Buscar indicadores de compromiso (IoC) y actividades sospechosas" (p. 1265).

© Acronis International GmbH, 2003-2025

Sintaxis

Operación	Ejemplo

Selección de fuente de datos y columnas
 	
Selecciona la fuente de datos y columnas sobre las que operará la consulta. Este operador debe ser el primer operador en la consulta. Las consultas para seleccionar fuentes de datos y columnas no distinguen entre mayúsculas y minúsculas.
	`eventType`
	
	`eventType | where column = 'string'`

Filtrado de datos
 	
Filtra datos basados en condiciones, y debe comenzar con la palabra clave `where`.
 	
Tenga en cuenta las siguientes opciones de filtrado:
• Las cadenas pueden estar encerradas entre comillas simples o dobles.
• Las búsquedas de columnas distinguen entre mayúsculas y minúsculas de manera predeterminada. Para realizar una comprobación de igualdad, las búsquedas pueden realizarse de modo que no distingan entre mayúsculas y minúsculas con "~=":
`eventType | where column = 'String'` distingue entre mayúsculas y minúsculas y solo coincidirá con `'String'`.
`eventType | where column ~= 'String'` no distingue entre mayúsculas y minúsculas y coincidirá con todos los casos de `'string'`.
• Los operadores lógicos como `AND` y `OR` se pueden usar para combinar los filtros.
`key = value AND key < value OR key = value`
• Se pueden añadir paréntesis alrededor de los operadores:
`(key = value) AND (key < value OR key = value)`
• Utilice `CONTAINS` para la coincidencia parcial de cadenas:
`key CONTAINS 'value'`
• Cuando realice una Búsqueda en varias columnas, `CONTAINS` puede incluir elementos individuales o una lista de elementos:
`CONTAINS 'String'`
`CONTAINS ('String1', 'String2', 'String3')`
• Utilice `ICONTAINS` para la coincidencia parcial de cadenas sin distinción de mayúsculas y minúsculas:
`key ICONTAINS 'value'`
• Utilice `IN` para verificar la pertenencia (distingue entre mayúsculas y minúsculas):
`key IN ('value1', 'value2')`
	`eventType | where field == 'value'`
	
	`eventType | where field != 'value'`
	
	`eventType | where field > 'value'`
	
	`eventType | where field < 'value'`
	
	`eventType | where field >= 'value'`
	
	`eventType | where field <= 'value'`
	
	`eventType | where field CONTAINS 'substring'`
	
	`eventType | where field NOT CONTAINS 'substring'`
	
	`eventType | where field ICONTAINS 'substring'`
	
	`eventType | where column ICONTAINS 'substring'`
	
	`eventType | where field NOT ICONTAINS 'substring'`
	
	`eventType | where column NOT ICONTAINS 'substring'`
	
	`eventType | where field IN ('value1', 'value2')`
	
	`eventType | where column IIN ('value1'. 'value2')`
	
	`eventType | where field NOT IN`

© Acronis International GmbH, 2003-2025

Operación	Ejemplo

• Utilice IIN para verificar la pertenencia (no distingue entre mayúsculas y minúsculas):
`key IIN ('value1', 'value2')`
• Use `ago` para filtrar fechas. Esta sintaxis solo acepta un valor numérico seguido de días (d), horas (h), minutos (m) o segundos (s):
`column < ago(3d)`
`column < ago(3h)`
`column < ago(3m)`
`column < ago(30s)`
• Utiliza la coincidencia de regex de acuerdo con el estándar RE2:
`key MATCHES 'regex string'`
	`('value1', 'value2')`
	`eventType | where field MATCHES 'value1*'`
	`eventType | where field NOT MATCHES 'value1*'`
	`eventType | where event_time > ago(5d)`

Selección de campos Especifica qué campos seleccionar y devolver de una consulta.	`eventType | columns field1, field2, field3 ...`

Clasificación
Ordena los resultados de la consulta, que pueden ser ascendentes o descendentes. Si no se especifica un orden, el orden predeterminado es ascendente.
	`eventType | order field1, field2, field3 ...`
	`eventType | order field asc`
	`eventType | order field desc`

Búsqueda en columnas Realiza la búsqueda de una cadena en todas las columnas de una tabla.	`eventType | search 'query string'`
Límite Limita el resultado de la consulta.	`eventType | limit 10` `eventType | limit 1000 | group [field1, field2] | limit 10`

Operación de grupo
Realiza una `group operation` en los datos.
(Opcional) Puede especificar funciones de agregación que se deben realizar en los campos agregados, o solo especificar funciones de agregación sin realizar `group operation` en campos específicos.
	`eventType | group [field]`
	`eventType | group [field1, field2, field3, ...]`
	`eventType | group with [max (field1), min(field2), avg (field3)]`
	`eventType | group [field1, field2, field3, ...] with [max (field1), min(field2), avg (field3)]`
	`eventType | group [field1, field2, field3, ...] with [max (field1) as max_field, min`

© Acronis International GmbH, 2003-2025

Operación	Ejemplo
	`(field2), avg(field3) as avg_field]`

Agregación
Agrega los resultados de la consulta para realizar una operación.
Estas funciones solo pueden usarse junto con `group operation` (ver arriba).
	`min(field)`
	`max(field)`
	`avg(field)`
	`count()`
	`count(field)`
	`countdistinct(field)`

Nota
Habitualmente, en lenguajes de programación se usa "==" para declarar condiciones y "=" para asignar valores.

Con Acronis XDR Query Language, solo puede declarar condiciones y puede usar "=" y "==" indistintamente.

Consultas de muestra

Esta sección incluye una serie de consultas de ejemplo para ilustrar cómo puede aplicar las reglas de sintaxis de XQL a su consulta.

- Selección de campos del tipo de evento `WinProcCreate`:

```
WinProcCreate | columns host_name, parent_start, parent_gpid, parent_pid, parent_
user, proc_name
```

- Filtrado con condiciones, antes de agrupar los resultados por `proc_name`, y aplicación de funciones de agregación `min()` en `parent_pid`:

```
WinProcCreate | where host_name == 'BNi-Kub' AND parent_pid != -1 AND proc_name
CONTAINS '1' AND host_name IN ('Computer1') | group [proc_name] with [min(parent_
pid)]
```

- Selección de datos con filtros, luego recuento del número de filas devueltas y establecimiento de orden:

© Acronis International GmbH, 2003-2025

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [count() as new_count] |
order new_count
```

- Selección de datos con filtros regex:

```
WinProcCreate | where host_name matches 'BNi.*'
```

- Selección de datos con filtros complejos y límite de los resultados:

```
WinProcCreate | where (host_name contains 'BNi-Kub') OR (host_name in
('Computer1', 'Computer2')) | limit 10
```

- Selección de datos con filtros, luego recuento de número distinto de filas devueltas:

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [countdistinct(*)]
```

- Selección de datos con filtros, orden por un campo y límite de número de filas devueltas:

```
WinProcCreate | where host_name == 'BNi-Kub' | order host_name | limit 10
```

Tipos de eventos y campos

Esta sección incluye:

- Tipos de eventos
- Tipos de datos de muestra
- Campos de eventos

Tipos de eventos

Nombre	Descripción	Tipo
WinProcCreate Para obtener más información sobre los	Eventos de creación de procesos de Windows	Eventos

© Acronis International GmbH, 2003-2025

Nombre	Descripción	Tipo
campos disponibles, consulte WinProcCreate.		
WinProcTerminate Para obtener más información sobre los campos disponibles, consulte WinProcTerminate.	Eventos de terminación de procesos de Windows	Eventos
WinNetAccess Para obtener más información sobre los campos disponibles, consulte WinNetAccess.	Eventos de acceso a la red de Windows	Eventos
WinRegAccess Para obtener más información sobre los campos disponibles, consulte WinRegAccess.	Eventos de acceso al registro de Windows	Eventos
WinScriptExec Para obtener más información sobre los campos disponibles, consulte WinScriptExec.	Eventos de ejecución de scripts de Windows (incluyendo PowerShell, VBS, etc)	Eventos
WinFileAccess Para obtener más información sobre los campos disponibles, consulte WinFileAccess.	Eventos de acceso a archivos de Windows (lectura/escritura)	Eventos
WinLogin Para obtener más información sobre los campos disponibles, consulte WinLogin.	Eventos de inicio de sesión de usuario de Windows	Eventos
WinLogout Para obtener más información sobre los campos disponibles, consulte WinLogout.	Eventos de cierre de sesión de usuario de Windows	Eventos
WinAgentDetection Para obtener más información sobre los campos disponibles, consulte WinAgentDetection.	Eventos de detección de Windows	Detecciones

Tipos de datos de muestra

Tipo de datos	Muestra	Descripción
Cadena	`WinProcCreate | where host_name == 'BNi-Kub'` `WinProcCreate | where host_name ==`	Las cadenas deben estar entre comillas simples o comillas dobles.

© Acronis International GmbH, 2003-2025

Tipo de datos	Muestra	Descripción
	`"BNi-Kub"`	
UUID	`WinProcCreate | where agent_id == '61f0c404-5cb3-11e7-907b-a6006ad3dba0'` `WinProcCreate | where agent_id == "61f0c404-5cb3-11e7-907b-a6006ad3dba0"`	Los UUID son valores de cadena y deben estar entre comillas simples o comillas dobles. Los valores de UUID deben estar en una secuencia de 8-4-4-4-12.
DateTime	`WinProcCreate | where event_time < '2022-11-01'` `WinProcCreate | where event_time < "2022-11-01"`	DateTime es un valor de cadena y debe estar entre comillas simples o comillas dobles. DateTime debe estar en formato AAAA-MM-DD.

Bool	`WinLogin | where is_admin == 1`
	`WinLogin | where is_admin == 0`
	`WinLogin | where is_admin == true`
	`WinLogin | where is_admin == false`
		Los valores booleanos pueden representarse por `1`, `0`, `true` o `false`.

Entero	`WinLogin | where proc_pid > 25`	Un valor entero.

Campos de eventos

Tipo de evento	Campo (tipo de datos)
WinProcCreate	• `agent_id (UUID)` • `customer (String)` • `event_time (DateTime)` • `host_name (String)` • `id (UUID)` • `owner (String)` • `parent_args (String)` • `parent_gpid (UUID)` • `parent_integrity_level (String)` • `parent_md5 (String)` • `parent_name (String)` • `parent_oname (String)` • `parent_path (String)` • `parent_pid (Int)` • `parent_sha1 (String)` • `parent_sha256 (String)` • `parent_start (DateTime)` • `parent_upn (String)`

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_prod (String) • proc_prod_desc (String) • proc_sha1 (String) • proc_sha256 (String) • proc_signatures (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinProcTerminate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String)

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• proc_user_domain (String) • resource_id (UUID) • term_args (String) • term_gpid (UUID) • term_integrity_level (String) • term_md5 (String) • term_name (String) • term_oname (String) • term_path (String) • term_pid (Int) • term_sha1 (String) • term_sha256 (String) • term_start (DateTime) • term_upn (String) • term_user (String) • term_user_domain (String) • timestamp (DateTime)
WinNetAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • net_dst_ip (String) • net_dst_port (Int) • net_host (String) • net_http_method (String) • net_http_url (String) • net_protocol (String) • net_src_ip (String) • net_src_port (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String)

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinRegAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String)

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • reg_key (String) • reg_operation (String) • reg_original_key (String) • reg_original_value_data (String) • reg_value_data (String) • reg_value_name (String) • reg_value_type (String) • resource_id (UUID) • timestamp (DateTime)
WinScriptExec	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String)

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • script_data (String) • script_fragment (Bool) • script_size (Int) • script_type (String) • timestamp (DateTime)
WinFileAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_op (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String)

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinLogin	• agent_id (UUID) • customer (String) • domain (String) • event_time (DateTime) • host_name (String) • id (UUID) • is_admin (Bool) • login_time (DateTime) • name (String) • owner (String) • resource_id (UUID) • security_id (String) • timestamp (DateTime) • type (String)

© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
WinLogout	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • logout_time (DateTime) • resource_id (UUID) • security_id (String) • timestamp (DateTime)
WinAgentDetection	• agent_id (UUID) • customer (String) • detection_type (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • mitre_stid (Int) • mitre_tactics (Int) • mitre_tid (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID)

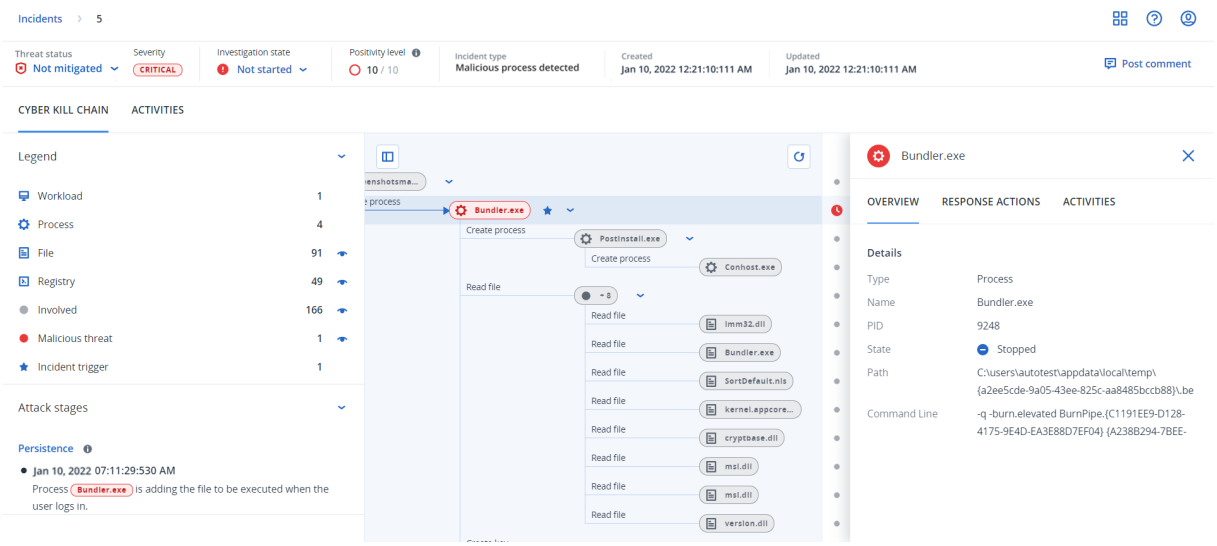
© Acronis International GmbH, 2003-2025

Tipo de evento	Campo (tipo de datos)
	• proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • severity (String) • threat_name (String) • timestamp (DateTime) • url (String) • url_blocked (Bool) • url_cat (Array(String)) • url_list (String) • url_md5 (String)

Investigación de incidentes

Endpoint Detection and Response (EDR) le permite investigar un incidente completo, incluidas todas las fases y los objetos del ataque (procesos, registros, tareas programadas y dominios) afectados por un atacante. Estos objetos se representan con nodos en la cyber kill chain fácil de entender, tal y como se muestra a continuación. Utilice la cyber kill chain para entender rápidamente qué ha ocurrido exactamente y cuándo.

© Acronis International GmbH, 2003-2025



Se pueden ver todos los pasos de un ataque en la cyber kill chain, que le ofrece una interpretación detallada de cómo y por qué ocurrió el incidente. La cyber kill chain utiliza oraciones y gráficos fáciles de comprender para explicar cada paso del ataque y ayudar a reducir el tiempo de investigación.

Puede entender rápidamente el ámbito y el impacto de un incidente, con la evolución del ataque asignada al marco MITRE. Esto le permite analizar lo que ha pasado en cada paso de un ataque, lo que incluye:

- El punto inicial de entrada
- Cómo se ejecutó el ataque
- Las remisiones de privilegios
- Evasión de técnicas de detección
- Desplazamientos laterales a otras cargas de trabajo
- Robo de credenciales
- Intentos de exfiltración

También puede hacer clic en **Copilot** para iniciar la herramienta de chat Copilot, que le permite introducir múltiples solicitudes y recibir acciones de respuesta sugeridas para el incidente seleccionado. Para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285).

Nota
Cada objeto impactado en el ataque, tanto si es un proceso, registro, tarea programada o dominio, se representa con un nodo en la cyber kill chain.

Pasos para investigar incidentes en la cyber kill chain

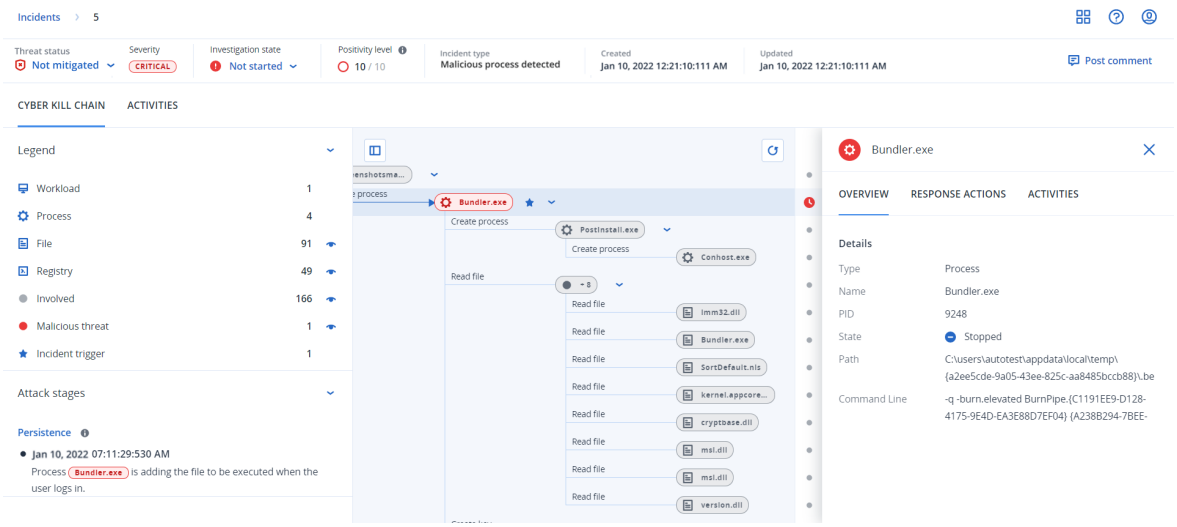
Podrá investigar todos los pasos de un ataque en la cyber kill chain. Siga las oraciones y los gráficos fáciles de comprender de cyber kill chain para entender cada paso del ataque, lo que también le

© Acronis International GmbH, 2003-2025

ayuda a reducir el tiempo de investigación.

Pasos para iniciar una investigación en la cyber kill chain

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.
2. En la lista de incidentes que se muestra, haga clic en en la columna situada en el extremo derecho del incidente que desee investigar. Se mostrará la cyber kill chain de los incidentes seleccionados.



3. Ver un resumen del incidente en la barra de estado de amenazas al principio de la página. La barra de estado de amenazas incluye la siguiente información:
   - Estado actual de la amenaza: El sistema define automáticamente el estado de la amenaza. Los incidentes con el estado **No mitigado** deben investigarse lo antes posible.

     Importante
     Un incidente se establece como **Mitigado** cuando se ha completado correctamente una restauración desde la copia de seguridad o cuando se han solucionado correctamente todas las detecciones mediante una acción de detención del proceso, cuarentena o reversión.

     Un incidente se establece como **No mitigado** cuando no se ha completado correctamente una restauración desde la copia de seguridad o cuando al menos una detección no se ha solucionado correctamente mediante una acción de detención del proceso, cuarentena o reversión.

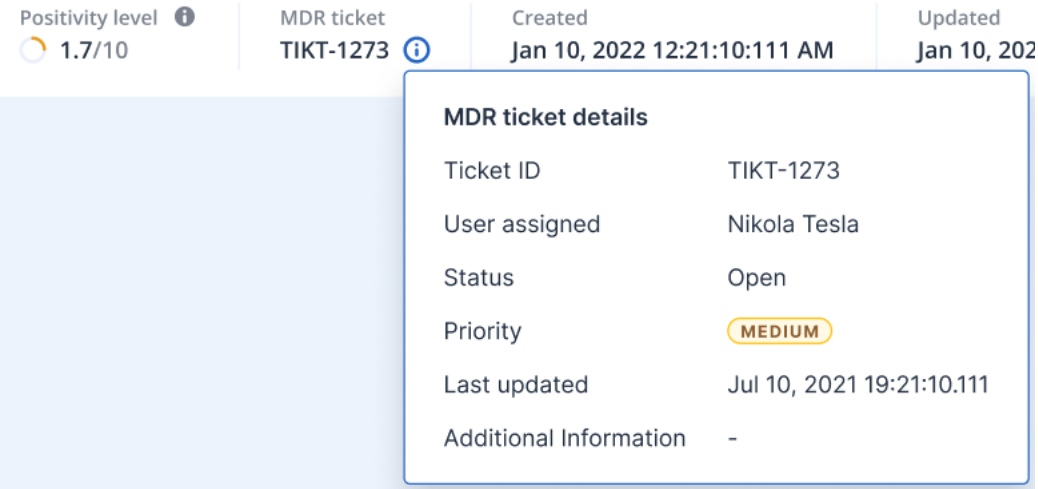
     También puede establecer el estado de la amenaza manualmente en **Mitigada** o **No mitigada**. Al seleccionar cada estado, se le pedirá que escriba un comentario. Este comentario se ha guardado como parte de las actividades de investigación y puede verse en la pestaña **Actividades**. Tenga en cuenta que la EDR aún puede revertir el estado de la amenaza a **Mitigada** o **No mitigada** si se descubrieron nuevas detecciones para el incidente o las acciones de respuesta se ejecutaron y se completaron correctamente.

© Acronis International GmbH, 2003-2025

- Gravedad del incidente: **Crítico**, **Alto** o **Intermedio**. Para obtener más información, consulte "Revisar incidentes" (p. 1258).
- Estado de la investigación actual: Uno de los siguientes: **Investigando**, **Sin iniciar** (el estado predeterminado), **Falso positivo** o **Cerrada**. Debe cambiar el estado cuando inicie la investigación del incidente para que el resto de colegas estén al tanto de los cambios que se produzcan en el mismo.
- Nivel de positividad: Indica la probabilidad de que un incidente sea verdaderamente un ataque malicioso, en una escala del 1 al 10. Para obtener más información, consulte "Revisar incidentes" (p. 1258).
- Tipo de incidente: uno o más casos de **Ransomware detectado**, **Malware detectado**, **Proceso sospechoso detectado**, **Proceso malicioso detectado**, **Detección de Microsoft Defender**, **URL sospechosa bloqueada** y **URL maliciosa bloqueada**.

  Nota
  Si Microsoft Defender Antivirus está habilitado para la protección en tiempo real en lugar de la protección en tiempo real de Acronis, solo se muestran los tipos de incidente **Detección de Microsoft Defender**, **URL sospechosa bloqueada** y **URL maliciosa bloqueada**.

- Si la detección y respuesta gestionadas (MDR) está habilitada en la carga de trabajo, se muestra un campo de **Ticket MDR**. Puede ver los detalles del ticket MDR creado para el incidente, y el analista de seguridad MDR asignado al incidente.



- El momento en que se creó y actualizó el incidente: Se detectó la fecha y hora del incidente o cuando se actualizó por última vez con nuevas detecciones registradas dentro del incidente.



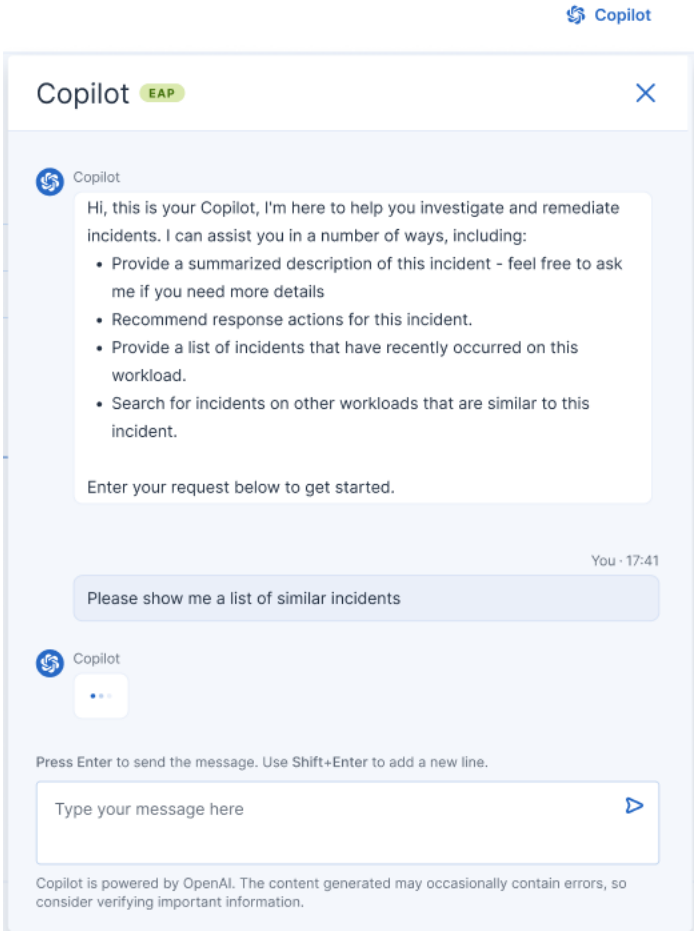
4. Haga clic en la pestaña **Leyenda** para ver los nodos que componen el gráfico de la kill chain y defina qué nodos desea ver. Para obtener más información, consulte "Comprender y personalizar la vista de la cyber kill chain" (p. 1289).
5. Siga los pasos siguientes para investigar y solucionar el incidente. Tenga en cuenta que se trata del flujo de trabajo típico para investigar y solucionar un incidente, pero puede variar en función de cada incidente y de sus requisitos.

© Acronis International GmbH, 2003-2025

a. Investigue cada fase del ataque en la pestaña **Fases del ataque**. Para obtener más información, consulte "Cómo ir a las fases del ataque" (p. 1291).

b. Haga clic en **Resolver incidente completo** para aplicar las acciones de resolución. Para obtener más información, consulte "Solucionar todo un incidente" (p. 1302). También puede resolver nodos individuales en la cadena de ciberataques, como se describe en "Acciones de respuesta para los nodos individuales de la cyber kill chain" (p. 1307).

   Como alternativa, haga clic en **Copilot** para iniciar la herramienta de chat asistida por IA Copilot. Copilot proporciona opciones de respuesta, según el incidente, e información contextual relevante para el incidente, como detalles sobre el tipo de ataque. Puede seleccionar la opción de respuesta relevante y, a continuación, seguir las instrucciones que aparecen en pantalla. Estas opciones de respuesta se describen en "Acciones de respuesta para los nodos individuales de la cyber kill chain" (p. 1307).



Importante

Hay un límite mensual de 1000 solicitudes por inquilino de partner al usar Copilot. Cuando se alcanza este límite, aparece un mensaje de error que le informa de que ha superado el límite mensual.

© Acronis International GmbH, 2003-2025

c. Revise las acciones tomadas para mitigar el incidente en la pestaña **Actividades**. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Comprender y personalizar la vista de la cyber kill chain

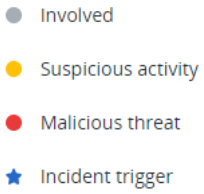
Para entender los nodos afectados en la cyber kill chain, acceda a la leyenda. La leyenda muestra todos los nodos afectados en un incidente, lo que le permite comprender cómo el atacante ha dañado los distintos nodos. También puede definir los nodos que desea ocultar o mostrar en la cyber kill chain.

Pasos para acceder a la leyenda

1. Haga clic en el icono de la flecha situado a la derecha de la sección Leyenda.
   La sección Leyenda se expande, como se muestra a continuación.



2. En la leyenda se utilizan cuatro colores principales que le permiten entender rápidamente qué ha pasado en cada nodo de la cyber kill chain, tal y como se muestra más abajo. Estos nodos con códigos de color también se incluyen en las fases del ataque, como se describe en "Cómo ir a las fases del ataque" (p. 1291).



Pasos para ocultar o mostrar nodos en la cyber kill chain

© Acronis International GmbH, 2003-2025

1. En la sección Leyenda expandida, asegúrese de que se muestra junto a los nodos que desea mostrar en la cyber kill chain. Si el icono que se muestra es , haga clic en él para cambiarlo a .
2. Para ocultar un nodo en la cyber kill chain, haga clic en . El icono cambia a y el nodo no se muestra en la cyber kill chain.

Investigue las fases del ataque de un incidente

Las fases del ataque de un incidente ofrecen interpretaciones fáciles de entender de cada incidente.

Cada fase del ataque resume lo que ha ocurrido exactamente y cuáles han sido los objetos objetivo (a los que se hace referencia como *nodos* en la cyber kill chain). Por ejemplo, si un archivo descargado estaba ocultando algo más, la fase del ataque lo indicará e incluirá enlaces al nodo relevante en la cyber kill chain que puede investigar y a la técnica MITRE ATT&CK pertinente.

Cada fase del ataque le proporciona la información que necesita para resolver tres cuestiones cruciales:

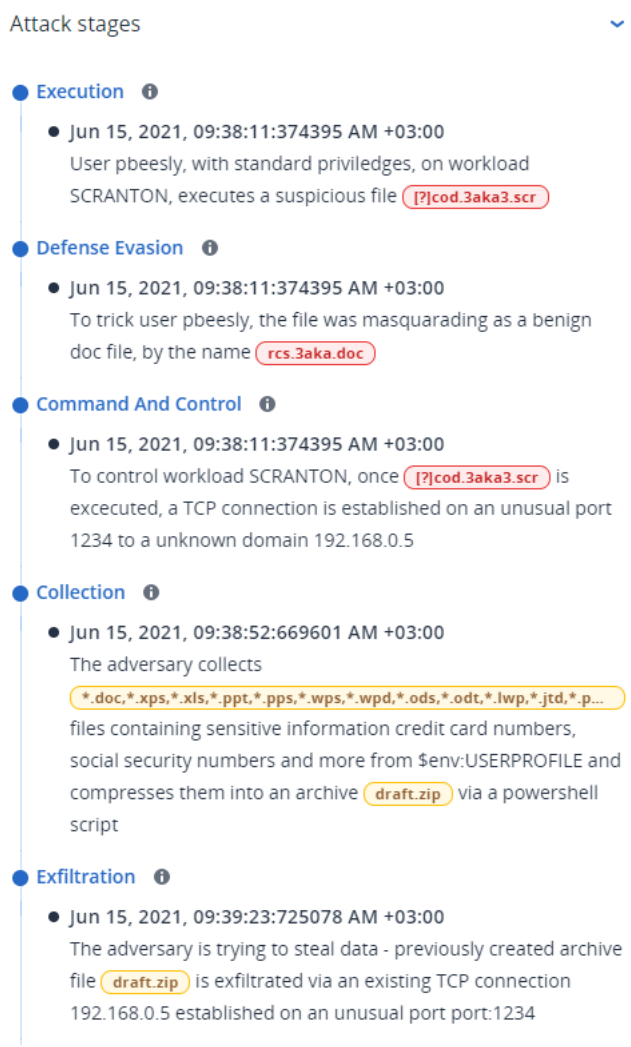
- ¿Cuál era el objetivo del ataque?
- ¿Cómo consiguió el atacante este objetivo?
- ¿Cuáles eran los nodos de destino?

Más importante aún, la interpretación proporcionada garantiza que el tiempo dedicado a investigar un incidente se reduzca considerablemente, ya que ya no es necesario revisar cada evento de seguridad desde una línea de tiempo o un nodo gráfico y luego intentar crear una interpretación del ataque.

Las fases del ataque también incluyen información sobre archivos comprometidos que contienen información confidencial, como números de tarjeta de crédito y números de la seguridad social, según se muestra en la fase **Recopilación** del ejemplo de más abajo.

Para obtener más información, consulte "¿Qué información se incluye en una fase de ataque?" (p. 1291).

© Acronis International GmbH, 2003-2025



Cómo ir a las fases del ataque

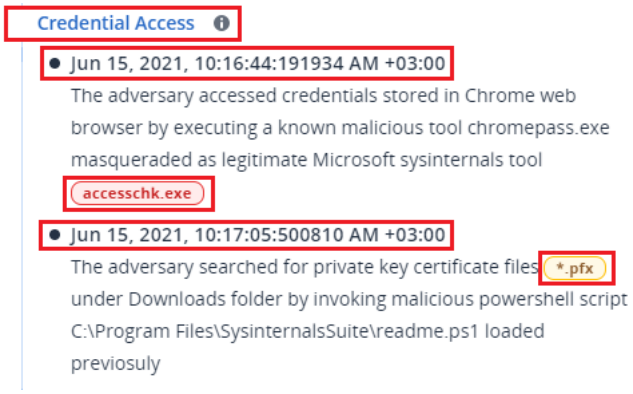
Las fases del ataque se enumeran en orden cronológico. Desplácese hacia abajo para ver la lista completa de fases del ataque para el incidente.

Para investigar más una fase del ataque específica, haga clic en cualquier parte en la fase del ataque para ir al nodo que corresponda en el gráfico de la cyber kill chain. Para obtener más información sobre cómo ir al gráfico de la cyber kill chain y a nodos específicos, consulte "Investigar nodos individuales en la cyber kill chain" (p. 1293).

¿Qué información se incluye en una fase de ataque?

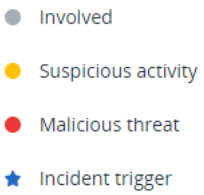
Cada fase de ataque ofrece una interpretación fácil de entender del ataque, en un lenguaje humano fácil de leer. Esta interpretación se compone de una serie de elementos, como se muestra y describe en la siguiente tabla.

© Acronis International GmbH, 2003-2025



Elemento de fase del ataque	Descripción
Encabezado	Describe lo que el atacante intentaba hacer y su objetivo (en el ejemplo anterior, **Acceso con credenciales**), con un enlace a una técnica de MITRE ATT&CK conocida. Haga clic en el enlace para obtener más información acerca del sitio web de MITRE ATT&CK. **Nota** Si una fase de ataque no es una técnica MITRE ATT&CK conocida, el texto del encabezado no estará enlazado. Esto es importante para las técnicas genéricas, como los archivos detectados en una carpeta aleatoria.
Marca de fecha	La hora a la que ocurrió la fase del ataque.
Técnica	Cómo consiguió técnicamente el atacante su objetivo y a qué objetos (entradas de registro, archivos o tareas programadas) afectó. Los enlaces con códigos de color a cada nodo afectado de la cyber kill chain se incluyen en la descripción de texto de la técnica del ataque, como se muestra en el ejemplo anterior. Estos enlaces con códigos de color le permiten ir rápidamente al nodo afectado e investigar qué ocurrió exactamente. Los colores que se utilizan en una fase de ataque indican lo siguiente:

© Acronis International GmbH, 2003-2025

Elemento de fase del ataque	Descripción
	 Si nos fijamos en la leyenda anterior, puede verse que la fase de ataque de ejemplo del acceso con credenciales tiene un enlace a un nodo de malware accesschk.exe y un nodo de archivo sospechoso *.pfx (haga clic en los enlaces para saltar al nodo correspondiente de la cyber kill chain). Para obtener más información sobre cómo ir a estos nodos y las acciones disponibles, consulte "Investigar nodos individuales en la cyber kill chain" (p. 1293). Tenga en cuenta que las fases del ataque también incluyen enlaces a nodos de archivos que tengan información sobre archivos comprometidos cuyo contenido sea información confidencial, como información de salud protegida (PHI), números de tarjeta de crédito y números de la seguridad social.

Nota
Cada fase del ataque es un evento de detección único. El contenido enumerado en cada fase (encabezado, fecha/hora, técnica) se genera según parámetros específicos en el evento de detección y se basa en plantillas de fases de ataques almacenadas por Endpoint Detection and Response (EDR).

Investigar nodos individuales en la cyber kill chain

Además de revisar las fases del ataque, también puede explorar los nodos del ataque en la cyber kill chain. Esto le permite profundizar en nodos específicos de la cyber kill chain e investigar y solucionar cada nodo según sea necesario.

Por ejemplo, puede determinar la probabilidad de que un incidente sea un ataque malicioso de verdad. Según su investigación, también puede aplicar una serie de acciones de respuesta al nodo, incluido el aislamiento de una carga de trabajo o la cuarentena de un archivo sospechoso.

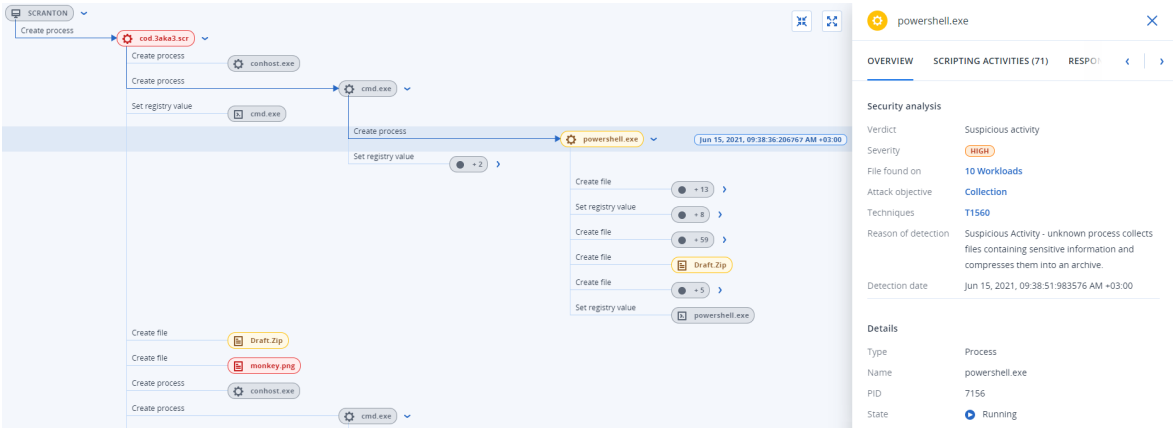
Pasos para investigar nodos individuales en la cyber kill chain

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.
2. En la lista de incidentes que se muestra, haga clic en  en la columna situada en el extremo derecho del incidente que desee investigar. Se mostrará la cyber kill chain de los incidentes seleccionados.
3. Vaya al nodo correspondiente y haga clic en él para mostrar la barra lateral del nodo.

   Nota
   Haga clic en el nodo para expandirlo y mostrar los nodos asociados.

   Por ejemplo, si hace clic en el nodo **powershell.exe** del ejemplo siguiente, se abrirá la barra lateral del nodo. También puede hacer clic en el icono de la flecha junto al nodo para ver los nodos asociados, incluidos los archivos y los valores de registro, que puedan estar afectados por el nodo **powershell.exe**. A su vez, puede hacer clic en los nodos asociados para obtener más información.



4. Investigue la información incluida en las pestañas de la barra lateral:
   - **Información general**: Incluye las dos principales secciones que ofrecen un resumen de seguridad del nodo atacado.
     - **Análisis de seguridad**: Ofrece un análisis del nodo atacado, incluido el veredicto de EDR de la amenaza (como actividad sospechosa), el objetivo del ataque según las técnicas de ataque de MITRE (haga clic en el enlace para ir al sitio web de MITRE), el motivo de la detección y el número de cargas de trabajo a las que pueda afectar el ataque (haga clic en el enlace **n Cargas de trabajo** para ver las cargas de trabajo afectadas).

       Nota
       El enlace **n Cargas de trabajo** significa que el objeto malicioso o sospechoso específico se ha *encontrado* en otras cargas de trabajo. No significa que el ataque esté ocurriendo en esas otras cargas de trabajo, sino que hay un indicador de compromiso en esas otras cargas de trabajo. Puede que el ataque ya haya ocurrido (y creado otro incidente), o que el atacante se esté preparando para golpear esas otras cargas de trabajo con el ataque «kit de herramientas».

© Acronis International GmbH, 2003-2025

  - **Detalles**: Incluye detalles acerca del nodo, como su tipo, nombre y estado actual, la ruta hasta el nodo y cualquier has del archivo y firmas digitales (como MD5 y números de serie de certificados).
- **Actividades de secuencias de comandos**: Incluye detalles de cualquier secuencia de comandos invocada o cargada en el ataque. Haga clic en  para copiar la secuencia de comandos a su portapapeles para investigar más.

Nota
La pestaña **Actividades de secuencias de comandos** solo se mostrará para los nodos de procesos que ejecutan comandos o secuencias de comandos (como cmd o comandos de PowerShell).

- **Medidas de respuesta**: Incluye un número de secciones que ofrecen más acciones de investigación, solución y prevención, según el tipo de nodo.
  Por ejemplo, en el caso de nodos de carga de trabajo, puede definir una serie de respuestas que incluyen una copia de seguridad forense y una restauración desde la copia de seguridad. De manera alternativa, para nodos maliciosos o sospechosos, puede detener un nodo o ponerlo en cuarentena, revertir los cambios hechos por el ataque y añadirlo a una lista de permitidos o de bloqueados de un plan de protección.
  Para obtener más información sobre la aplicación de acciones de respuesta a nodos específicos, consulte "Acciones de respuesta para los nodos individuales de la cyber kill chain" (p. 1307).
- **Actividades**: Muestra las acciones aplicadas al incidente en orden cronológico. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Entienda las acciones emprendidas para mitigar un incidente

Después de revisar un incidente e investigar cómo ha ocurrido el ataque, por lo general aplicará acciones de respuesta. Una vez que haya aplicado acciones de respuesta, dichas acciones se podrán ver en una serie de lugares para entender mejor qué pasos se han tomado para mitigar el incidente.

Nota
Los incidentes creados por las capas de prevención se aplican automáticamente a las acciones configuradas en el plan de protección. Para los puntos de detección, debe definir las acciones de respuesta que correspondan para mitigar el escenario de cada ataque.

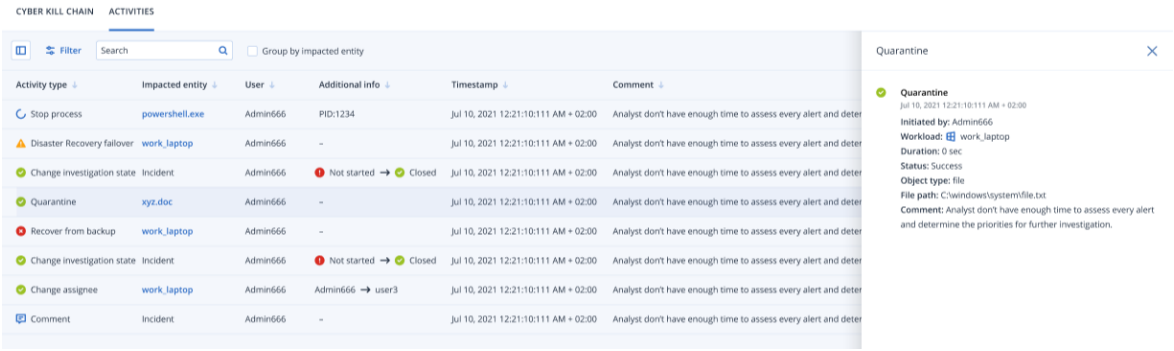
Para entender las acciones de respuesta emprendidas, puede ver todas las acciones de respuesta aplicadas a un incidente completo o a un nodo específico en la cyber kill chain del incidente.

Pasos para ver todas acciones de respuesta aplicadas a un incidente

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.

© Acronis International GmbH, 2003-2025

2. En la lista de incidentes que se muestra, haga clic en en la columna situada en el extremo derecho del incidente que desee investigar. Se mostrará la cyber kill chain de los incidentes seleccionados.
3. Haga clic en la pestaña **Actividades**.
   Se mostrará la lista de medidas de respuesta que ya se han aplicado al incidente.



Nota
Si la acción de respuesta se inició como parte de un flujo de trabajo automatizado, el campo **Iniciada por** mostrará **Flujo de trabajo automatizado**. Para obtener más información, consulte "Trabajar con flujos de trabajo automatizados" (p. 1330).

4. Puede llevar a cabo una serie de acciones en la lista mostrada:
   - Haga clic en una fila de tipo de actividad para mostrar más información sobre la actividad seleccionada. La información se muestra en una barra lateral, como se ve en el Paso 3, e incluye información sobre quién inició la acción, su estado, ruta de archivo y cualquier comentario añadido por la persona que la inició.
   - Utilice el cuadro **Buscar** para buscar una acción específica.
   - Haga clic en **Filtro** para aplicar filtros a la lista.
   - Seleccione la casilla de verificación **Agrupar por entidad afectada** para agrupar las acciones correspondientes según la entidad.
   - Haga clic en para mostrar u ocultar la lista de acciones completadas.
     Asegúrese de que se muestra junto a las acciones que desea mostrar. Si desea ocultar una acción de la lista mostrada, haga clic de nuevo para cambiarla a .

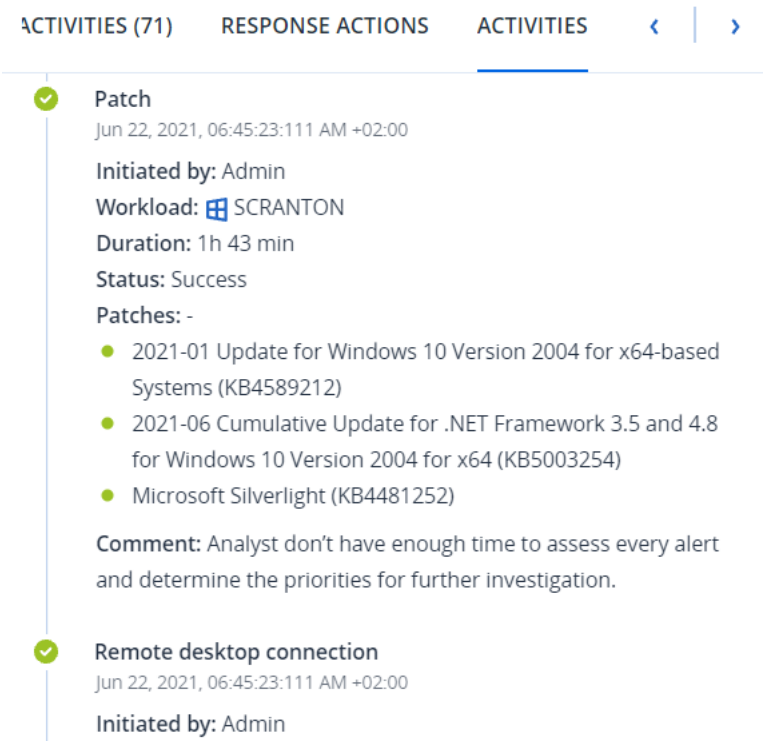
© Acronis International GmbH, 2003-2025



Pasos para ver las acciones de respuesta aplicadas a un nodo específico

© Acronis International GmbH, 2003-2025

1. En la cyber kill chain, haga clic en un nodo para ver la barra lateral de dicho nodo.
2. Haga clic en la pestaña **Actividades**.



3. Para entender por completo qué acciones se han aplicado y por qué, quizá necesite desplazarse por las acciones de respuesta aplicadas al nodo. Por ejemplo, en el caso de las acciones de conexión a escritorio remoto, puede ver quién inició la acción y cuándo, la duración de la acción y su estado general (si se completó correctamente, si falló o si se completó con errores).

Nota
Si la acción de respuesta se inició como parte de un flujo de trabajo automatizado, el campo **Iniciada por** mostrará **Flujo de trabajo automatizado**. Para obtener más información, consulte "Trabajar con flujos de trabajo automatizados" (p. 1330).

Busque indicadores de compromiso (IOC) de ataques conocidos públicamente en sus cargas de trabajo

Endpoint Detection and Response (EDR) incluye la capacidad de revisar los ataques conocidos existentes en las fuentes de información sobre amenazas de sus cargas de trabajo. Estas fuentes de información sobre amenazas se generan automáticamente según los datos sobre amenazas recibidos del centro de operaciones de ciberprotección (CPOC); la EDR le permite comprobar si una amenaza ha afectado a su carga de trabajo o no y llevar a cabo los pasos necesarios para anular la amenaza.

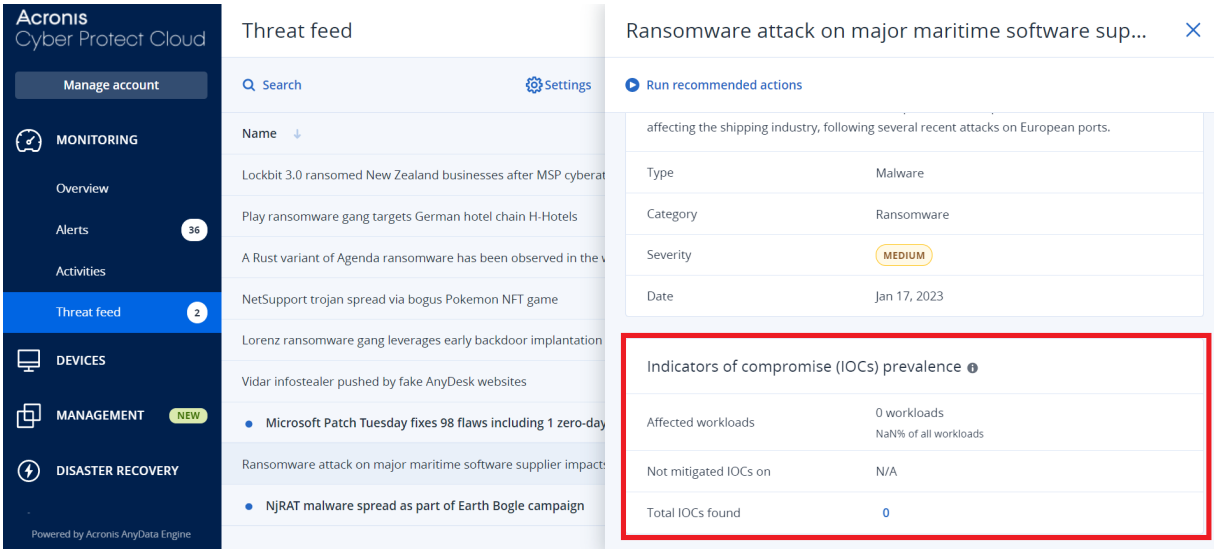
Puede acceder a las fuentes de información sobre amenazas desde el menú **Supervisión** de la consola de Cyber Protect. Para obtener más información, consulte "Fuente de amenazas" (p. 352).

© Acronis International GmbH, 2003-2025

Para revisar la información específica de las amenazas y confirmar si afectan a sus cargas de trabajo, haga clic en una fuente de información sobre amenazas. Puede ver el número de IOC detectado y las cargas de trabajo afectadas, y profundizar en las cargas de trabajo que contienen IOC no mitigados.

Nota

Si el plan de protección no tiene habilitada la EDR, no se mostrará esta funcionalidad adicional de fuente de información sobre amenazas, como se muestra a continuación.



Defina la configuración de la fuente de información sobre amenazas

Puede definir una serie de ajustes de la fuente de información sobre amenazas para localizar y mitigar las amenazas conocidas automáticamente.

Pasos para definir la configuración de la fuente de información sobre amenazas

1. En la consola de Cyber Protect, vaya a **Supervisión > Fuente de información sobre amenazas**.
2. En la página Fuente de información sobre amenazas que se muestra, haga clic en **Configuración**.

© Acronis International GmbH, 2003-2025

3. En el cuadro de diálogo que se muestra, seleccione cualquiera de las siguientes opciones:

Opción	Descripción
Buscar indicadores de compromiso (IOC)	Haga clic en el conmutador para habilitar la búsqueda automática de IOC en sus cargas de trabajo. Cuando esta opción esté habilitada, también se mostrarán las opciones **Acción sobre la detección** y **Generar alerta**.
Acción sobre la detección	En la lista desplegable, seleccione la acción que debe llevarse a cabo en los archivos correspondientes cuando se detecte una amenaza en una carga de trabajo: • **Sin acción** • **Cuarentena** • **Eliminar** • **Aislar cargas de trabajo**
Generar alerta	Seleccione la casilla de verificación para generar una alerta si se encuentra un IOC en una carga de trabajo. La alerta se mostrará en la página Alertas.

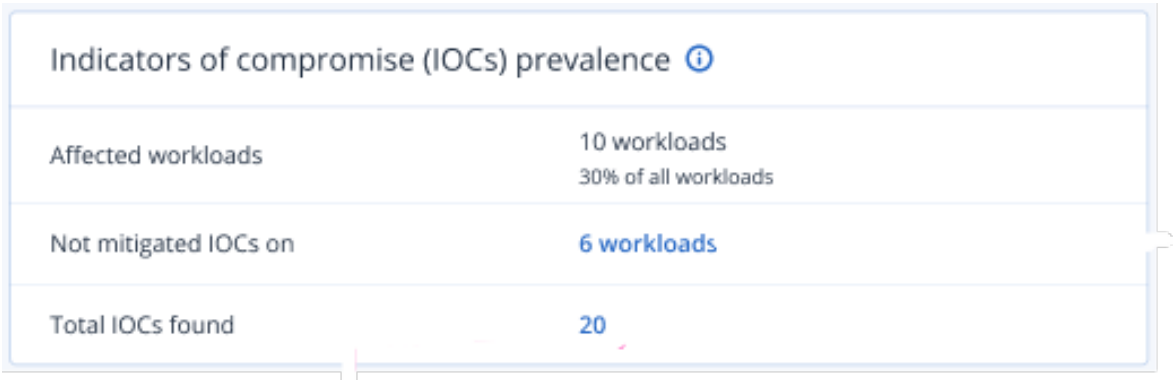
4. Haga clic en **Aplicar**.

Revise y mitigue los IOC mitigados en las cargas de trabajo afectadas

Cuando se habilita Endpoint Detection and Response (EDR) en un plan de protección, puede ver cualquier amenaza conocida que afecta a las cargas de trabajo del plan de protección. También puede mitigar cualquier indicador de compromiso (IOC) restante que no se haya mitigado automáticamente. Para obtener más información sobre cómo mitigar automáticamente los IOC, consulte "Defina la configuración de la fuente de información sobre amenazas" (p. 1299).

Pasos para revisar y mitigar las cargas de trabajo afectadas

1. En la consola de Cyber Protect, vaya a **Supervisión > Fuente de información sobre amenazas**.
2. Haga clic en una amenaza para mostrar los detalles.
3. En la sección **Prevalencia de los indicadores de compromiso (IOC)**, haga clic en el enlace ***n* cargas de trabajo** para ver las cargas de trabajo con IOC no mitigados.



© Acronis International GmbH, 2003-2025

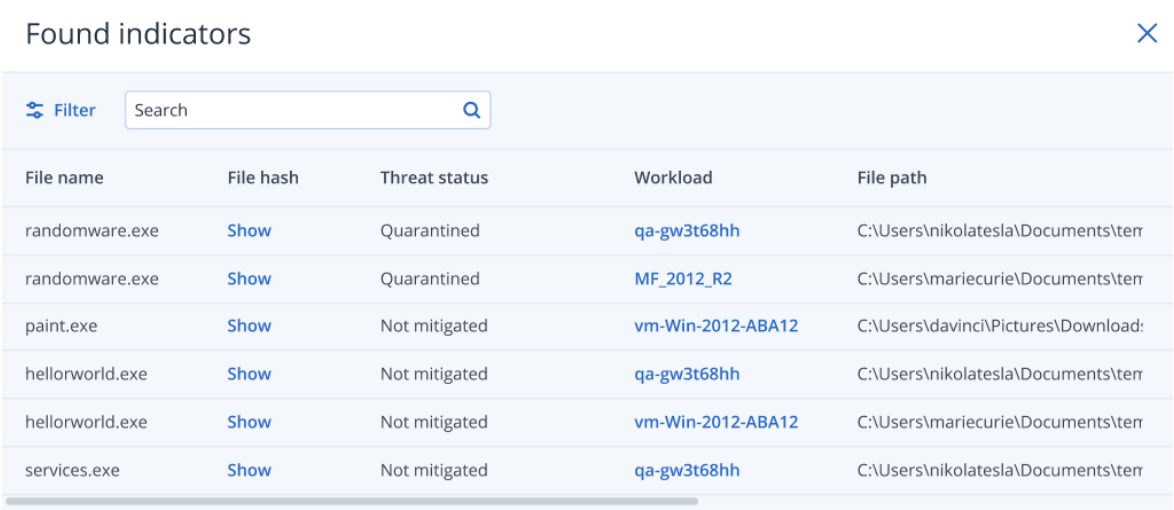
4. En la página Cargas de trabajo que se muestra, haga clic en la carga de trabajo correspondiente y revise la información. Puede ejecutar la funcionalidad específica en la carga de trabajo, incluida la definición de URL adicionales para filtrar (consulte "Filtrado de URL" (p. 1192)) y bloquear los procesos maliciosos (consulte la sección Exclusiones en "Configuración de los ajustes de la protección antivirus y antimalware" (p. 1166)).
   Por ejemplo, si una fuente de información sobre amenazas indica que un IOC ha afectado a una carga de trabajo, primero localice y analice el IOC, según se describe en "Revise y analice los IOC descubiertos" (p. 1301). A continuación, vaya al plan de protección de la carga de trabajo y defina la protección adicional, como el bloqueo de procesos o hash de archivo maliciosos.

Revise y analice los IOC descubiertos

Además de revisar las cargas de trabajo afectadas por amenazas conocidas, también puede revisar y analizar indicadores de compromiso (IOC) específicos. Esto le permite ver las cargas de trabajo individuales afectadas por un IOC y mitigarlo.

Pasos para revisar y analizar los IOC

1. En la consola de Cyber Protect, vaya a **Supervisión > Fuente de información sobre amenazas**.
2. Haga clic en una amenaza para mostrar los detalles.
3. En la sección **Prevalencia de los indicadores de compromiso (IOC)**, haga clic en el enlace **Total de IOC encontrados**.
   Se mostrará la página Indicadores encontrados.



4. (Opcional) Utilice la opción **Filtro** para filtrar la lista de IOC según su estado. También puede utilizar la opción **Buscar** para buscar IOC específicos.
5. Para ver la carga de trabajo afectada por un IOC, haga clic en el enlace de la columna **Carga de trabajo**. Podrá llevar a cabo varias acciones en la carga de trabajo, como ejecutar la gestión de parches o modificar un plan de protección.
6. (Opcional) En la columna **Hash del archivo**, haga clic en **Mostrar** para mostrar los hash del archivo encontrados para un IOC específico. En el cuadro de diálogo que se muestra, haga clic en para copiar el hash del archivo del IOC a un editor de texto.

© Acronis International GmbH, 2003-2025

Solución de incidentes

Endpoint Detection and Response (EDR) le permite solucionar incidentes completos o los puntos de ataque individuales de un incidente.

Al solucionar todo el incidente, puede elegir las soluciones que desea ejecutar de forma global en el incidente. Si necesita gestionar el incidente con mayor detalle, puede solucionar puntos de ataque individuales según sea necesario. Por ejemplo, es posible que quiera aislar la red de una carga de trabajo con el fin de detener el movimiento lateral o las actividades de comando y control (C&C). Esto le garantiza que incluso aunque la carga de trabajo esté aislada, todas las tecnologías de Acronis Cyber Protect seguirán funcionando y se podrá ejecutar una investigación.

La EDR garantiza una solución efectiva al:

- Mitigar: para garantizar que se detiene la amenaza.
- Recuperar: para garantizar que los servicios vuelven a estar en línea inmediatamente.
- Prevenir: para garantizar que se evitan las técnicas utilizadas en un ataque en futuros ataques.

Solucionar todo un incidente

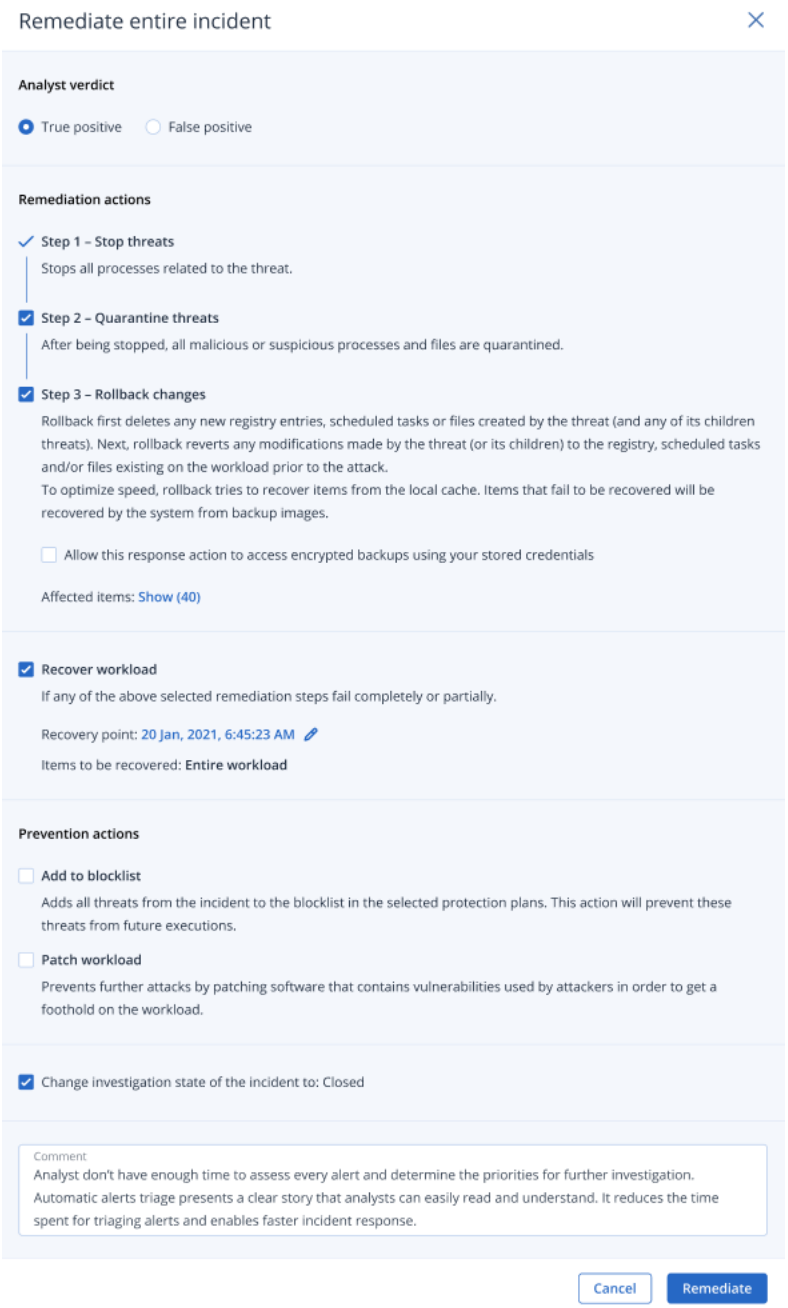
Al solucionar todo un incidente, puede elegir rápida y fácilmente las soluciones que desea ejecutar de forma global en el incidente. Endpoint Detection and Response (EDR) le guía a través del proceso de solución, paso a paso.

Si necesita gestionar su red y el incidente con mayor detalle, consulte "Acciones de respuesta para los nodos individuales de la cyber kill chain" (p. 1307).

Pasos para solucionar todo un incidente

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.
2. En la lista de incidentes que se muestra, haga clic en  en la columna del extremo derecho del incidente que desee investigar. Se mostrará la cyber kill chain de los incidentes seleccionados.
3. Haga clic en **Solucionar todo el incidente**. Se mostrará el diálogo Solucionar todo el incidente.

© Acronis International GmbH, 2003-2025



4. En la sección **Veredicto del analista**, según su investigación del incidente, seleccione una de las siguientes opciones:
   - **Verdadero positivo**: Seleccione si está seguro de que es un ataque legítimo. Una vez seleccionado, puede añadir acciones de solución y prevención, tal y como se describe en los siguientes pasos.
   - **Falso positivo**: Seleccione si está seguro de que no es un ataque real. En este modo, podrá definir cómo prevenir que esto vuelva a ocurrir, por ejemplo al añadiendo el incidente a una lista de permitidos del plan de protección.

© Acronis International GmbH, 2003-2025

Nota
Después de seleccionar **Falso positivo**, solo podrá definir acciones de prevención. Para obtener más información, consulte "Solucionar un incidente con falso positivo" (p. 1306).

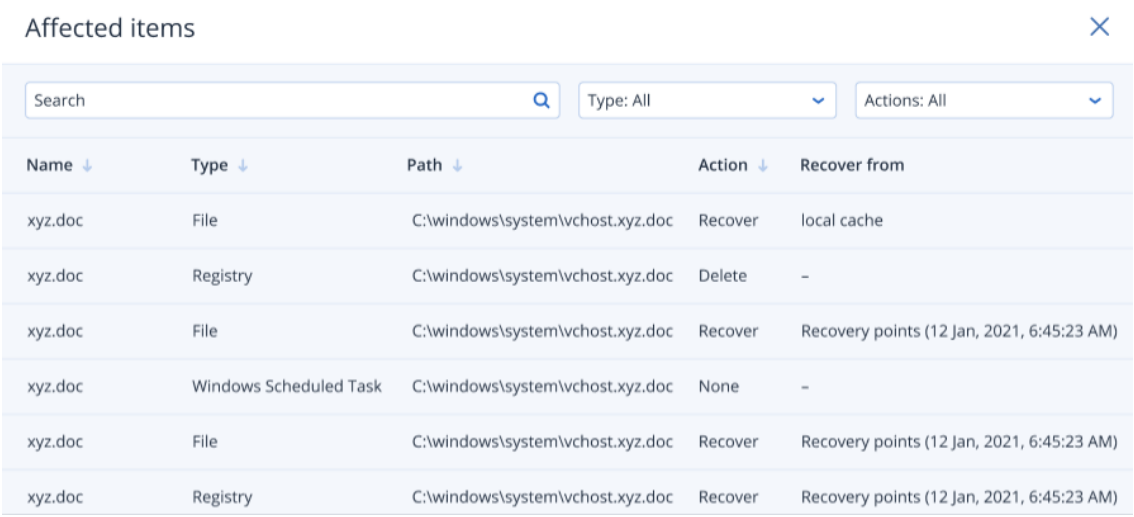
5. En la sección **Acciones de solución**, lleve a cabo los siguientes pasos de solución. Tenga en cuenta que deben seguirse en orden secuencial. Por ejemplo, no puede seleccionar el paso 2 antes de completar el paso 1.
   a. **Paso 1: detenga las amenazas**: Seleccione la casilla de verificación para detener todos los procesos relacionados con la amenaza.
   b. **Paso 2: ponga en cuarentena las amenazas**: Una vez detenida la amenaza, seleccione la casilla de verificación para poner en cuarentena todos los procesos y archivos maliciosos y sospechosos.
   c. **Paso 3: revierta los cambios**: Después de poner en cuarentena las amenazas, seleccione la casilla de verificación para eliminar cualquier entrada de registro, tarea o archivo nuevos que la amenaza (y cualquier amenaza secundaria) haya programado o creado. A continuación, el proceso de reversión revierte cualquier modificación que la amenaza (o sus procesos secundarios) haya hecho al registro, tareas programadas o archivos que estaban en la carga de trabajo antes del ataque. Para optimizar la velocidad, el proceso de reversión intenta recuperar los elementos desde la caché local. A partir de imágenes de la copia de seguridad, el sistema se encargará de los elementos que no se puedan recuperar.

   Nota
   El proceso de reversión solo recupera los elementos en la caché local. Se podrán revertir archivos de copia de seguridad en próximas versiones.

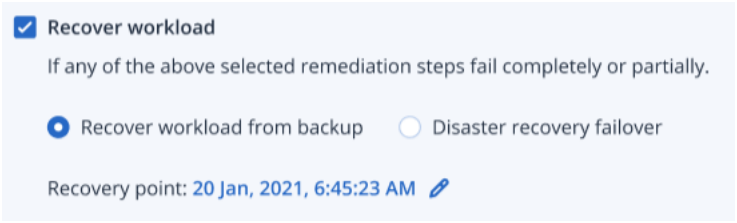
   Seleccione la casilla de verificación **Permitir que esta acción de respuesta acceda a copias de seguridad cifradas mediante credenciales almacenadas** si el acceso a las correspondientes copias de seguridad está cifrado. La EDR accede a las credenciales de usuario almacenadas para descifrar los archivos cifrados y buscar los archivos correspondientes.

   También pueden hacer clic en los **Elementos afectados** para ver todos los elementos (archivos, registro o tareas programadas) afectados por la reversión, las acciones aplicadas (**Eliminar**, **Recuperar** o **Ninguna**) y si los elementos se están restaurando desde la caché local o las imágenes de la copia de seguridad.

© Acronis International GmbH, 2003-2025



d. **Recuperar carga de trabajo**: Seleccione la casilla de verificación para recuperar una carga de trabajo si alguno de los pasos de solución mencionados anteriormente da error total o parcialmente.



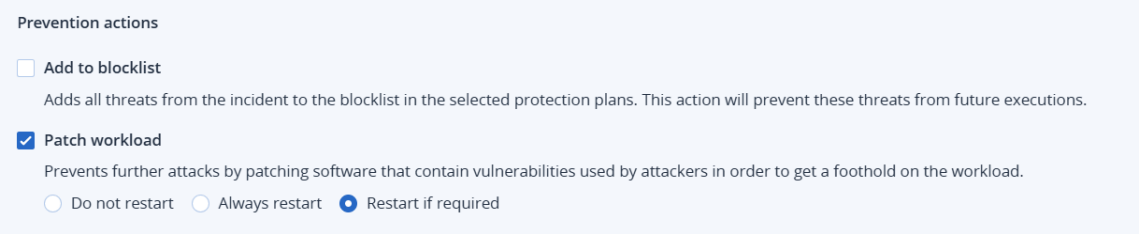
Seleccione uno de las siguientes opciones de recuperación:

- **Recuperar carga de trabajo a partir de la copia de seguridad**: Le permite recuperar una carga de trabajo desde un punto de recuperación específico. Haga clic en el icono de edición del punto de recuperación para seleccionar de entre una lista de copias de seguridad de recuperación.
- **Conmutación por error de la recuperación ante desastres**: Le permite ejecutar la recuperación ante desastres si tiene esta funcionalidad habilitada en su plan de protección. Le recomendamos utilizar esta opción para las cargas de trabajo críticas, como los servidores de AD o los servidores de la base de datos. Para obtener más información, consulte "Implementación de la recuperación ante desastres" (p. 1010).

6. En la sección **Acciones de prevención**, seleccione los pasos de solución que correspondan:
   - **Añadir a la lista de bloqueados**: marque la casilla de verificación y, desde la lista del plan de protección que se muestra, seleccione los planes de protección que correspondan. Esta acción de prevención garantiza que todas las detecciones del incidente dejarán de ejecutarse para los planes de protección seleccionados.
   - **Reparar carga de trabajo**: marque la casilla de verificación para reparar cualquier software vulnerable y evitar que los atacantes obtengan acceso a la carga de trabajo. Puede seleccionar la acción que corresponda para ejecutar una vez que el parche esté completo (**No reiniciar**, **Reiniciar siempre** o **Reiniciar si es necesario**), en función de si el usuario ha iniciado sesión

© Acronis International GmbH, 2003-2025

o no.



7. Seleccione la casilla de verificación **Modificar estado de la investigación del incidente a: Cerrada**. Si no se selecciona, el estado de la investigación seguirá siendo el anterior.
8. Haga clic en **Solucionar**. Las acciones de solución que selecciona se ejecutarán, paso a paso, con el progreso de cada paso de solución mostrado en el diálogo Solucionar todo el incidente. Cuando se haga clic en el botón, se mostrará **Ir a las actividades**. Haga clic en **Ir a las actividades** para revisar todas las acciones de respuesta aplicadas al incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Solucionar un incidente con falso positivo

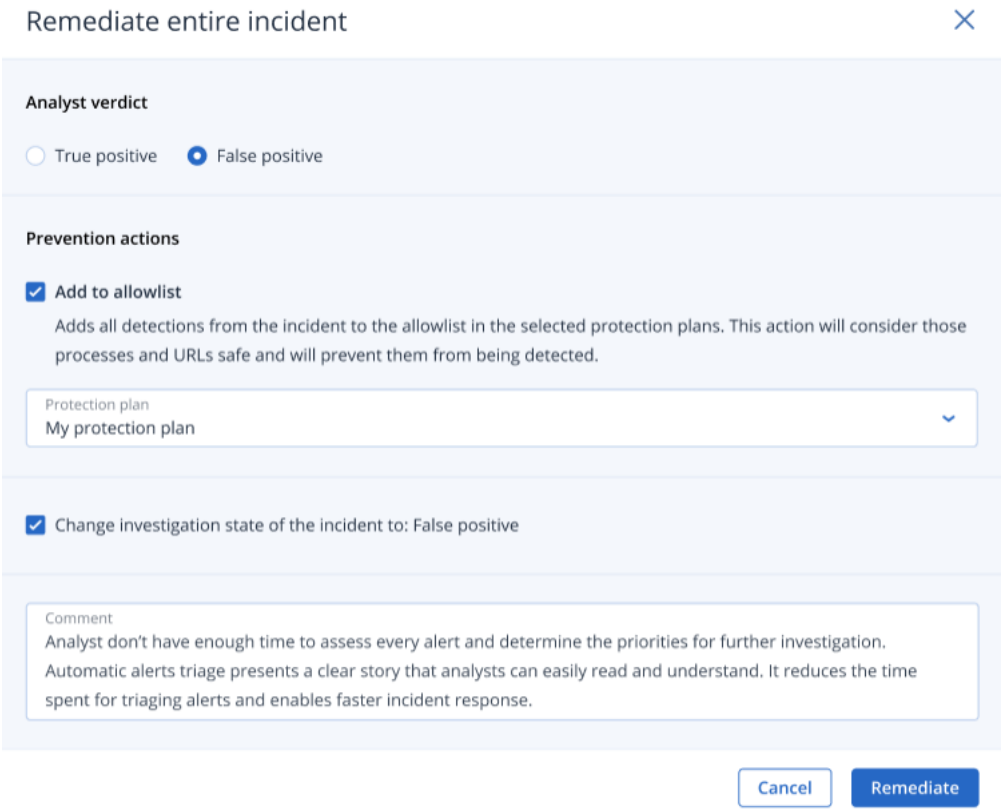
Si tiene claro que un ataque no lo es en realidad, en otras palabras, es un falso positivo, puede definir cómo evitar que el incidente ocurra de nuevo. Por ejemplo, podrá añadir el incidente a la lista de permitidos de un plan de protección.

Pasos para solucionar un incidente con falso positivo

1. En la cyber kill chain del incidente seleccionado, haga clic en **Solucionar todo el incidente**. Se mostrará el diálogo Solucionar todo el incidente.

© Acronis International GmbH, 2003-2025

2. En la sección **Veredicto del analista**, seleccione **Falso positivo**.



3. En la sección **Acciones de prevención**, seleccione la casilla de verificación **Añadir a la lista de permitidos**. Desde la lista del plan de protección que se muestra, seleccione los planes de protección que correspondan.
   Esta acción de prevención garantiza que todas las detecciones del incidente dejarán de detectarse para los planes de protección seleccionados.
4. Seleccione la casilla de verificación **Modificar estado de la investigación del incidente a: Falso positivo**.
5. Haga clic en **Solucionar**.
   Cuando se haga clic en el botón, se mostrará **Ir a las actividades**. Haga clic en **Ir a las actividades** para revisar las acciones de respuesta aplicadas al incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Acciones de respuesta para los nodos individuales de la cyber kill chain

Si necesita gestionar el incidente con mayor detalle, puede aplicar varias acciones de respuesta a nodos individuales de la cyber kill chain. Estas acciones de respuesta le permite solucionar rápida y fácilmente cualquier nodo.

Nota
Para aplicar acciones de respuesta globales a todo el incidente, consulte "Solucionar todo un incidente" (p. 1302).

© Acronis International GmbH, 2003-2025

Las acciones de respuesta se dividen en las siguientes categorías, aunque no todos los nodos incluyen todas las categorías siguientes:

- **Solucionar**: Las acciones de esta categoría le permiten aplicar una respuesta inmediata al ataque e incluyen la gestión del aislamiento de la red para una carga de trabajo y la eliminación y puesta en cuarentena de archivos, procesos y valores de registro.
- **Investigar**: las acciones de esta categoría (aplicables solo a cargas de trabajo) le permiten ejecutar una copia de seguridad forense, una conexión a escritorio remoto o una línea de comandos o terminal remoto para una investigación más profunda.
- **Recuperación**: Las acciones de esta categoría (se aplican solo a cargas de trabajo) le permiten responder a ataques intensivos mediante la ejecución de la recuperación desde la copia de seguridad o la conmutación por error de Disaster Recovery.
- **Prevenir**: Las acciones de esta categoría le permiten prevenir futuras amenazas o falsos positivos al añadirlos a una lista de permitidos o una lista de bloqueados del plan de protección.

Nota
Si se cierra un incidente, no podrá aplicar una acción de respuesta a un nodo. No obstante, puede volver a abrir un incidente cerrado cambiando su estado de investigación a **Investigando**. Una vez reabierto, puede aplicar las acciones de respuesta.

La siguiente tabla describe los tipos de nodo de la cyber kill chain, las categorías aplicables de cada nodo y las acciones de respuesta disponibles.

Nodo	Categoría	Medidas de respuesta
Carga de trabajo	Solucionar	• Gestionar aislamiento de red • Reiniciar carga de trabajo
	Investigar	• Copia de seguridad forense • Conexión a escritorio remoto • Ejecutar línea de comandos remota (Windows) • Ejecutar terminal (macOS)

© Acronis International GmbH, 2003-2025

Nodo	Categoría	Medidas de respuesta
	Recuperación	• Recuperación a partir de la copia de seguridad • Conmutación por error de Disaster Recovery
	Prevenir	• Parche
Proceso	Solucionar	• Detener proceso • Cuarentena
	Prevenir	• Añadir a la lista de permitidos • Añadir a la lista de bloqueados
Archivo	Solucionar	• Eliminar • Cuarentena
	Prevenir	• Añadir a la lista de permitidos • Añadir a la lista de bloqueados
Registro	Solucionar	• Eliminar
Red	Prevenir	• Añadir a la lista de permitidos • Añadir a la lista de bloqueados

Defina las acciones de respuesta para una carga de trabajo afectada

Como parte de su respuesta a un ataque, puede aplicar las siguientes acciones a las cargas de trabajo afectadas:

- **Gestionar aislamiento de red**: Le permite gestionar el aislamiento de red para una carga de trabajo con el fin de detener el movimiento lateral o las actividades de comando y control (C&C). Para obtener más información, consulte "Gestione el aislamiento de red de una carga de trabajo" (p. 1310).

© Acronis International GmbH, 2003-2025

- **Parche**: Le permite aplicar parches a una carga de trabajo para evitar futuras explotaciones de vulnerabilidades en futuros ataques potenciales. Para obtener más información, consulte "Aplicar parche a una carga de trabajo" (p. 1314).
- **Reiniciar carga de trabajo**: Le permite reiniciar una carga de trabajo inmediatamente o reiniciar una carga de trabajo según un periodo de tiempo de espera predefinido. Para obtener más información, consulte "Reiniciar una carga de trabajo" (p. 1317).
- **Copia de seguridad forense**: Permite realizar una copia de seguridad forense bajo demanda para auditorías u otros fines de investigación. Para obtener más información, consulte "Ejecutar una copia de seguridad forense bajo demanda en una carga de trabajo" (p. 1318).
- **Conexión a escritorio remoto**: Permite acceder de forma remota a la carga de trabajo que se está investigando. Para obtener más información, consulte "Conexión remota a una carga de trabajo" (p. 1319).
- **Recuperación a partir de la copia de seguridad**: Le permite recuperar todo el equipo a partir de la copia de seguridad o de archivos o carpetas específicos. Para obtener más información, consulte "Recuperación a partir de la copia de seguridad" (p. 1320).
- **Conmutación por error de Disaster Recovery**: Le permite ejecutar "Implementación de la recuperación ante desastres" (p. 1010). Tenga en cuenta que su carga de trabajo debe tener una suscripción para Advanced Disaster Recovery. Para obtener más información, consulte "Conmutación por error de Disaster Recovery" (p. 1321).

Gestione el aislamiento de red de una carga de trabajo

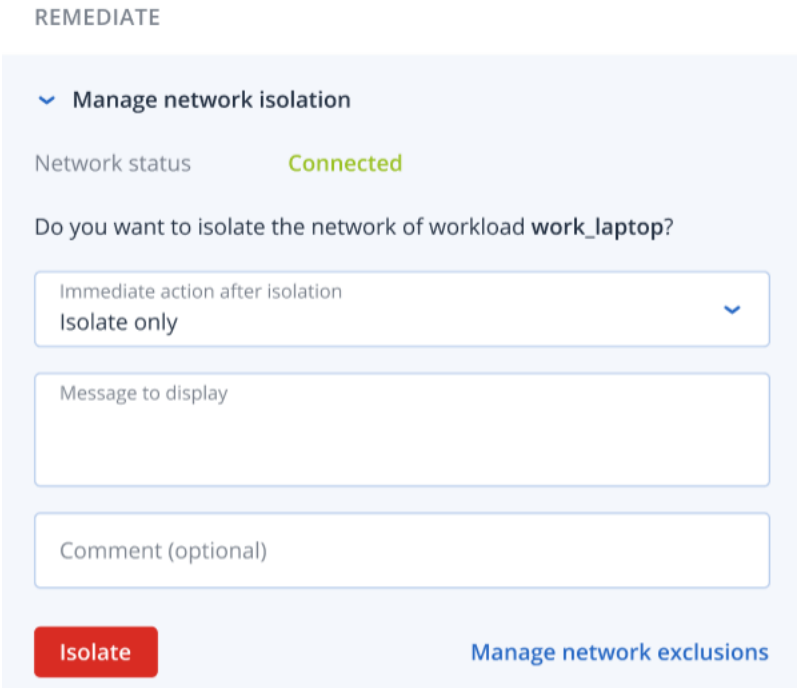
La EDR le permite gestionar el aislamiento de red para una carga de trabajo con el fin de detener el movimiento lateral o las actividades de comando y control (C&C). Hay una serie de opciones de aislamiento entre las que elegir, según sus requisitos. Tenga en cuenta que todas las tecnologías Acronis Cyber Protect son funcionales incluso si una carga de trabajo está aislada, lo que garantiza que pueda llevarse a cabo la investigación por completo.

Pasos para aislar una carga de trabajo desde la red

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo que desee solucionar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.

© Acronis International GmbH, 2003-2025

3. En la sección **Solucionar** haga clic en **Gestionar aislamiento de red**.



Nota
El valor **Estado de red** indica si la carga de trabajo está conectada o no actualmente. Si el valor muestra **Aislada**, puede volver a conectar la carga de trabajo aislada a la red, según se describe en el procedimiento siguiente. Si la carga de trabajo está offline, puede aislar la carga de trabajo; cuando la carga de trabajo vuelva a estar en línea, se pondrá automáticamente en estado **Aislada**.

4. En la lista desplegable **Acción inmediata después del aislamiento**, seleccione una de las siguientes opciones:
   - **Solo aislar**
   - **Aislar y hacer copia de seguridad de la carga de trabajo**
   - **Aislar y hacer copia de seguridad de la carga de trabajo con datos forenses**
   - **Aislar y apagar la carga de trabajo**

   Para obtener más información acerca de cómo definir dónde hacer una copia de seguridad de la carga de trabajo y las opciones de cifrado, consulte "Gestión de la copia de seguridad y recuperación de cargas de trabajo y archivos" (p. 499).
5. [Opcional] En el campo **Mensaje a mostrar**, añada un mensaje para mostrar a los usuarios finales cuando accedan a la carga de trabajo aislada. Por ejemplo, puede informar a los usuarios de que la carga de trabajo ahora está aislada y que el acceso a la red dentro y fuera de la carga de trabajo no está disponible actualmente. Tenga en cuenta que este mensaje también se muestra como una notificación de Tray Monitor y se sigue mostrando hasta que el usuario descarga el mensaje.

© Acronis International GmbH, 2003-2025

6. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
7. Haga clic en **Gestionar exclusiones de red** para añadir puertos, URL, nombres de host y direcciones IP que tendrán acceso a la carga de trabajo durante el aislamiento. Para obtener más información, consulte Cómo gestionar las exclusiones de red.
8. Haga clic en **Aislar**.
   La carga de trabajo está aislada. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Nota
La carga de trabajo también se muestra como **Aislada** en el menú **Cargas de trabajo** de la consola de Cyber Protect. También puede aislar una o varias cargas de trabajo desde el menú **Cargas de trabajo > Cargas de trabajo con agentes**; seleccionar las cargas de trabajo correspondientes y, en la barra lateral de la derecha, seleccionar **Gestionar aislamiento de red**. En el diálogo mostrado, puede gestionar las exclusiones de red y hacer clic en **Aislar** o **Aislar todas** para aislar las cargas de trabajo seleccionadas.

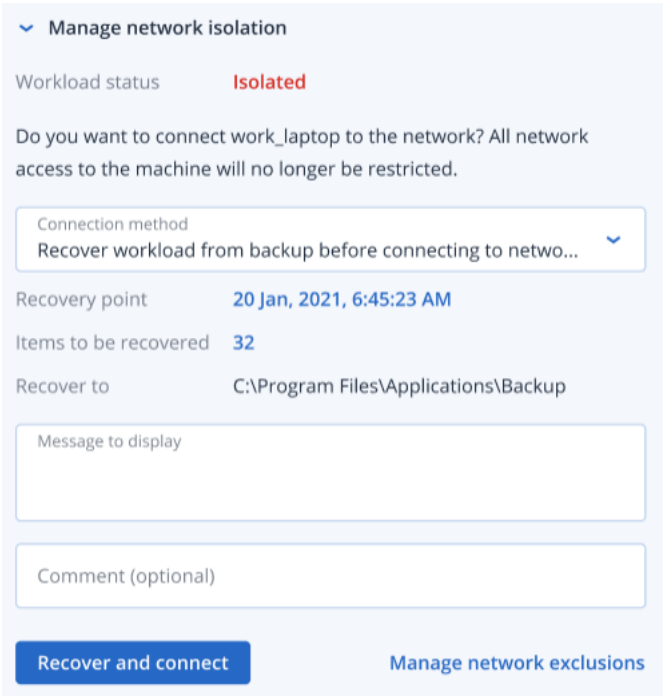
Pasos para volver a conectar una carga de trabajo aislada a la red

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo que desee reconectar.

Nota
Si la carga de trabajo aislada está offline actualmente, aún así puede volver a conectarla a la red; cuando la carga de trabajo vuelva a estar en línea, se pondrá automáticamente en estado **Conectada**.

2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Solucionar** haga clic en **Gestionar aislamiento de red**.
4. Seleccione una de las siguientes opciones:
   - **Conectar a la red inmediatamente**: La carga de trabajo se reconecta a la red.
   - **Recuperar carga de trabajo a partir de la copia de seguridad al conectarse a la red**: Seleccione un punto de recuperación desde el cual recuperar la carga de trabajo.
     a. En el campo **Punto de recuperación**, haga clic en **Seleccionar**.
     b. En la barra lateral que se muestra, seleccione el punto de recuperación que corresponda.
     c. Haga clic en **Recuperar > Toda la carga de trabajo** para recuperar todos los archivos y carpetas de la carga de trabajo.
        O
        Haga clic en **Recuperar > Archivos/carpetas** para recuperar archivos y carpetas específicos de la carga de trabajo. Se le pedirá que seleccione los archivos o carpetas que desee. Una vez seleccionados, puede ver la lista de elementos haciendo clic en el valor correspondiente del campo **Elementos para recuperar**.

© Acronis International GmbH, 2003-2025



Nota
Si el punto de recuperación que selecciona está cifrado, se le pedirá la contraseña.

5. [Opcional] Seleccione la casilla de verificación **Reinicie la carga de trabajo automáticamente, si es necesario**. Esta opción solo aplica si ha seleccionado **Recuperar > Toda la carga de trabajo** en el paso 4.
6. [Opcional] En el campo **Mensaje a mostrar**, añada un mensaje para mostrar a los usuarios finales cuando accedan a la carga de trabajo conectada. Por ejemplo, puede informar a los usuarios de que se ha restaurado una copia de seguridad a la carga de trabajo y que el acceso a la red dentro y fuera de la carga de trabajo se ha reanudado.
7. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
8. Haga clic en **Conectar** si ha seleccionado **Conectar a la red inmediatamente** en el paso 4.
   O
   Haga clic en **Recuperar y conectar** si ha seleccionado **Recuperar carga de trabajo a partir de la copia de seguridad al conectarse a la red** en el paso 4.
   La carga de trabajo se volverá a conectar a la red y ya no se limitará el acceso de toda la red a la carga de trabajo.

© Acronis International GmbH, 2003-2025

Nota
También puede conectar una o varias cargas de trabajo aisladas desde el menú **Cargas de trabajo > Cargas de trabajo con agentes** en la consola de Cyber Protect; seleccione las cargas de trabajo correspondientes y, en la barra lateral de la derecha, seleccione **Gestionar aislamiento de red**. En el cuadro de diálogo, haga clic en **Conectar** o **Conectar todo** para volver a conectar las cargas de trabajo seleccionadas a la red.

Pasos para gestionar exclusiones de red

Nota
Incluso si todas las tecnologías de Acronis Cyber Protect funcionan cuando la carga de trabajo está en aislamiento, es posible que haya casos en los que necesite que se establezcan más conexiones de red (por ejemplo, puede que tenga que cargar un archivo desde la carga de trabajo a un directorio compartido). En estos escenarios, puede añadir una exclusión de red, pero asegúrese de eliminar cualquier amenaza antes de añadir la exclusión.

1. En la sección **Solucionar** de la pestaña **Medidas de respuesta**, haga clic en **Gestionar exclusiones de red**.
2. En la barra lateral de exclusiones de red, añada las exclusiones que correspondan. Para cada una de las opciones disponibles, (Puertos, direcciones URL y nombres de host o direcciones IP) haga lo siguiente:
   a. Haga clic en **Agregar** e introduzca los puertos, direcciones URL, nombres de host o direcciones IP correspondientes.
   b. En la lista desplegable **Dirección del tráfico**, seleccione entre **Conexiones entrantes y salientes**, **Solo conexiones entrantes** o **Solo conexiones salientes**.
   c. Haga clic en **Agregar**.
3. Haga clic en **Guardar**.

Aplicar parche a una carga de trabajo

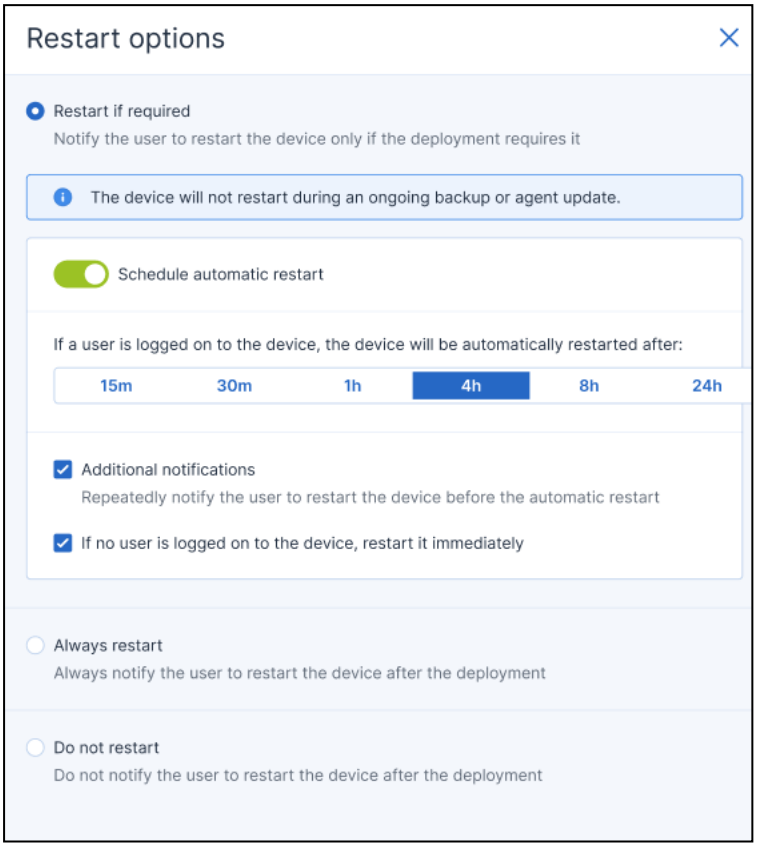
La EDR detecta automáticamente si una carga de trabajo requiere un parche y le permite aplicar parches a la carga de trabajo para evitar futuras explotaciones de vulnerabilidades en futuros ataques potenciales. Tenga en cuenta que esta funcionalidad solo está disponible si la carga de trabajo del partner tiene una suscripción a RMM.

Pasos para aplicar parches a una carga de trabajo

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo al que desee aplicar el parche.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Solucionar** haga clic en **Parche**.
4. En el campo **Parches a instalar**, haga clic en **Seleccionar**. En el diálogo que se muestra, seleccione los parches que correspondan y haga clic en **Seleccionar**.

© Acronis International GmbH, 2003-2025

5. En el campo **Opciones de reinicio**, haga clic en el enlace que se muestra. Se mostrará el cuadro de diálogo de **Opciones de reinicio**.
6. Seleccione si quiere que la carga de trabajo se reinicie después de instalar los parches.



La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se

© Acronis International GmbH, 2003-2025

Opción	Descripción
se reiniciará automáticamente después de:	reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

7. Haga clic en **Guardar**.
8. En la pestaña **Medidas de respuesta**, haga clic en **Parche**.
   Se ejecutará el parche seleccionado. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

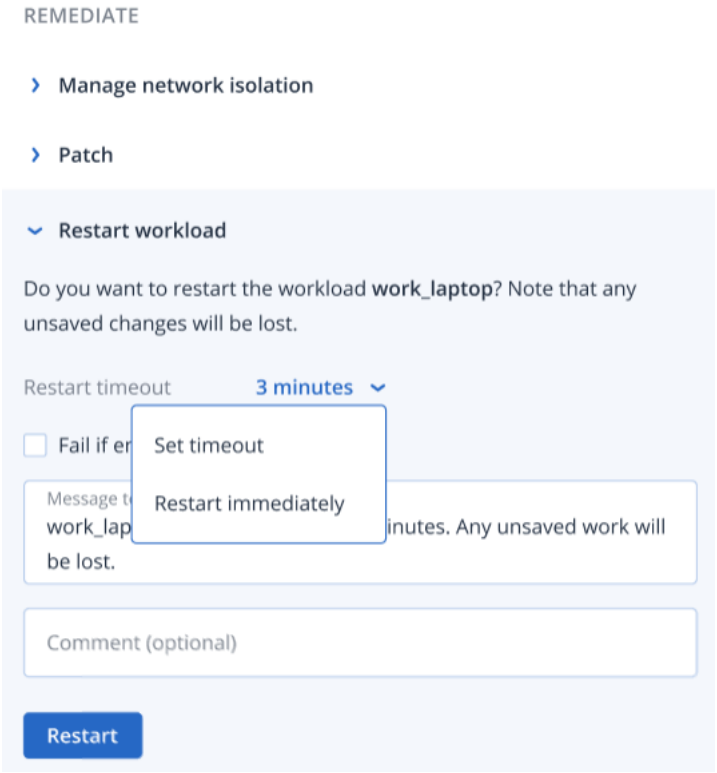
© Acronis International GmbH, 2003-2025

Reiniciar una carga de trabajo

Como parte de su respuesta de solución a un ataque, la EDR le permite reiniciar una carga de trabajo inmediatamente o reiniciar una carga de trabajo según un periodo de tiempo de espera predefinido.

Pasos para reiniciar una carga de trabajo

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo para el que desee planificar un reinicio.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Solucionar** haga clic en **Reiniciar carga de trabajo**.



4. En el campo **Tiempo de espera del reinicio**, haga clic en el enlace mostrado y seleccione una de las siguientes opciones:
   - **Establecer tiempo de espera**: En el diálogo Reiniciar tiempo de espera, establezca el periodo de reinicio para la carga de trabajo y haga clic en **Guardar**.
   - **Reiniciar inmediatamente**: Seleccione para reiniciar la carga de trabajo inmediatamente.
5. [Opcional] Seleccione la casilla de verificación **Error si el usuario ha iniciado sesión** para asegurarse de que la carga de trabajo no se reinicia si el usuario ha iniciado sesión.
6. En el campo **Mensaje a mostrar**, añada un mensaje para mostrar a los usuarios cuando accedan a la carga de trabajo aislada.
7. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.

© Acronis International GmbH, 2003-2025

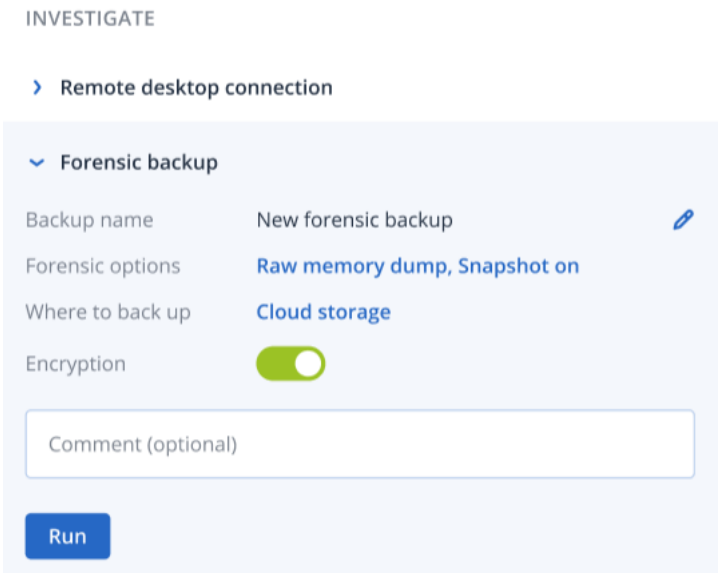
8. Haga clic en **Reiniciar**.
   La carga de trabajo está configurada para que se reinicie según la planificación definida. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Ejecutar una copia de seguridad forense bajo demanda en una carga de trabajo

Como parte de la investigación de un ataque, la EDR permite ejecutar una copia de seguridad forense bajo demanda para auditorías u otros fines de investigación. Tenga en cuenta que esta característica solo está disponible si la carga de trabajo del partner tiene una suscripción a Advanced Backup.

Para ejecutar una copia de seguridad forense

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo en la que desee ejecutar una copia de seguridad forense.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Investigar**, haga clic en **Copia de seguridad forense**.



4. [Opcional] En el campo **Nombre de la copia de seguridad**, haga clic en el icono de edición para editar el nombre de la copia de seguridad.
5. En el campo **Opciones forenses**, haga clic en el enlace que se muestra. En el diálogo Opciones forenses, seleccione una de las siguientes opciones:
   - **Recopilar un volcado de memoria sin procesar**
   - **Recopilar un volcado de memoria del kernel**

   También puede seleccionar la casilla de verificación **Instantánea de procesos en ejecución** para añadir información sobre los procesos que están en ejecución cuando se inicia la copia de seguridad. Esta información se almacena en una imagen de copia de seguridad.
   Haga clic en **Guardar** para cerrar el diálogo Opciones forenses.

© Acronis International GmbH, 2003-2025

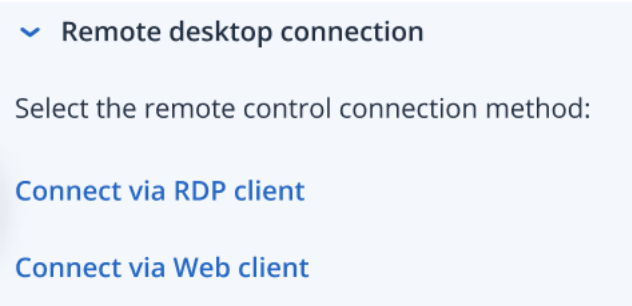
6. En el campo **Dónde guardar las copias de seguridad**, haga clic en el enlace que se muestra para definir una ubicación para la copia de seguridad.
7. [Opcional] Haga clic en la opción **Cifrado** para habilitar el cifrado. En el cuadro que se muestra, introduzca la contraseña para la copia de seguridad cifrada y seleccione el algoritmo de cifrado correspondiente.
8. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
9. Haga clic en **Ejecutar**.
   Se iniciará la copia de seguridad forense. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Conexión remota a una carga de trabajo

Como parte de la investigación de un ataque, la EDR permite acceder de forma remota a la carga de trabajo que se está investigando.

Para conectarse de forma remota a una carga de trabajo

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo a la que desee conectarse de forma remota.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Investigar**, haga clic en **Conexión a escritorio remoto**.



4. Seleccione uno de los siguientes métodos de conexión remota:
   - **Conectar mediante cliente RDP**: Este método le pedirá que descargue e instale el cliente de conexión a escritorio remoto. A continuación, podrá conectarse de forma remota a una carga de trabajo desde la consola de Cyber Protect.
   - **Conectar mediante cliente web**: Este método no requiere la instalación de un cliente RDP en la carga de trabajo. Se le redirigirá a la pantalla de inicio de sesión, donde debe introducir sus credenciales para el equipo remoto.

   Cuando se haya iniciado la conexión remota, puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

© Acronis International GmbH, 2003-2025

Ejecutar la línea de comando remota

Como parte de su investigación sobre un ataque, puede ejecutar de forma remota la línea de comando de la carga de trabajo en investigación.

Pasos para ejecutar de forma remota la línea de comando de una carga de trabajo

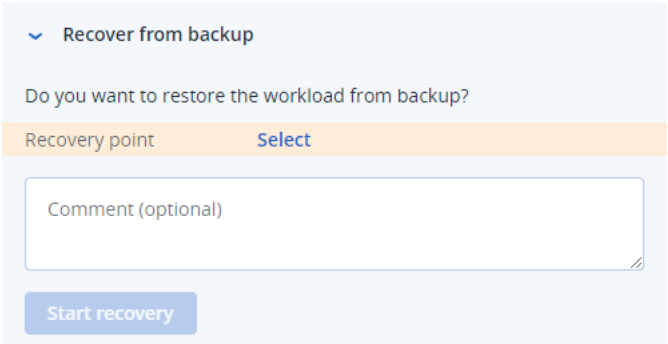
1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo a la que desea conectarse de forma remota.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. Dependiendo del sistema operativo de la carga de trabajo, realice una de las siguientes acciones:
   - [Para cargas de trabajo en Windows] En la sección **Investigar**, expanda **Interfaz de línea de comandos remota** y, a continuación, haga clic en **Ejecutar línea de comandos**.
   - [Para cargas de trabajo en macOS] En la sección **Investigar**, expanda **Terminal remoto** y, a continuación, haga clic en **Ejecutar terminal**.

Recuperación a partir de la copia de seguridad

Como parte de su respuesta de recuperación a un ataque, la EDR, le permite recuperar todo el equipo a partir de la copia de seguridad o de archivos o carpetas específicos.

Pasos para recuperar su carga de trabajo a partir de la copia de seguridad

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo que desee recuperar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Recuperación**, haga clic en **Recuperación desde la copia de seguridad**.



4. En el campo **Punto de recuperación**, haga clic en **Seleccionar** y ejecute los siguientes pasos:
   a. En la barra lateral que se muestra, seleccione el punto de recuperación que corresponda.
   b. Haga clic en **Recuperar > Toda la carga de trabajo** para recuperar todos los archivos y carpetas de la carga de trabajo.
   O
   Haga clic en **Recuperar > Archivos/carpetas** para recuperar archivos y carpetas específicos de la carga de trabajo. Se le pedirá que seleccione los archivos o carpetas que desee. Una vez seleccionados, puede los elementos seleccionados para la recuperación haciendo clic en el valor correspondiente del campo **Elementos para recuperar**.

© Acronis International GmbH, 2003-2025

Nota
Si el punto de recuperación que selecciona está cifrado, se le pedirá la contraseña.

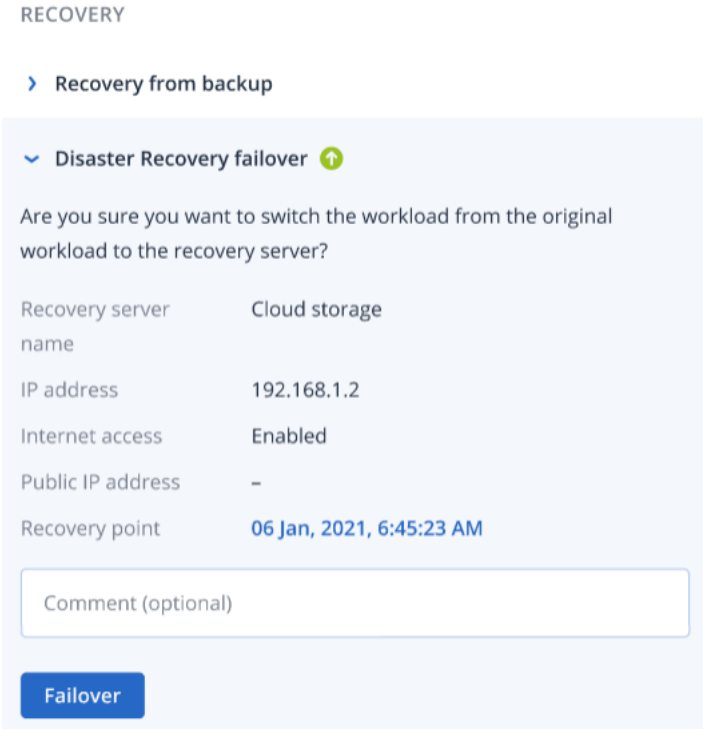
5. [Opcional] Seleccione la casilla de verificación **Reinicie la carga de trabajo automáticamente**. Esta opción solo aplica si ha seleccionado **Recuperar > Toda la carga de trabajo** en el paso 4.
6. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
7. Haga clic en **Iniciar recuperación**.
   El proceso para recuperar los inicios de la carga de trabajo. Puede ver el progreso para esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Conmutación por error de Disaster Recovery

Como parte de su respuesta de recuperación a un ataque, con la EDR puede ejecutar "Implementación de la recuperación ante desastres" (p. 1010), lo que le permite cambiar la carga de trabajo al servidor de recuperación. Tenga en cuenta que su carga de trabajo debe tener una suscripción para Advanced Disaster Recovery.

Pasos para ejecutar la conmutación por error de Disaster Recovery

1. En la cyber kill chain, haga clic en el nodo de la carga de trabajo que desee recuperar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Recuperación**, haga clic en **Conmutación por error de Disaster Recovery**.



© Acronis International GmbH, 2003-2025

4. En el campo **Punto de recuperación**, ejecute los siguientes pasos:
   a. Haga clic en la fecha del punto de recuperación actual para seleccionar un punto de recuperación.
   b. En la barra lateral que se muestra, seleccione el punto de recuperación que corresponda.

   Nota
   Si tiene una suscripción a Advanced Disaster Recovery, puede seleccionar el servidor de recuperación que corresponda (la máquina virtual offline) creado en Disaster Recovery. Si no tiene una suscripción, se le pedirá que configure Disaster Recovery.

5. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
6. Haga clic en **Conmutación por error**.
   La carga de trabajo se traslada al servidor de recuperación. Puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Defina las acciones de respuesta para un proceso sospechoso

Como parte de su respuesta de solución a un ataque, puede aplicar las siguientes acciones a los procesos sospechosos:

- Detener un proceso (consulte más adelante)
- Poner en cuarentena un proceso (consulte más adelante)
- Revertir los cambios realizados por un proceso (consulte más adelante)
- Agregar el proceso a la lista de permitidos o la lista de bloqueados de un plan de protección (consulte "Añade o elimina un proceso, archivo o red en la lista de bloqueados o permitidos del plan de protección" (p. 1328))

Pasos para detener un proceso sospechoso

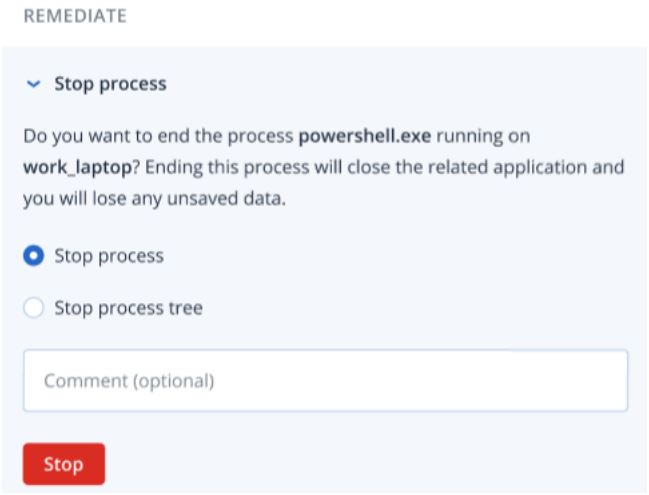
1. En la cyber kill chain, haga clic en el nodo del proceso que desee solucionar.

   Nota
   Los procesos críticos de Windows o los que no se ejecutan no se pueden detener y se deshabilitarán en la cyber kill chain.

2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.

© Acronis International GmbH, 2003-2025

3. En la sección **Solucionar** haga clic en **Detener proceso**.



4. Seleccione una de las siguientes opciones:
   - **Detener proceso** (detiene el proceso específico)
   - **Detener árbol de procesos** (detiene el proceso específico y todos los procesos secundarios)
5. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
6. Haga clic en **Detener**. El proceso se detendrá.

Nota
Se cerrará la aplicación relacionada y se perderán los datos que no se hayan guardado.

También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Pasos para poner en cuarentena un proceso sospechoso

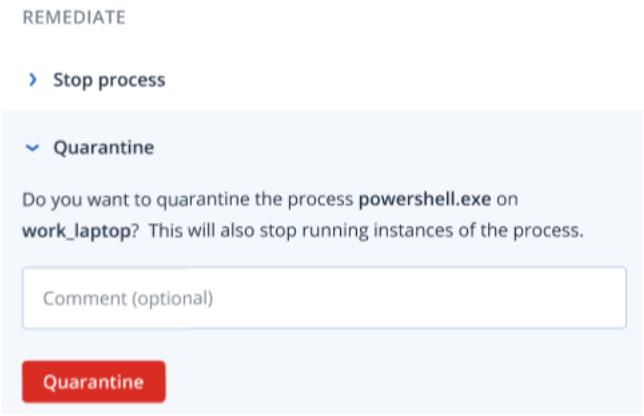
1. En la cyber kill chain, haga clic en el nodo del proceso que desee poner en cuarentena.

Nota
Los procesos críticos de Windows no se pueden poner en cuarentena y se deshabilitarán en la cyber kill chain.

2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.

© Acronis International GmbH, 2003-2025

3. En la sección **Solucionar** haga clic en **Cuarentena**.



4. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
5. Haga clic en **Cuarentena**. El proceso se detendrá y se pondrá en cuarentena.

> **Nota**
> El proceso se añade y se gestiona en la sección de cuarentena disponible en protección antimalware.

También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Cómo revertir cambios

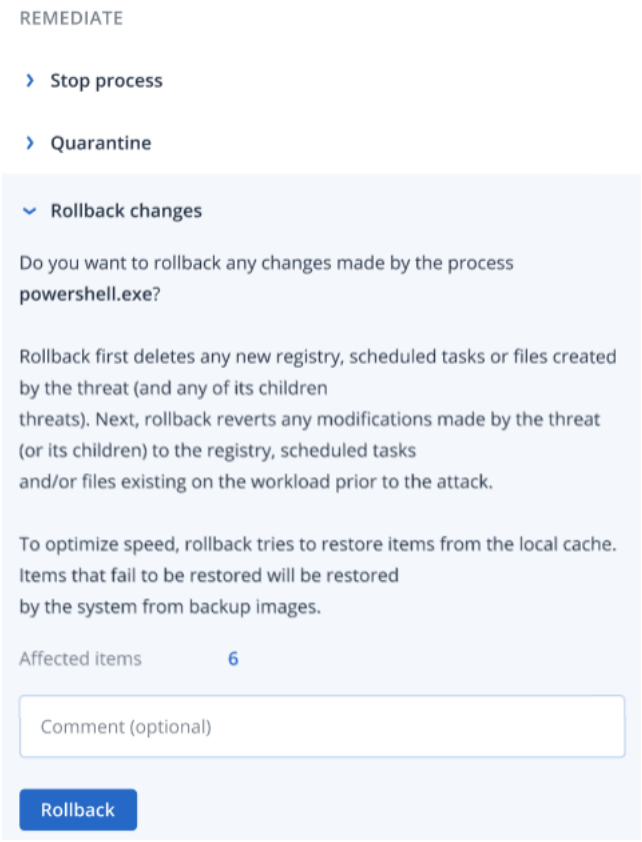
1. En la cyber kill chain, haga clic en el nodo del proceso para el que desee revertir los cambios.

> **Nota**
> Esta acción solo está disponible para los nodos de detección (que se muestran como nodos rojos o amarillos).

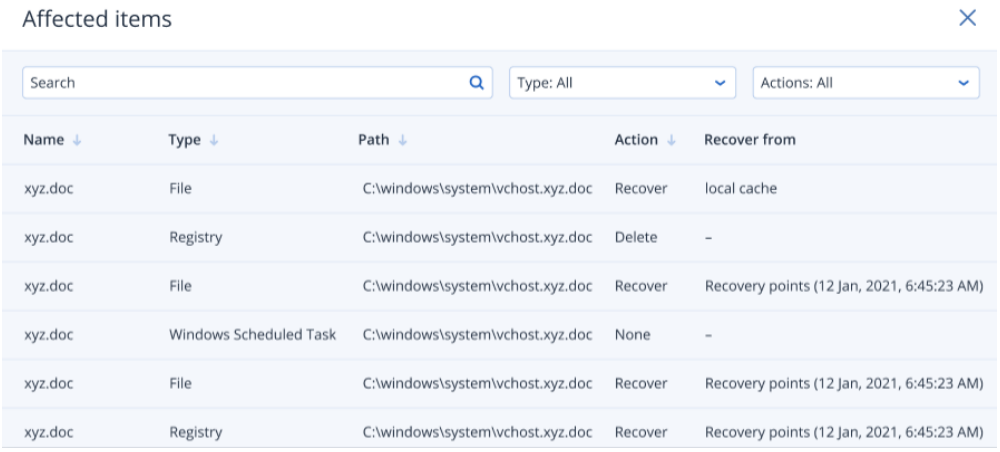
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.

© Acronis International GmbH, 2003-2025

3. En la sección **Solucionar** haga clic en **Revertir cambios**.



4. Para ver los elementos afectados por los cambios de la reversión, haga clic en el enlace **Elementos afectados**. El diálogo que aparece muestra todos los elementos (archivos, registro, tareas programadas) que la restauración revertirá y con qué acción (**Eliminar**, **Recuperar**, o **Ninguna**). Asimismo, puede ver si los elementos restaurados se recuperarán desde la caché local o desde puntos de recuperación de la copia de seguridad.



5. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
6. Haga clic en **Reversión**. La funcionalidad reversión revierte los cambios de cualquier registro, archivo o tarea programada que haya hecho el proceso en los siguientes pasos:

© Acronis International GmbH, 2003-2025

a. Se elimina cualquier entrada nueva (registro, tareas programadas, archivos) creada por la amenaza (y sus procesos secundarios).
b. Se revierte cualquier modificación que la amenaza (y sus procesos secundarios) haya hecho al registro, tareas programadas o archivos que estaban en la carga de trabajo antes del ataque.
c. La reversión intenta recuperar los elementos desde la caché local. Para los elementos que no se pueden recuperar, la EDR los recuperará automáticamente desde las imágenes de copias de seguridad limpias.

También puede ver la acción de reversión en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

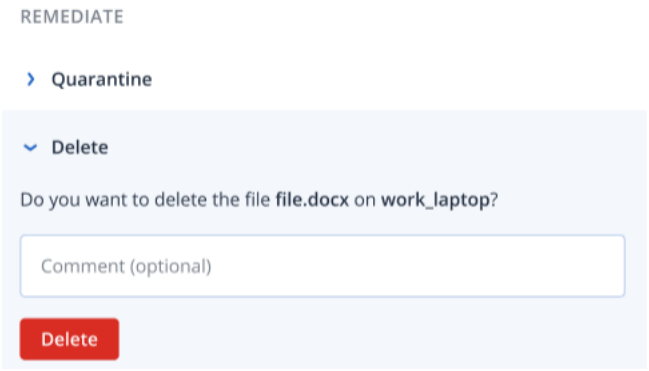
Defina las acciones de respuesta para un archivo sospechoso

Como parte de su respuesta a una solución, puede aplicar las siguientes acciones a los archivos sospechosos:

- Eliminar un archivo (consulte más adelante)
- Poner en cuarentena un archivo (consulte más adelante)
- Añadir el archivo a la lista de permitidos o la lista de bloqueados de un plan de protección (consulte "Añade o elimina un proceso, archivo o red en la lista de bloqueados o permitidos del plan de protección" (p. 1328))

Pasos para eliminar un archivo sospechoso

1. En la cyber kill chain, haga clic en el nodo del archivo que desee solucionar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Solucionar** haga clic en **Eliminar**.

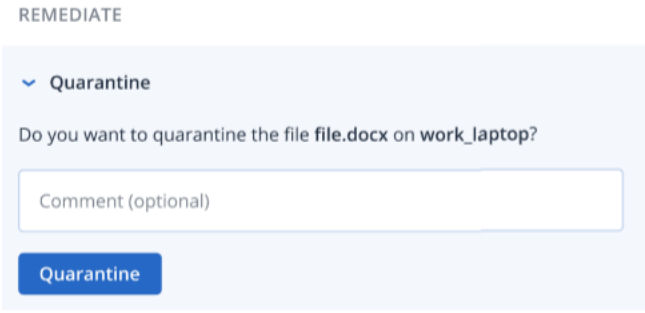


4. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
5. Haga clic en **Eliminar**.
   Se ha eliminado el archivo. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

© Acronis International GmbH, 2003-2025

Pasos para poner en cuarentena un archivo sospechoso

1. En la cyber kill chain, haga clic en el nodo del archivo que desee solucionar.
2. En la barra lateral que se muestra, vaya a **Medidas de respuesta**.
3. En la sección **Solucionar** haga clic en **Cuarentena**.



4. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
5. Haga clic en **Cuarentena**.
   El archivo se ha puesto en cuarentena. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

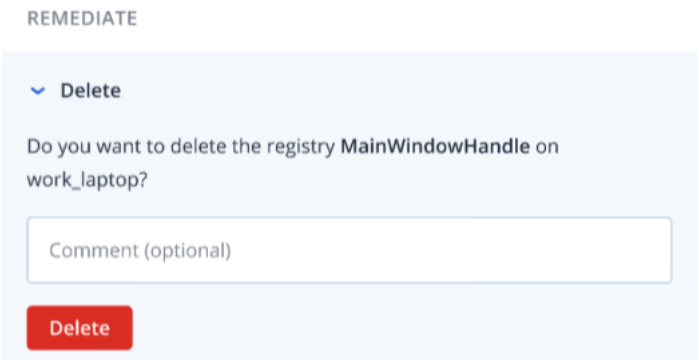
Defina las acciones de respuesta para una entrada de registro sospechosa

Como parte de su respuesta de solución a un ataque, puede eliminar las entradas de registro sospechosas.

Esta opción está disponible para nodos de la cyber kill chain del registro.

Pasos para eliminar una entrada de registro sospechosa

1. En la cyber kill chain, haga clic en el nodo que desee solucionar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Solucionar** haga clic en **Eliminar**.



4. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.

© Acronis International GmbH, 2003-2025

5. Haga clic en **Eliminar**.
   La entrada del registro se ha eliminado. También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Añade o elimina un proceso, archivo o red en la lista de bloqueados o permitidos del plan de protección

Como parte de su respuesta de prevención frente a un ataque, puede añadir un nodo a la lista de permitidos o a la lista de bloqueados de un plan de protección.

Puede añadir un nodo a una lista de permitidos si considera que es seguro y desea evitar que se detecte en el futuro. Añada un nodo a una lista de bloqueados para que deje de ejecutarse en el futuro.

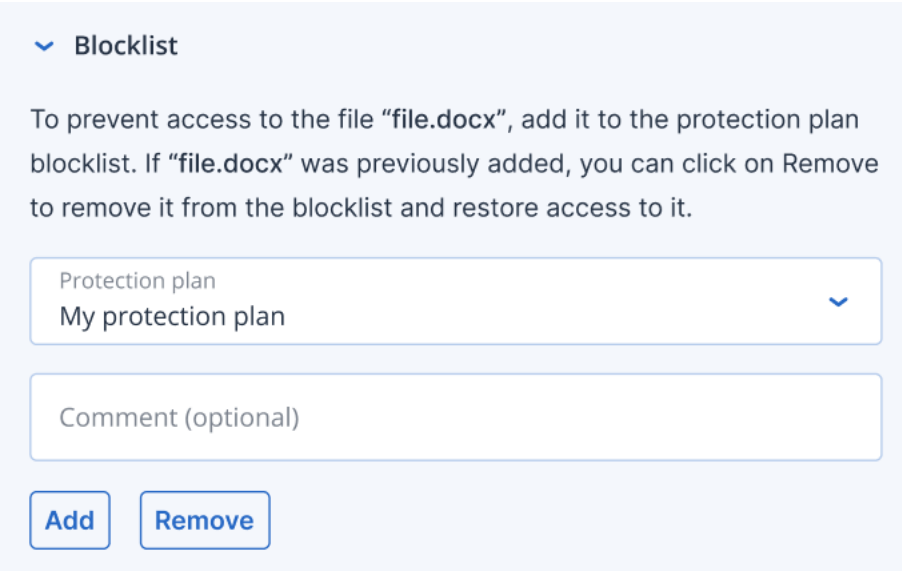
También puede eliminar un nodo de la lista de permitidos o bloqueados para permitir o prevenir cualquier acceso futuro al nodo.

Esta opción está disponible para los siguientes nodos de cyber kill chain:

- Proceso
- Archivo
- Red

Para añadir o eliminar un proceso, archivo o red en la lista de bloqueados del plan de protección

1. En la cyber kill chain, haga clic en el proceso, archivo o nodo de red que desee remediar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Prevenir**, haga clic en el icono de flecha junto a **Lista de bloqueados**.



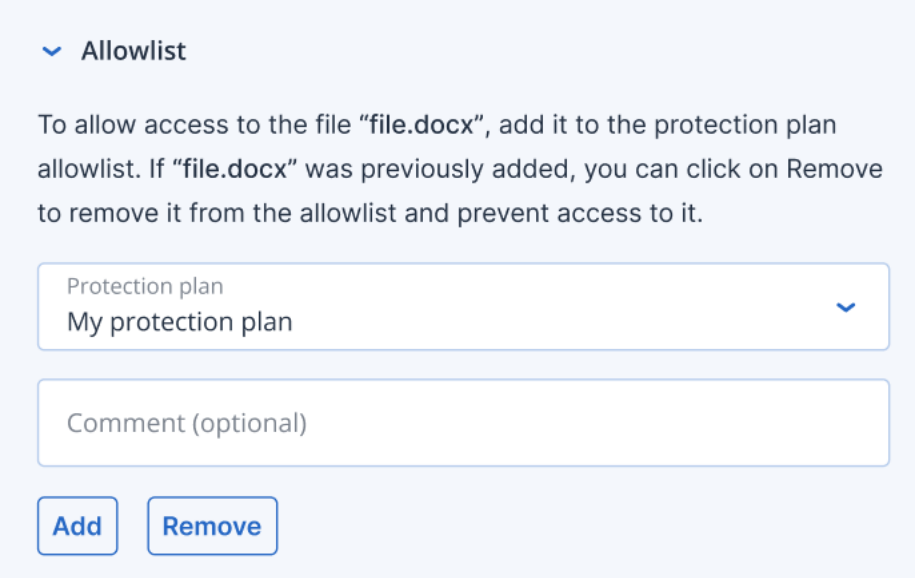
4. Seleccione los planes de protección correspondientes a los que desee aplicar esta acción.

© Acronis International GmbH, 2003-2025

5. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
6. Haga clic en **Agregar**.
   La acción se implementa, y se evitará que el proceso, archivo o red se inicie en el futuro.
   Alternativamente, si el proceso, archivo o red se añadió previamente a la lista de bloqueados y ahora desea eliminarlo de ella, haga clic en **Eliminar**. Esto permitirá el acceso futuro al nodo.
   La acción de adición o eliminación también se puede ver en las pestañas de **Actividades** tanto del nodo individual como de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

Para añadir o eliminar un proceso, archivo o red en la lista de permitidos del plan de protección

1. En la cyber kill chain, haga clic en el proceso, archivo o nodo de red que desee remediar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Medidas de respuesta**.
3. En la sección **Prevenir**, haga clic en el icono de flecha junto a **Lista de permitidos**.



4. Seleccione los planes de protección correspondientes a los que desee aplicar esta acción.
5. [Opcional] Añada un comentario. Este comentario puede verse en la pestaña **Actividades** (para un único nodo o todo el incidente) y puede ayudarle (o a sus colegas) a recordar por qué se llevó a cabo esa acción cuando vuelva a analizar el incidente.
6. Haga clic en **Agregar**.
   La acción se implementa y se evitará la detección del proceso, archivo o red en el futuro.
   Alternativamente, si el proceso, archivo o red se agregó previamente a la lista de permitidos y ahora desea eliminarlos de la lista de permitidos, haga clic en **Eliminar**. Esto evitará cualquier acceso futuro al nodo.
   La acción de adición o eliminación también se puede ver en las pestañas de **Actividades** tanto del nodo individual como de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

© Acronis International GmbH, 2003-2025

Trabajar con flujos de trabajo automatizados

Puede utilizar los flujos de trabajo automatizados de Acronis para aplicar un conjunto de acciones predefinidas que pueden solucionar automáticamente los incidentes en Endpoint Detection and Response (EDR) y Extended Detection and Response (XDR). Estos flujos de trabajo, o manuales, le permiten optimizar sus operaciones de seguridad para mejorar el tiempo de respuesta, mientras que reducen la carga operativa para gestionar y responder a los incidentes de seguridad.

Hay seis flujos de trabajo EDR predefinidos, cada uno de los cuales se puede configurar según sea necesario. Para obtener más información, consulte "Flujos de trabajo de Endpoint Detection and Response (EDR)" (p. 1330).

Para acceder a los flujos de trabajo automatizados, vaya a **Gestión > Flujos de trabajo**. La lista de flujos de trabajo que se muestra indica cuáles están habilitados o deshabilitados, su última hora de ejecución y su estado.

Flujos de trabajo de Endpoint Detection and Response (EDR)

Hay seis flujos de trabajo de EDR predeterminados que puede configurar según sus requisitos:

- Amenaza en cuarentena (cuando se crea un incidente de EDR)
- Amenaza en cuarentena (cuando se actualiza un incidente de EDR)
- Aislar la carga de trabajo (cuando se crea un incidente de EDR)
- Aislar la carga de trabajo (cuando se actualiza un incidente de EDR)
- Incidente de malware que requiere atención
- Incidente que requiere atención

La siguiente tabla describe los desencadenantes, las condiciones y las acciones predeterminadas aplicables a cada flujo de trabajo. Para obtener más información sobre cómo modificar estas condiciones y acciones, consulte "Configuración de un flujo de trabajo automatizado de Endpoint Detection and Response (EDR)" (p. 1333).

© Acronis International GmbH, 2003-2025

Flujo de trabajo	Activación	Condiciones	Acciones
Amenaza en cuarentena	Incidente de EDR creado	Estado de la amenaza = "No mitigada" Y Estado del incidente = "No iniciado" Y Gravedad = "Alta" Y Tipo de incidente = "Proceso detectado" O "Malware detectado"	1. Detener el proceso. 2. Poner el proceso en cuarentena. 3. Añada un comentario. El texto predeterminado del comentario es "<Workflow name>: amenaza de gravedad alta en cuarentena". 4. Cerrar el incidente.
Amenaza en cuarentena	Incidente de EDR actualizado		
Aislar la carga de trabajo	Incidente de EDR creado	Estado de la amenaza = "No mitigada" Y Estado del incidente = "No iniciado" Y Gravedad = "Crítico" Y Veredicto = "Malicioso" Y Nivel de positividad > 9 Y Tipo de incidente = "Proceso detectado" O "Malware detectado"	1. Detener el proceso. 2. Poner el proceso en cuarentena. 3. Aislar la carga de trabajo 4. Añada un comentario. El texto predeterminado del comentario es "<Workflow name>: la carga de trabajo <Workload name> se ha aislado después de la detección de malware crítico". 5. Enviar correo electrónico a los usuarios de la consola de Cyber Protect seleccionados.
Aislar la carga de trabajo	Incidente de EDR actualizado		
Incidente de malware que requiere atención	Incidente de EDR creado	Estado de la amenaza = "No mitigada" Y	1. Detener el proceso. 2. Poner el proceso

© Acronis International GmbH, 2003-2025

Flujo de trabajo	Activación	Condiciones	Acciones
		Estado del incidente = "No iniciado" Y Antigüedad del incidente > 8 horas Y Gravedad = "Alta" O "Crítica" Y Veredicto = "Malicioso" Y Tipo de incidente = "Detección de malware"	en cuarentena. 3. Añada un comentario. El texto predeterminado del comentario es "<Workflow name>: cuarentena de amenaza de gravedad alta/crítica debido a que no se investigó durante 8 h". 4. Enviar correo electrónico a los usuarios de la consola de Cyber Protect seleccionados.
Incidente que requiere atención	Incidente de EDR creado	Estado de la amenaza = "No mitigada" Y Estado del incidente = "No iniciado" Y Antigüedad del incidente > 24 horas Y Gravedad = "Alta" O "Crítica" Y Veredicto = "Malicioso"	1. Detener el proceso. 2. Poner el proceso en cuarentena. 3. Añada un comentario. El texto predeterminado del comentario es "<Workflow name>: cuarentena de amenaza de gravedad alta/crítica debido a que no se investigó durante 24 h". 4. Enviar correo electrónico a los usuarios de la consola de Cyber Protect seleccionados.

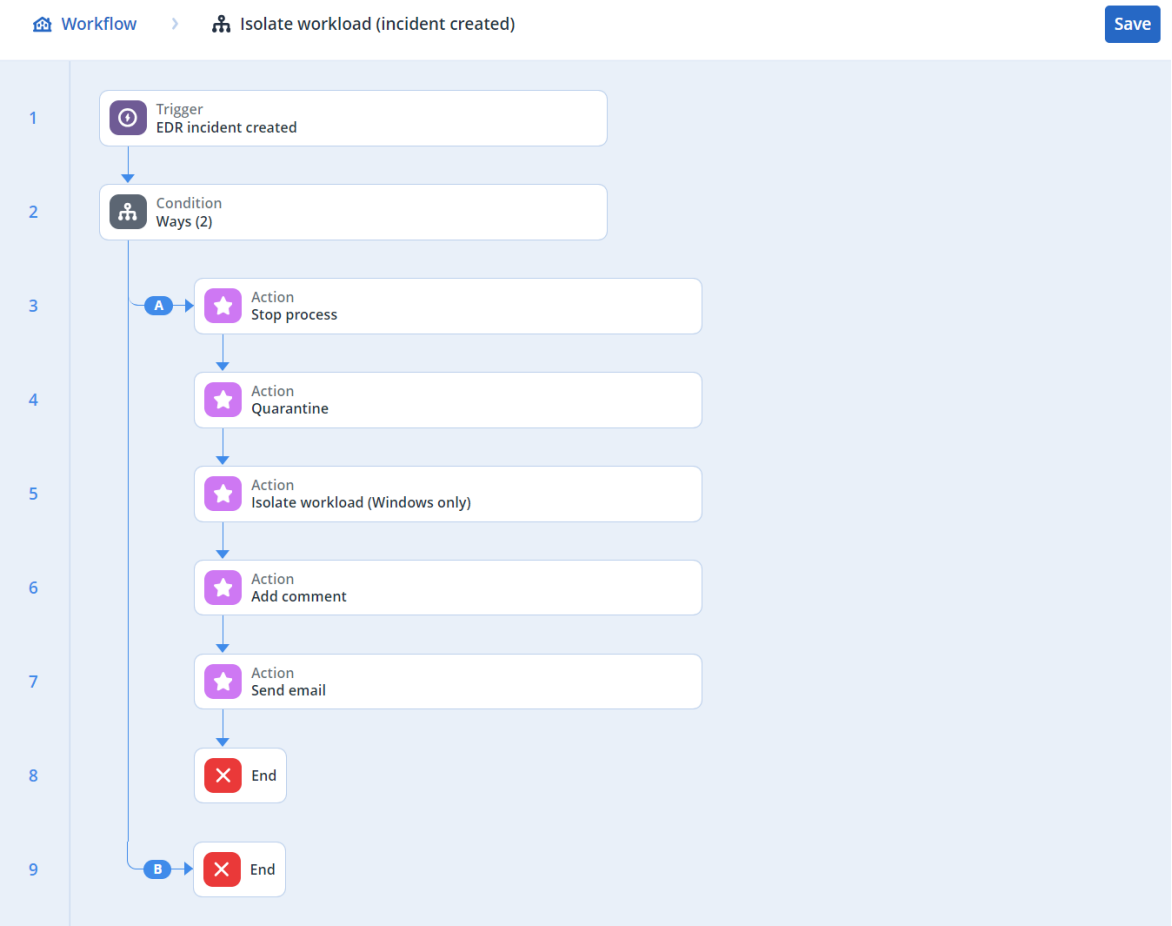
© Acronis International GmbH, 2003-2025

Configuración de un flujo de trabajo automatizado de Endpoint Detection and Response (EDR)

Puede configurar cualquiera de los flujos de trabajo de EDR predefinidos según sus requisitos.

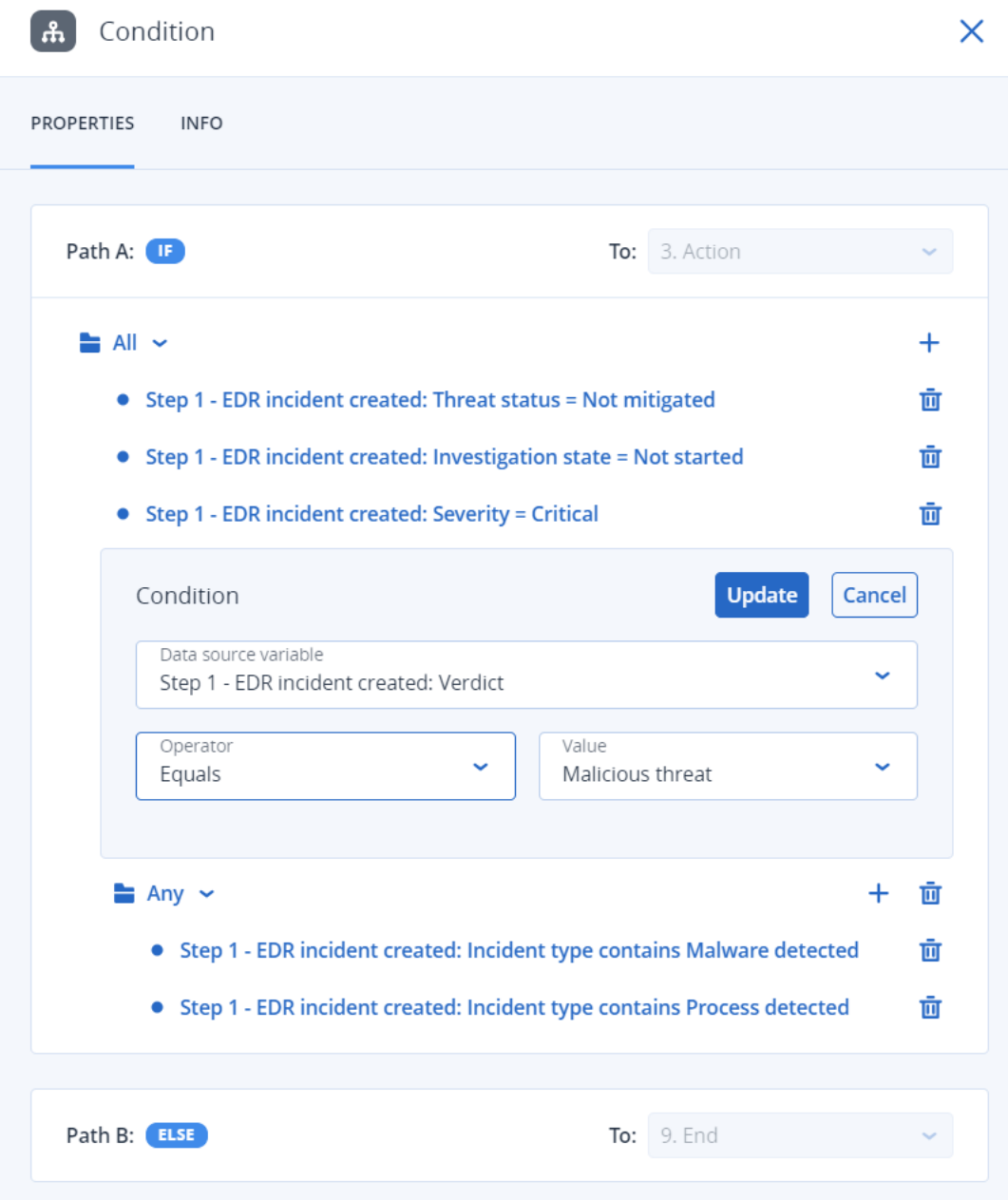
Pasos para configurar un flujo de trabajo de EDR

1. En la consola de Cyber Protect, vaya a **Administración > Flujos de trabajo**.
2. En la columna más a la derecha, haga clic en el icono de elipsis (...) en la fila del flujo de trabajo que desea configurar y después seleccione **Abrir**.
   O bien, haga clic en el flujo de trabajo correspondiente y en el panel que se muestra, haga clic en **Abrir**.
   Se muestran las condiciones y acciones del flujo de trabajo.



3. Para ver y modificar cualquiera de las condiciones del flujo de trabajo, haga clic en el bloque **Condición**.

© Acronis International GmbH, 2003-2025



El bloque de condición define un conjunto de condiciones que deben ejecutarse como parte del flujo de trabajo y consta de dos tipos de bloque:

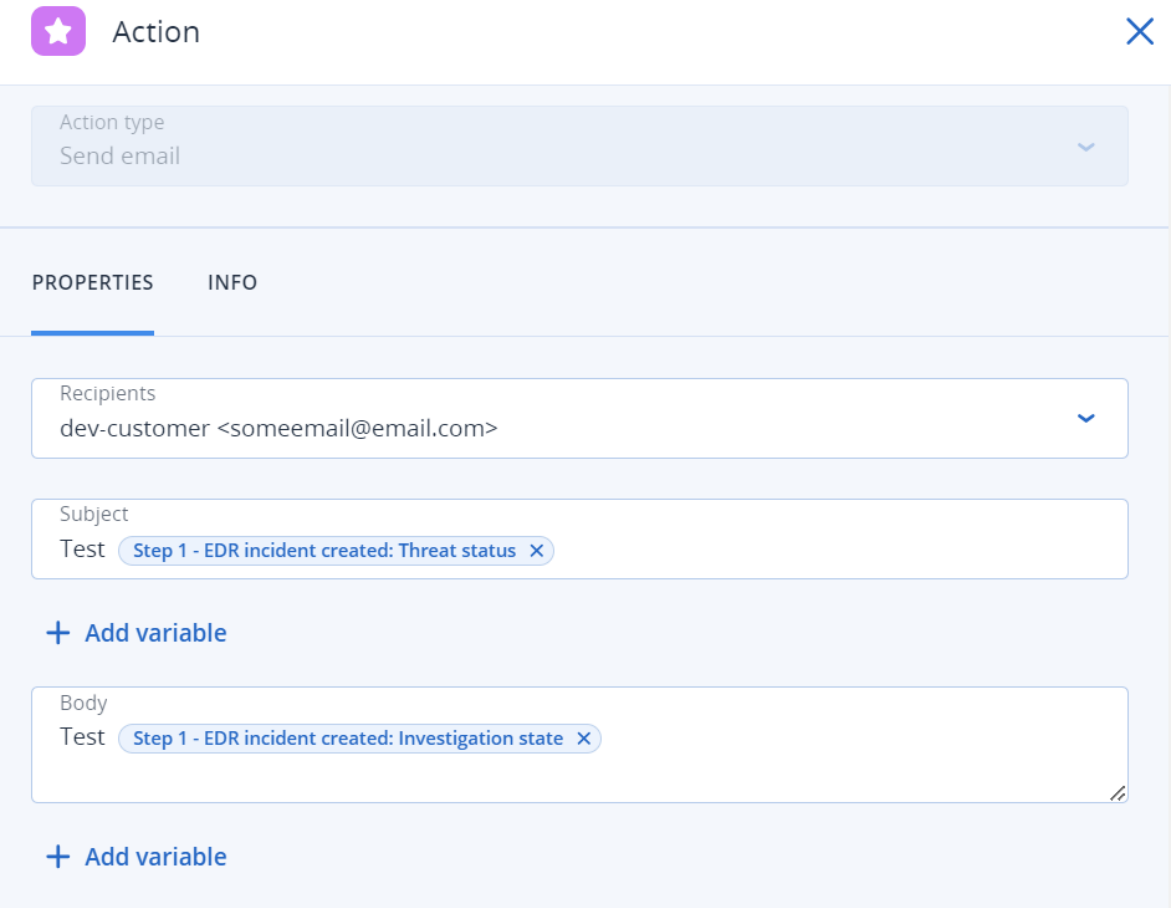
- **Todas**: se deben cumplir todas las condiciones de este bloque para continuar con el siguiente paso del flujo de trabajo.
- **Cualquiera**: al menos una de las condiciones de este bloque debe cumplirse para continuar con el siguiente paso del flujo de trabajo.

4. Para modificar una condición, haga clic en la condición y modifique los valores correspondientes. Cuando haya terminado, haga clic en **Actualizar**.

   Tenga en cuenta que también puede eliminar una condición al hacer clic en el icono de la papelera que se encuentra junto a ella.
5. Para modificar una acción, haga clic en la acción que desee modificar.
6. Realice los cambios pertinentes en el panel que se muestra.

© Acronis International GmbH, 2003-2025

Por ejemplo, haga clic en la acción **Enviar correo electrónico** y, a continuación, modifique los destinatarios seleccionados, el cuerpo y el asunto del correo electrónico que se envía como parte de este flujo de trabajo.



7. [Opcional] Modifique las acciones adicionales.
8. Haga clic en **Guardar**.
   Si el flujo de trabajo no estaba habilitado previamente y se encontraba en estado **Borrador**, haga clic en **Guardar y habilitar** para habilitarlo. De forma alternativa, haga clic en **Guardar** para dejar el flujo de trabajo **Deshabilitado**.
   Tenga en cuenta que puede habilitar y deshabilitar un flujo de trabajo desde la pantalla principal al hacer clic en el flujo de trabajo correspondiente y seleccionar **Habilitar** o **Deshabilitar**, según sea necesario.

Habilitar el modo de supervisión para Endpoint Detection and Response (EDR)

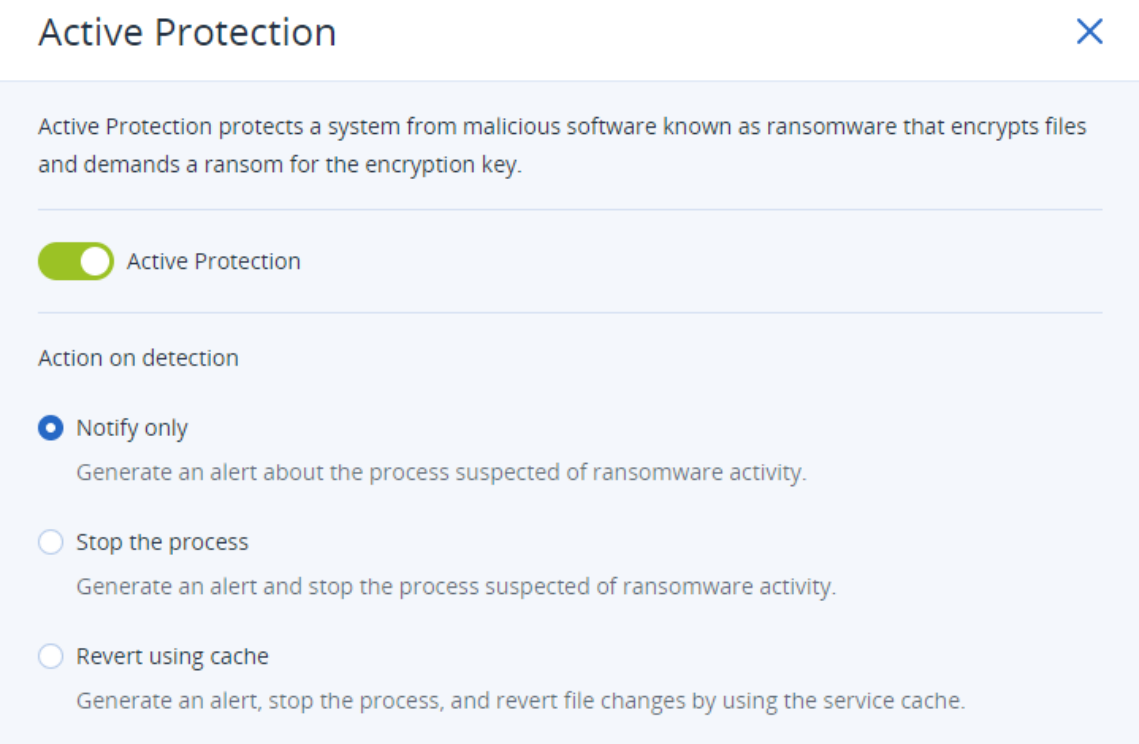
El modo de supervisión de Cyber Protection permite usar la EDR en un entorno de producción. A su vez, esto permite verificar si hay falsos positivos y hacer las exclusiones necesarias antes de desplegar completamente la EDR.

© Acronis International GmbH, 2003-2025

En modo de supervisión, nada se bloquea ni se detiene y se crean incidentes, pero no se inician respuestas.

Para habilitar el modo de supervisión para EDR

1. En el plan de protección correspondiente, asegúrese de que la EDR esté habilitada. Para más información, consulte "Habilitación de la funcionalidad Endpoint Detection and Response (EDR)" (p. 1254).
2. Amplíe el módulo **Protección antivirus y antimalware** y, luego, defina lo siguiente:
   - Haga clic en **Active Protection** y, en la sección **Acción sobre la detección**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Active Protection" (p. 1166).

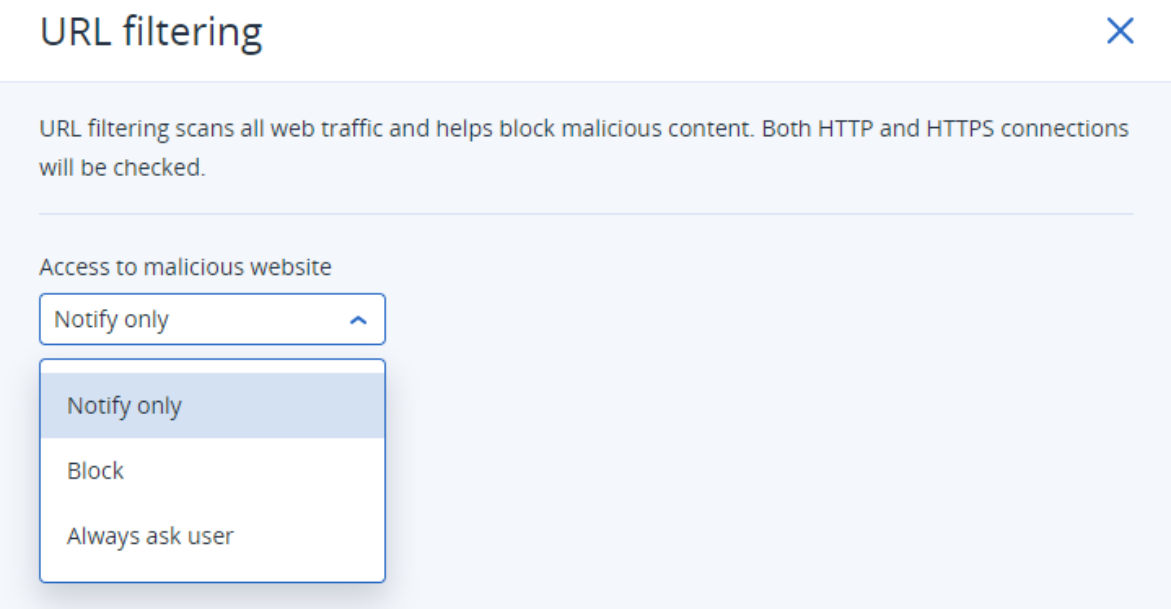


   - Haga clic en **Motor de comportamiento** y, en la sección **Acción sobre la detección**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Motor de comportamiento" (p. 1172).
   - Haga clic en **Prevención de vulnerabilidades** y, en la sección **Acción sobre la detección**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Prevención de vulnerabilidades" (p. 1173).
   - Haga clic en **Protección en tiempo real** y, en la sección **Acción sobre la detección**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Protección en tiempo real" (p. 1174).
   - Haga clic en **Planificar análisis** y, en la sección **Acción sobre la detección**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Planificar análisis" (p. 1175).

© Acronis International GmbH, 2003-2025

- Haga clic en **Aplicación potencial no deseada** y, en la sección **Acción sobre la detección**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Aplicación potencialmente no deseada" (p. 1183).

3. Amplíe el módulo **Filtrado de URL** y, en la lista desplegable **Acceso a sitio web malicioso**, seleccione **Solo notificar**. Luego, haga clic en **Listo**. Para obtener más información, consulte "Filtrado de URL" (p. 1192).



Cómo probar si Endpoint Detection and Response (EDR) funciona correctamente

Para garantizar que la EDR se implementa y funciona, puede ejecutar un número de comandos que desencadenan las detecciones de la EDR.

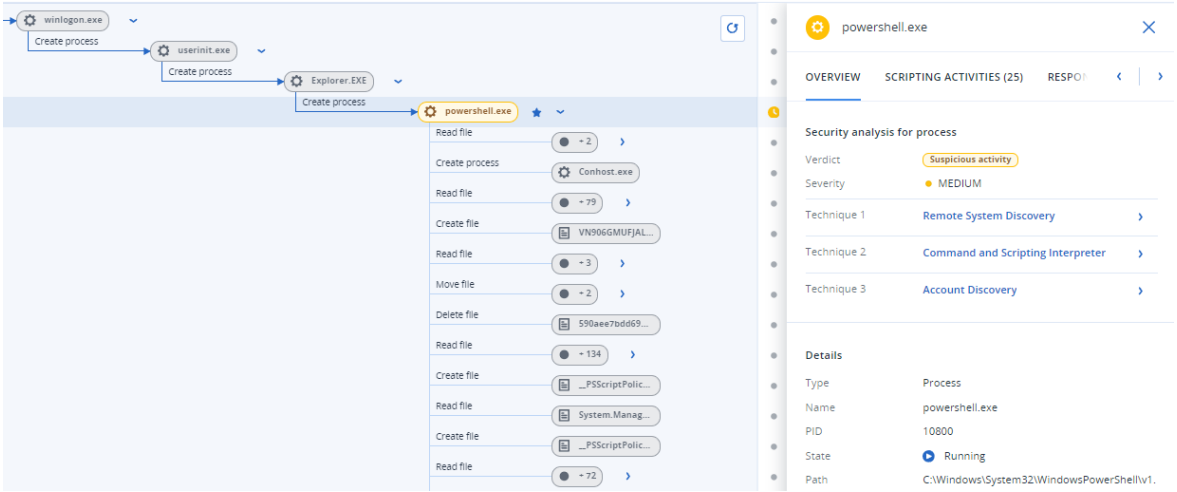
Nota
Cuando se implemente la EDR, debería ver incidentes inmediatamente si ocurre cualquier actividad sospechosa. Los pasos indicados a continuación le permiten comprobar si la EDR funciona si no se desencadenan incidentes nuevos durante varios días.

Pasos para probar si la EDR se implementa y funciona correctamente

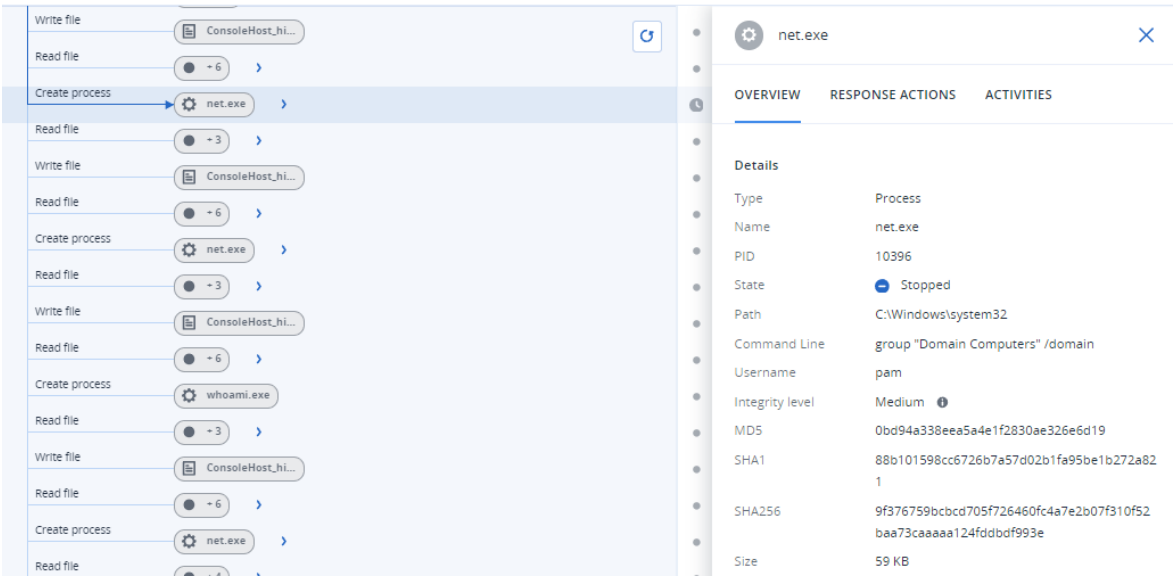
1. Inicie sesión en la cuenta de usuario de Active Directory vinculada al dominio correspondiente.
2. En Windows PowerShell, ejecute los siguientes dos comandos:
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. En la consola de Cyber Protect, vaya a **Protección > Incidentes** para ver el incidente generado.

© Acronis International GmbH, 2003-2025

También puede hacer clic en el incidente de tipo de gravedad **Medio** desencadenado para mostrarlo en la cadena de eliminación cibernética de EDR y confirmar los comandos de PowerShell que ejecutó en el paso anterior, como se muestra en el siguiente ejemplo.



4. En Windows PowerShell, ejecute los siguientes comandos:
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. En la cyber kill chain de la EDR, haga clic en los nodos ejecutables (por ejemplo, **net.exe** o **whoami.exe**) para mostrar los comandos de PowerShell exactos ejecutados en la línea de comandos. Estos comandos se muestran en la sección **Detalles** de la pestaña **Información general** del siguiente ejemplo.



© Acronis International GmbH, 2003-2025

6. Después de confirmar que se ha generado un incidente de la EDR, establezca manualmente el **Estado de la amenaza** para el incidente en **Mitigada** y el **Estado de la investigación** en **Cerrada**. Para obtener más información, consulte "Pasos para investigar incidentes en la cyber kill chain" (p. 1285). También puede escribir un comentario para el incidente para indicar que fue un incidente de la prueba.

Extended Detection and Response (XDR)

Nota
Esta funcionalidad forma parte del paquete de Advanced Security + XDR Protection, que a su vez se incluye en el servicio de ciberprotección. Tenga en cuenta que debe habilitar la funcionalidad Endpoint Detection and Response (EDR) en un plan de protección para que XDR funcione.

XDR utiliza EDR para la correlación de eventos y la identificación de ataques avanzados en los endpoints, y luego amplía esa funcionalidad al identificar amenazas avanzadas en los endpoints, el correo electrónico, la identidad, etc.

Al utilizar el gráfico XDR a través de múltiples integraciones XDR (incluidas Perception Point y Microsoft 365), también puede responder a los incidentes con acciones específicas disponibles para cada tipo de integración, como bloquear remitentes de correo electrónico o suspender usuarios.

XDR es compatible con estaciones de trabajo, servidores, máquinas virtuales y servidores de alojamiento web.

¿Por qué necesita Extended Detection and Response (XDR)?

Los MSP que ofrecen servicios de seguridad anteriormente tenían que elegir entre protección insuficiente o incompleta, o soluciones costosas y complejas. XDR supera estas limitaciones al ampliar y enriquecer la funcionalidad proporcionada por "Endpoint Detection and Response (EDR)" (p. 1250) e identificar amenazas avanzadas en endpoints, correo electrónico, identidad y más allá.

Con una *superficie de ataque en constante crecimiento* (múltiples clientes en ubicaciones remotas, una combinación de recursos informáticos in situ y en la nube, y nubes privadas y públicas), *brechas en la infraestructura de seguridad* (debido a la gran cantidad de herramientas de seguridad desplegadas para diferentes clientes, alertas que abruman a los técnicos y la falta de talento en seguridad) y *amenazas cibernéticas en constante evolución* (como herramientas basadas en IA para que los atacantes encuentren y exploten vulnerabilidades desde el día cero y generadores de ransomware), la necesidad de una solución para detener las amenazas cibernéticas modernas con pasos de reparación simplificados es evidente.

Estos son los motivos por los que necesita XDR:

- **Ampliación de la protección**: proteja los entornos de los clientes frente a amenazas sofisticadas en superficies de ataque vulnerables con una visibilidad extensa que abarca los endpoints, el correo electrónico, Microsoft Entra ID y las aplicaciones de Microsoft 365 (como SharePoint, OneDrive y Teams). Esa visibilidad mejorada significa detecciones más rápidas de lo que EDR

© Acronis International GmbH, 2003-2025

puede proporcionar.

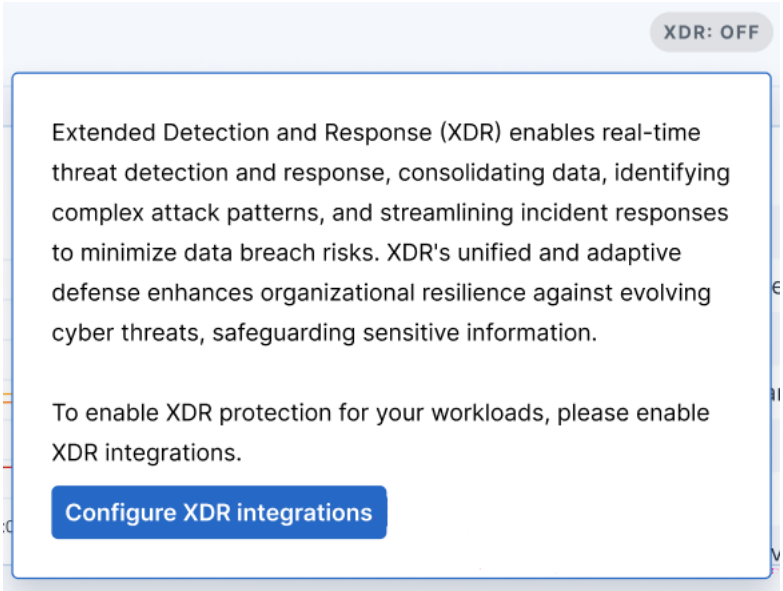
- **Integración nativa**: Integre fácilmente plataformas de ciberseguridad, protección de datos y gestión de endpoints. XDR está diseñado para proteger las superficies de ataque vulnerables para una continuidad de la actividad empresarial sin igual.
- **Muy eficiente con una remediación mejorada**: inicie, gestione, escale y ofrezca servicios de seguridad con facilidad. Además, XDR incluye un análisis de incidentes basado en la IA y una respuesta con un solo clic para una investigación y corrección sencillas, con acciones de corrección asistidas por la IA y automáticas que protegen contra amenazas cibernéticas avanzadas y de varias fases. La seguridad proactiva también permite a los técnicos identificar y solucionar problemas potenciales antes de que un atacante los explote.

Activación de Extended Detection and Response (XDR)

Importante
Para que XDR funcione, primero debe habilitar la opción Endpoint Detection and Response (EDR) en los planes de protección correspondientes. Esto garantiza que el interruptor de la opción **XDR: Activado/Desactivado** se muestre para los inquilinos del cliente. Si este interruptor de opción no se muestra, póngase en contacto con su administrador de partner.

Pasos para activar XDR

1. Asegúrese de que EDR esté habilitado en sus planes de protección. Para obtener más información, consulte "Habilitación de la funcionalidad Endpoint Detection and Response (EDR)" (p. 1254).
2. Vaya a **Protección** > **Incidentes**.
3. En la esquina superior derecha de la pantalla, haga clic en XDR: OFF.
4. Se le pedirá que configure las integraciones de XDR, que son necesarias para que XDR proteja sus recursos informáticos. Haga clic en **Configurar las integraciones de XDR**.



© Acronis International GmbH, 2003-2025

Si tiene integraciones XDR configuradas y desea añadir integraciones adicionales, haga clic en **Añadir integraciones de XDR**.

Se le redirigirá automáticamente al portal de administración, donde podrá seleccionar y configurar las integraciones de XDR pertinentes. Para obtener más información, consulte Integración de Advanced Security + XDR con plataformas de terceros.

Para obtener más información sobre la integración con Microsoft 365, consulte estos pasos de integración.

Para obtener más información sobre la integración con Perception Point, consulte estos pasos de integración.

Cuando se configura al menos una configuración de XDR, el interruptor de la opción de XDR se habilita 

, y puede comenzar a trabajar con XDR.

Trabajar con el gráfico XDR

El gráfico XDR añade otra perspectiva enriquecida para ver los incidentes de EDR (Endpoint Detection and Response) al correlacionar las detecciones con los eventos de las fuentes de datos de XDR, incluidos el correo electrónico y los metadatos de la gestión de identidades.

El tipo de nodos que se muestran en el gráfico depende de las integraciones XDR. Por ejemplo, cuando se integra con la gestión de correo electrónico e identidad, el gráfico mostrará nodos de correo electrónico, nodos de archivos adjuntos de correo electrónico y nodos de identidad de usuario. Cuando se integra con los servicios de Microsoft 365, el gráfico mostrará nodos de aplicaciones de colaboración, como Teams, OneDrive y SharePoint.

Para obtener más información sobre los distintos iconos de nodo que se muestran en el gráfico XDR, consulte "Iconos del gráfico XDR" (p. 1346).

Utilice el gráfico XDR para lo siguiente:

- Investigar nodos individuales
- Aplicar acciones de respuesta a un nodo
- Ver errores de integración

Para acceder al gráfico XDR, vaya a **Protección > Incidentes**, haga clic en el incidente correspondiente y, a continuación, haga clic en la pestaña **XDR**.

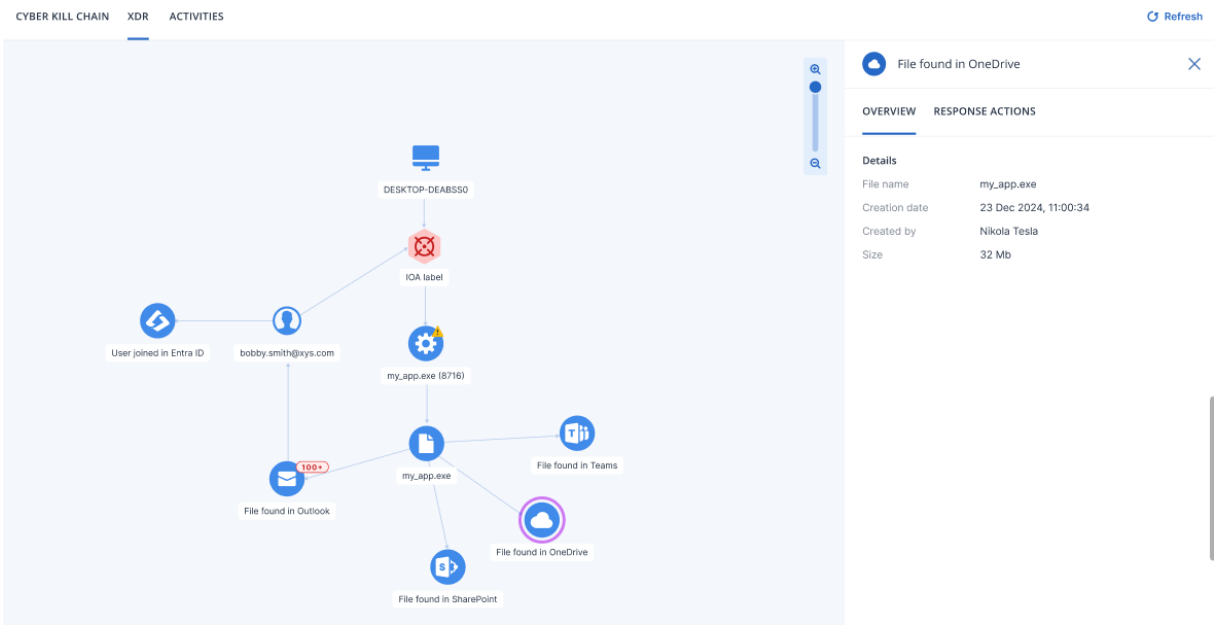
Para actualizar el contenido del gráfico XDR, haga clic en 

.

Nota

La pestaña **XDR** se muestra solo si XDR está habilitado. Para obtener más información, consulte "Activación de Extended Detection and Response (XDR)" (p. 1340).

© Acronis International GmbH, 2003-2025



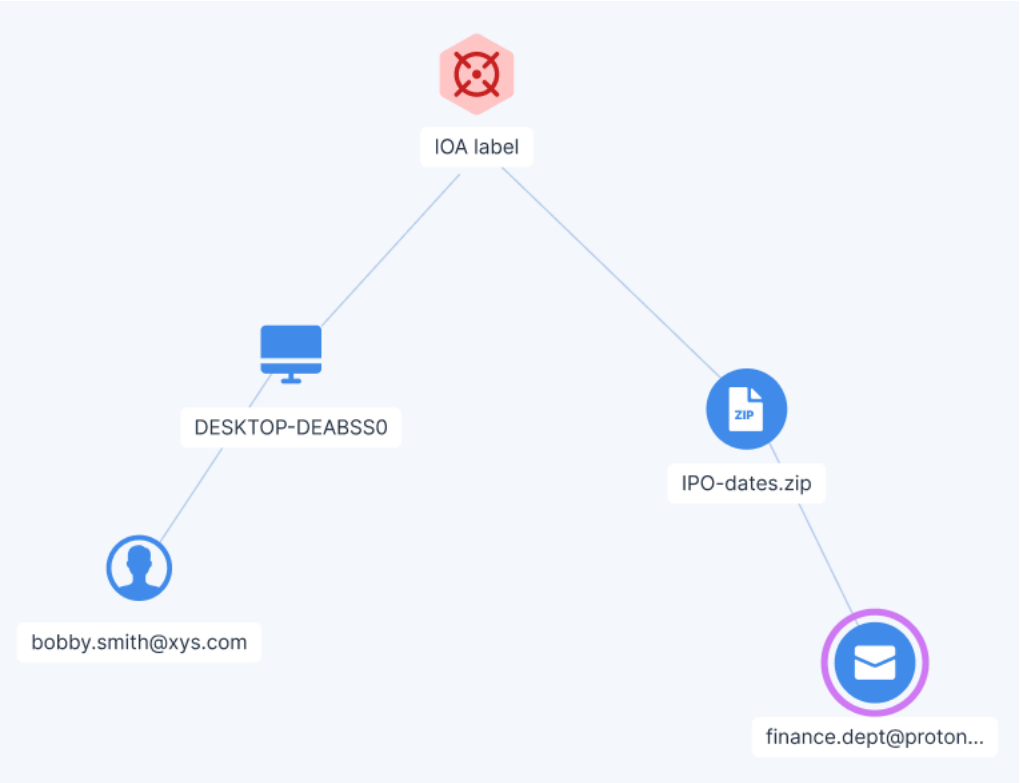
Cómo analizar el gráfico XDR

XDR (Extended Detection and Response) añade detalles adicionales a un incidente de EDR (Endpoint Detection and Response), como verificar si la amenaza provino de un archivo adjunto de correo electrónico, una aplicación de colaboración o un enlace en un correo electrónico, y qué usuario inició sesión y fue responsable de abrir el archivo adjunto malintencionado. Al analizar el gráfico de XDR, se le proporciona un contexto adicional de lo que sucedió en el incidente y si se requiere una acción más allá de la funcionalidad de EDR, como bloquear la cuenta del usuario y/o bloquear el remitente del correo electrónico.

Al observar los nodos que del gráfico XDR que se muestran a continuación, puede ver que se extrajo una amenaza malintencionada de un archivo ZIP adjunto a un correo electrónico descargado en **DESKTOP-DEABSS0**. La dirección de correo electrónico del remitente fue **finance.dept@proton.me** y el usuario que inició sesión y abrió el archivo ZIP fue **bobby.smith@xys.com**.

Al hacer clic en el icono del escritorio, puede ver en la pestaña **Información general** si la carga de trabajo es la carga de trabajo habitual del usuario que ha iniciado sesión. Si el usuario ha iniciado sesión con un sistema operativo o una dirección IP que nunca ha utilizado anteriormente, es probable que el incidente sea malintencionado. A continuación, puede aplicar las acciones de respuesta necesarias a los usuarios de los dispositivos comprometidos para asegurarse de que no tengan acceso a datos confidenciales y recursos de TI.

© Acronis International GmbH, 2003-2025



Hay elementos de gráficos XDR adicionales que le ayudan a comprender exactamente lo que sucedió.

Por ejemplo, la integración XDR con los servicios de Microsoft 365 incluye lo siguiente:

- Cuando un archivo malicioso se encuentra en una aplicación de Microsoft 365 (OneDrive, SharePoint, Teams o Outlook), se muestra una línea para conectar el nodo del archivo malicioso al nodo de la aplicación de colaboración correspondiente.

Del mismo modo, la integración de XDR con Perception Point incluye lo siguiente:

- Cuando un archivo malintencionado es un archivo adjunto directo de un correo electrónico, se muestra una línea para conectar el nodo del archivo malintencionado con el nodo del correo electrónico.
- Cuando el nodo malintencionado es un nodo de URL, se muestra una línea para conectar el nodo de URL malintencionado con el nodo de correo electrónico.
- Cuando se extrae un archivo malintencionado de un archivo comprimido adjunto (u otro tipo de archivo comprimido), se crea un nodo de archivo para el archivo comprimido y se muestra una línea para conectar el nodo de archivo malintencionado con el nodo del archivo adjunto.

Investigación de nodos individuales

Puede ver los detalles de cualquiera de los nodos del gráfico XDR. Esto le permite profundizar en nodos específicos del gráfico e investigar y aplicar acciones de respuesta a cada nodo según sea necesario.

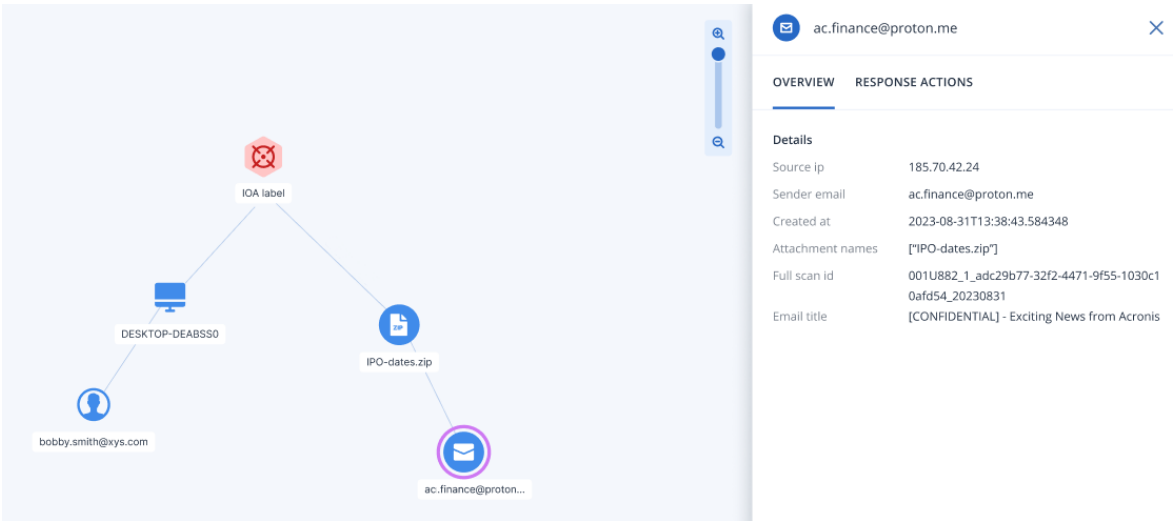
© Acronis International GmbH, 2003-2025

Los nodos que se muestran variarán según las integraciones de XDR implementadas. Los detalles del nodo se muestran en la pestaña **Información general** y las acciones de respuesta disponibles para ese nodo se muestran en la pestaña **Medidas de respuesta**.

Nota
No hay acciones de respuesta disponibles para los nodos de Indicadores de compromiso (IoC) e Indicadores de ataque (IoA).

Pasos para investigar nodos individuales

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.
2. En la lista de incidentes que se muestra, haga clic en en la columna situada en el extremo derecho del incidente que desee investigar.
3. Haga clic en la pestaña **XDR**.
4. Vaya al nodo correspondiente y haga clic en él para mostrar la barra lateral del nodo.
   Por ejemplo, si hace clic en el nodo del correo electrónico del ejemplo siguiente, se abrirá la barra lateral del nodo.



5. Investigue la información incluida en las pestañas de la barra lateral:
   - **Información general**: esta pestaña incluye detalles sobre el nodo seleccionado, según el tipo de nodo.
     - Nodos de Indicador de ataque (IoA): incluye la fecha/hora de detección, la gravedad de la detección, la descripción de la detección, la táctica y técnica de MITRE, y el nombre de la amenaza.
     - Nodos de Indicador de compromiso (IoC): cada tipo de nodo de IoC (proceso, archivo o URL) tiene su propio conjunto de campos, que también se utilizan en Endpoint Detection and Response (EDR). Para obtener más información, consulte "Investigar nodos individuales en la cyber kill chain" (p. 1293).
     - Nodos de integración: incluye detalles sobre el nodo seleccionado, dependiendo de la integración.

© Acronis International GmbH, 2003-2025

Por ejemplo, los nodos de Teams, OneDrive y SharePoint incluyen el nombre del archivo, su fecha de creación, el usuario que lo creó, el último usuario que lo modificó y su tamaño.

De forma similar, el nodo de correo electrónico incluye detalles sobre la dirección IP del remitente, el nombre y el cliente utilizado, así como el nombre, el formato y el tamaño de cada archivo adjunto.

- **Medidas de respuesta**: esta pestaña enumera las distintas acciones de respuesta disponibles, según la integración. Por ejemplo, el nodo de correo electrónico mostrará opciones para bloquear el correo electrónico del remitente como malintencionado y eliminar los archivos adjuntos. Para obtener más información, consulte "Aplicación de medidas de respuesta" (p. 1345).

Aplicación de medidas de respuesta

Puede aplicar varias acciones de respuesta a nodos de gráficos XDR individuales. Estas acciones de respuesta le permiten reparar cualquier nodo de forma rápida y sencilla.

Pasos para aplicar una acción de respuesta

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.
2. En la lista de incidentes que se muestra, haga clic en  en la columna situada en el extremo derecho del incidente que desee investigar.
3. Haga clic en la pestaña **XDR**.
4. Vaya al nodo correspondiente y haga clic en él para mostrar la barra lateral del nodo.

   Tenga en cuenta que si el nodo es de un tipo de nodo de identidad, correo electrónico o colaboración agrupado (indicado por un número de etiqueta en el nodo), las acciones de respuesta aplicadas a este nodo se aplicarán a todos los subnodos del nodo de grupo.
5. Haga clic en la pestaña **Medidas de respuesta**.
6. Haga clic en **Ejecutar** en el caso de la acción de respuesta necesaria.

   Por ejemplo, la integración de Perception Point admite la acción de respuesta del remitente de la lista de bloqueados.

   Para la integración de Microsoft 365, están disponibles las acciones de respuesta de terminar sesión de usuario, restablecimiento forzoso de la contraseña y suspensión de usuario.

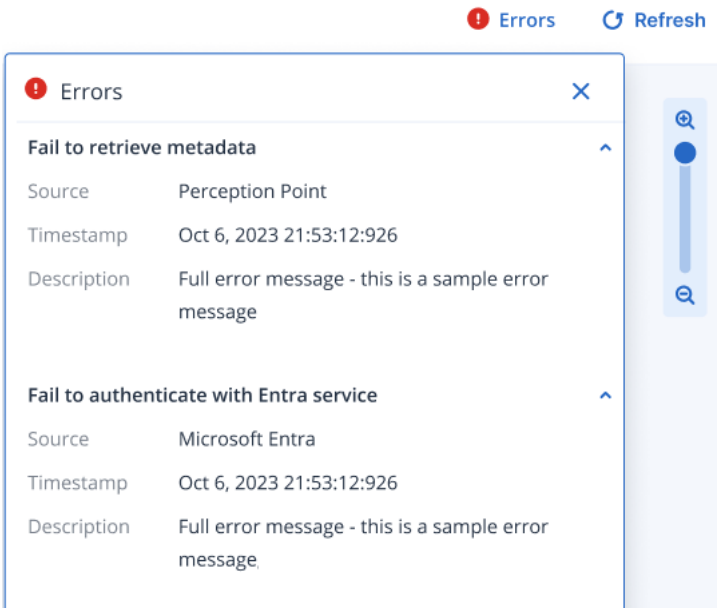
   Nota
   Al hacer clic en **Ejecutar**, las demás acciones de respuesta se deshabilitan temporalmente. Cuando la acción se completa, las demás acciones de respuesta se habilitan.
7. (Opcional) Haga clic en la pestaña **Actividades** para revisar todas las acciones de respuesta aplicadas al nodo. Tenga en cuenta que las acciones de respuesta ejecutadas para los incidentes de XDR se muestran junto con los incidentes de Endpoint Detection and Response (EDR). Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 1295).

© Acronis International GmbH, 2003-2025

Visualización de errores de integración de XDR

Si se produce un error durante la integración con soluciones XDR de terceros, se muestra el cuadro de diálogo Errores. Este cuadro de diálogo muestra los errores de integración, incluidos los fallos al conectar con la fuente de integración o si la integración se configuró incorrectamente.

El cuadro de diálogo Errores se muestra automáticamente (si hay errores) al acceder al gráfico XDR. Para acceder a este cuadro de diálogo en cualquier otro momento, haga clic en **Errores**, en la esquina superior derecha del gráfico XDR. Tenga en cuenta que el botón **Errores** no se muestra si no hay errores actuales en el gráfico XDR.



Iconos del gráfico XDR

La tabla que aparece a continuación enumera los distintos iconos actualmente disponibles en el gráfico XDR.

Tenga en cuenta que un nodo puede estar "agrupado" para incluir una cantidad de nodos individuales del mismo tipo. El icono que representa el nodo muestra un número que indica la cantidad de nodos dentro del nodo agrupado.

Por ejemplo, 

indica que hay más de 100 procesos en el incidente. Si el número de nodos agrupados es inferior a 100, se muestra el número real.

Icono	Descripción
	Indicador de compromiso (IoC) que indica un proceso genérico o inyectado. El icono lleva la etiqueta con el nombre del proceso, por ejemplo, **nombreproceso.exe**.

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Indicador de compromiso (IoC) que indica un archivo genérico, de documento, ejecutable o de script. El icono está etiquetado con el nombre del archivo, por ejemplo, **nombrearchivo.dll**.
	Indicador de compromiso (IoC) que indica una URL. El icono está etiquetado con la URL, por ejemplo, **abc.com**.
	Indicador de ataque (IoA). El icono lleva la etiqueta con el nombre de IoA, por ejemplo, **Minikatz**.
	Carga de trabajo El icono está etiquetado con el nombre del recurso informático, por ejemplo, **DESKTOP-D123**.
	Identidad (usuario) El icono está etiquetado con la ID de la cuenta de usuario, por ejemplo **david.smith@b.com**. Este nodo incluye información adquirida localmente por el agente, que no requiere una conexión a la API de Microsoft.
	Icono de correo electrónico que indica un correo electrónico de Outlook, un archivo adjunto o una URL genéricos. El icono está etiquetado según la integración correspondiente. Al realizar la integración con Perception Point, la etiqueta muestra la dirección de correo electrónico del remitente, por ejemplo **david.smith@b.com**. Al realizar la integración con Microsoft 365, se muestra **Archivo encontrado en Outlook**.
	OneDrive El icono está etiquetado con **Archivo encontrado en OneDrive**.
	SharePoint El icono está etiquetado con **Archivo encontrado en SharePoint**.
	Teams El icono está etiquetado con **Archivo encontrado en Teams**.
	Microsoft Entra ID El icono está etiquetado con la ID de la cuenta de usuario, por ejemplo **david.smith@b.com**. Este nodo incluye el UPN proporcionado desde Entra ID. Haga clic en el nodo para mostrar el UPN en el campo **Nombre de usuario de AD**.

© Acronis International GmbH, 2003-2025

Gestión y supervisión del entorno de Microsoft 365

Importante
Esta funcionalidad está incluida en las funciones de **Protección estándar** bajo la licencia basada en servicios y bajo la licencia de Seguridad y RMM o Ultimate Protection bajo la licencia basada en soluciones.

En licencias basadas en servicios, la **Protección estándar** incluye la auditoría de la posición de seguridad de Microsoft 365, con líneas base de las mejores prácticas y la incorporación de usuarios. El servicio **RMM** adicional proporciona un nivel avanzado de supervisión y gestión de Microsoft 365, incluida la auditoría continua de la posición de seguridad de Microsoft 365 con líneas base de las mejores prácticas, la corrección de desviaciones y riesgos de usuario, y la incorporacion o baja de usuarios.

Con licencias basadas en soluciones, la funcionalidad completa está incluida en la licencia de Seguridad y RMM y la de Ultimate Protection.

Se aplica un cargo por cada usuario al que se le asigne una licencia de buzón de correo de Exchange Online.

El servicio de supervisión y gestión de la seguridad de Microsoft 365 en Cyber Protection le permite:

- Incorporar de forma sencilla inquilinos de clientes de Microsoft 365 a Cyber Protect Cloud.
- Proporcionar una auditoría continua de la posición de seguridad de los clientes de Microsoft 365.
- Supervisar las infracciones y los riesgos con las plantillas de línea base de las mejores prácticas de Microsoft 365.
- Corregir las desviaciones de línea base (en un solo clic) y las configuraciones erróneas de los controles de seguridad.
- Supervisar y gestionar los riesgos de usuario de Microsoft 365.
- Incorporar y dar de baja a usuarios de Microsoft 365.

Configuración de conexiones de Microsoft 365

Nota
Esta función solo está disponible para los usuarios administradores de partner.

Cuando se habilita la supervisión y gestión de seguridad de Microsoft 365 en Cyber Protect, puede conectarse a los clientes de Microsoft 365 asociados con su cuenta de Microsoft (o la de su cliente).

A continuación, puede asignar los inquilinos de Microsoft 365 a los clientes correspondientes en Cyber Protect e indicar el modo de producto (**Gratuito** o **Avanzado**) para cada cliente.

© Acronis International GmbH, 2003-2025

Conexión a una cuenta de Microsoft

Como administrador del partner, puede conectarse a su cuenta de Microsoft CSP o a su cuenta normal de Microsoft.

Cuando inicia sesión en su cuenta de Microsoft CSP, el sistema recupera automáticamente todos los inquilinos de clientes asociados con la cuenta CSP.

Cuando inicia sesión en una cuenta normal de Microsoft, puede conectarse a las cuentas de Microsoft de sus clientes una por una, siempre que disponga de las credenciales correspondientes.

Importante
Cuando se realiza la incorporación de inquilinos con un gran número de usuarios (por ejemplo, más de 1000), el sistema puede tardar un tiempo en recuperar todos los detalles relevantes. Esto se debe a que cada usuario debe ser verificado y algunas API de Microsoft solo se pueden activar una vez cada dos segundos. Este problema es relevante tanto para las cuentas de CSP como para las cuentas de Microsoft normales.

Pasos para conectarse a una cuenta de Microsoft

Cuenta de Microsoft CSP

1. En la consola de Cyber Protect, vaya a **Gestión de M365** > **Configuración**.
2. Haga clic en **Conectar cuenta de Microsoft**.
   Se le redirigirá a la página de inicio de sesión de Microsoft.
3. Inicie sesión en la cuenta de Microsoft con sus credenciales de CSP y acepte los permisos solicitados por Acronis. Al hacer clic en **Aceptar**, se le redirigirá a la consola de Cyber Protect.

   Nota
   Los permisos solicitados al iniciar sesión en una cuenta de Microsoft son para la aplicación empresarial de **Octiga Multi-Tenant Security** registrada en Entra ID. Esta aplicación está conectada con el inquilino de Microsoft 365 de los proveedores de servicios y les permite gestionar las operaciones
   de seguridad de sus clientes.

4. En la pestaña **Asignación de clientes** que se muestra, asigne los clientes de Microsoft 365 con los clientes correspondientes en Cyber Protect Cloud. Para obtener más información, consulte "Asignación de clientes" (p. 1350).
   El sistema enumera automáticamente todos los inquilinos de Microsoft 365 asociados con la cuenta de Microsoft en la pestaña **Asignación de clientes**, cada uno con el estado inicial de **Incorporación del inquilino**.

Cuenta normal de Microsoft

1. En la consola de Cyber Protect, vaya a **Gestión de M365 > Configuración**.
2. Haga clic en **Conectar cuenta de Microsoft**.

© Acronis International GmbH, 2003-2025

Se le redirigirá a la página de inicio de sesión de Microsoft.

3. Inicie sesión en la cuenta de Microsoft y acepte los permisos solicitados por Acronis.
   Al hacer clic en **Aceptar**, se le redirige a la consola de Cyber Protect.

   Nota
   Los permisos solicitados son para la aplicación empresarial **Octiga Multi-Tenant Security** registrada en la cuenta de Entra ID del inquilino del partner.

4. Haga clic en **Añadir cuenta de Microsoft del cliente**.
   Se le solicitará que inicie sesión con las credenciales de la cuenta de cliente correspondiente. Acepte los permisos solicitados por Acronis. Al hacer clic en **Aceptar**, se le redirigirá nuevamente a la consola de Cyber Protect.

   Nota
   Los permisos solicitados son para la aplicación empresarial de **Octiga Cloud Security** registrada en la cuenta de Entra ID del inquilino del cliente.

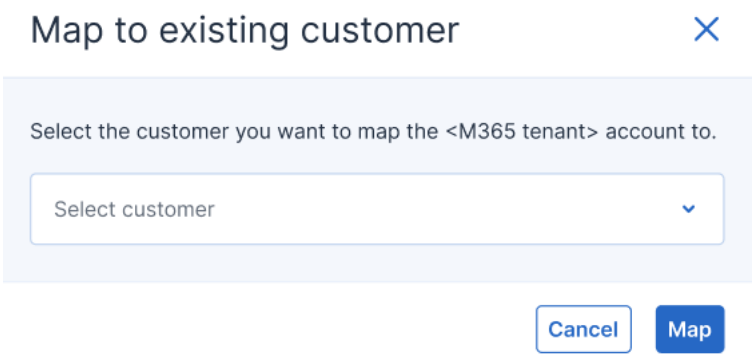
5. En la pestaña **Asignación de clientes** que se muestra, asigne los clientes de Microsoft 365 con los clientes correspondientes en Cyber Protect Cloud. Para obtener más información, consulte "Asignación de clientes" (p. 1350).
6. [Opcional] Para repetir los pasos indicados anteriormente para cuentas de Microsoft de clientes adicionales, haga clic en **Agregar cuenta de Microsoft** en la pestaña **Asignación de clientes**.

Asignación de clientes

Después de que se complete la incorporación de inquilinos de Microsoft 365 en Cyber Protect Cloud, puede asignar los inquilinos de Microsoft 365 asociados con esa cuenta a los clientes en Cyber Protect Cloud.

Pasos para asignar inquilinos de Microsoft 365 a clientes

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Configuración**.
2. En la pestaña **Asignación de clientes**, seleccione el inquilino o inquilinos de Microsoft 365 correspondientes y, a continuación, haga clic en **Asignar a cliente existente**.
3. Seleccione el cliente correspondiente en el menú desplegable y haga clic en **Asignar**.



© Acronis International GmbH, 2003-2025

Cuando el cliente se haya asignado correctamente:

- Se muestra 

en la columna **Estado de asignación** en la pestaña **Asignación de clientes**.
- El modo de producto **avanzado** está habilitado para el cliente asignado. Para modificar el modo de producto, consulte "Definición del modo del producto" (p. 1351).
- El sistema aplica las líneas base de inquilinos predefinidas al inquilino del cliente. Para obtener más información, consulte "Supervisión de líneas base" (p. 1355).
- El seguimiento de la posición de seguridad comienza y se ejecuta para el inquilino del cliente. Para obtener más información, consulte "Revisión de la posición de seguridad" (p. 1352).

Nota
La supervisión de la posición de seguridad se ejecuta de forma continua solo en el modo Avanzado. En el modo gratuito, se ejecuta "bajo demanda" al iniciar sesión en la consola de Cyber Protect.

Pasos para eliminar la asignación entre inquilinos y clientes de Microsoft 365

1. En la pestaña **Asignación de clientes**, seleccione el o los inquilinos de Microsoft 365 correspondientes y, a continuación, haga clic en **Eliminar asignación**.
2. En el diálogo de confirmación, haga clic en **Eliminar**.
   Si está conectado a una cuenta de Microsoft CSP, se elimina la asignación entre el cliente seleccionado y el cliente de Cyber Protect Cloud. El cliente seguirá apareciendo en la pestaña **Asignación de clientes**, con el estado **No asignado**.
   Si está conectado a una cuenta de normal de Microsoft, se elimina la asignación entre el inquilino seleccionado y el cliente Cyber Protect Cloud, y también se elimina la aplicación de Acronis del directorio de **registros de aplicaciones** en la cuenta de Microsoft Entra ID del cliente. El inquilino se elimina de la pestaña **Asignación de clientes**.

Nota
Cuando se elimina la asignación, el servicio de supervisión y gestión de seguridad de Microsoft 365 se deshabilita automáticamente para el cliente o clientes seleccionados.

Definición del modo del producto

Puede definir el modo del producto (Gratuito o Avanzado) que se aplicará a cada cliente.

Nota
De manera predeterminada, los clientes se incorporan al servicio de supervisión y gestión de la seguridad de Microsoft 365 en el modo Avanzado.

Pasos para definir el modo del producto

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Configuración**.
2. Haga clic en la pestaña **Modo de producto**.

© Acronis International GmbH, 2003-2025

3. Seleccione los clientes a los que desee cambiar el modo de producto y, a continuación, haga clic en **Cambiar modo de producto**.
4. En el cuadro de diálogo de confirmación, seleccione el modo de producto correspondiente (**Gratuito** o **Avanzado**) y haga clic en **Modificar**.

   El modo **gratuito** incluye la supervisión de la seguridad y la gestión de licencias de Microsoft 365, y la incorporación de usuarios. El modo **gratuito** también requiere que la cuota de servicio **Protección estándar** > **Licencias de Microsoft 365** se aplique a todos las licencias de Microsoft 365 del cliente.

   El modo **Avanzado** incluye la supervisión de seguridad de Microsoft 365 y la gestión de licencias, la remediación de riesgos de seguridad y configuraciones incorrectas en su entorno de Microsoft y la incorporación o baja de usuarios. En el modo de licencia basado en servicios, el modo **Avanzado** requiere que la cuota de servicio **RMM** > **Licencias de Microsoft 365** se aplique a todos las licencias de Microsoft 365 del cliente. En licencias basadas en soluciones, la funcionalidad completa se habilita con la licencia **Seguridad y RMM** o **Protección definitiva**.

   Al hacer clic en **Modificar**, acepta que las cuotas de servicio requeridas se aplicarán automáticamente.

Cómo deshabilitar el servicio de gestión de Microsoft 365

Puede deshabilitar el servicio de gestión de Microsoft 365 para clientes que se han incorporado anteriormente (consulte "Conexión a una cuenta de Microsoft" (p. 1349)) en Cyber Protect Cloud.

Para deshabilitar el servicio de gestión de Microsoft 365

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Configuración**.
2. Haga clic en la pestaña **Configuración** y, a continuación, en **Deshabilitar servicio**.
3. En el cuadro de diálogo de confirmación, haga clic en **Deshabilitar**.

   Si se deshabilita el servicio, se eliminará:
   - La aplicación de Acronis conectada desde el directorio de **registros de aplicaciones** en el Microsoft Entra ID de su inquilino.
   - Todos los datos relacionados con los clientes almacenados en Cyber Protect Cloud, incluida la asignación de clientes a los inquilinos de Microsoft 365.

Revisión de la posición de seguridad

Los administradores de partner pueden revisar la posición de seguridad de varios inquilinos de Microsoft 365 en un panel de control.

Para acceder a la funcionalidad de la posición de seguridad, vaya a **Gestión de Microsoft 365** > **Posición de seguridad**.

La pantalla **Posición de seguridad** proporciona una descripción general de la posición de seguridad y muestra los siguientes datos para cada inquilino de Microsoft 365:

© Acronis International GmbH, 2003-2025

- Nombre del inquilino
- Líneas base de inquilinos (se muestra el número de desviaciones de línea base de inquilinos, si es relevante)
- Usuarios (número de usuarios)
- Buzones de correo (el número de buzones de correo)

En la parte superior de la pantalla, puede ver los iconos que indican:

- El número total de inquilinos de Microsoft 365 con desviaciones en las líneas base.
- El número total de desviaciones en las líneas base de inquilinos entre los inquilinos afectados.

Nota
Puede ver datos adicionales de la posición de seguridad al hacer clic en la fila del inquilino para mostrar el panel de control de riesgos del inquilino seleccionado. Para obtener más información, consulte "Revisión del panel de control de riesgos" (p. 1353).

Revisión del panel de control de riesgos

El panel de control de riesgos resalta cualquier peligro (o desviación) a las líneas base, categorías de líneas base y cuentas de usuario de un inquilino de Microsoft 365.

Puede acceder al panel de control de riesgos de un inquilino específico al hacer clic en la fila del inquilino correspondiente en la pantalla Posición de seguridad (consulte "Revisión de la posición de seguridad" (p. 1352)).

De forma alternativa, para ver el panel de control de riesgos para el inquilino o inquilinos de Microsoft 365 asignados a un cliente específico, seleccione el cliente en el menú desplegable **Todos los clientes** (ubicado sobre el menú de navegación).

© Acronis International GmbH, 2003-2025

Baselines

Tenant baselines	3 passed	11 deviated

Baseline categories

Audit	1 passed	0 deviated
Authentication & Authorisation	0 passed	6 deviated
Email Security	0 passed	4 deviated
Remote Access	2 passed	0 deviated
Sharing	0 passed	1 deviated

User account risks

MFA	6 affected user accounts
Admin mailboxes	No affected user accounts
Anonymous admins	1 affected user account
Shared mailboxes	No affected user accounts
Dormant accounts	No affected user accounts
Dormant admins	No affected user accounts
Guests	18 affected user accounts

© Acronis International GmbH, 2003-2025

El panel de control de Riesgos incluye la siguiente información:

- **Líneas base**
  - Líneas base de inquilinos (con el número de líneas base aprobadas y desviadas)
- **Categorías de líneas base** (cada una de las siguientes categorías incluye el número de líneas base aprobadas y desviadas)
  - Seguridad del correo electrónico
  - Autenticación y autorización
  - Compartir
  - Control
  - Acceso remoto
- **Riesgos de las cuentas de usuario**
  - Autenticación multifactor (con el número de cuentas de usuario afectadas en las que la autenticación multifactor está deshabilitada o sin registrar)
  - Buzones de correo de administrador (con el número de cuentas de usuario que son cuentas de administrador globales con un buzón de correo)
  - Administradores anónimos (con el número de cuentas de usuario que podrían ser cuentas de administrador compartidas)
  - Buzones de correo compartidos (con el número de cuentas de usuario que tienen buzones de correo compartidos)
  - Cuentas inactivas (con el número de cuentas de usuario que no han iniciado sesión durante tres meses)
  - Administradores inactivos (con el número de cuentas de usuario que son cuentas de administrador pero que no han iniciado sesión durante seis meses)
  - Invitados (con el número de cuentas de usuario que son cuentas de invitado)

Supervisión de líneas base

La gestión de Microsoft 365 le permite supervisar el estado de todas las líneas base de inquilinos aplicadas.

Para acceder a la funcionalidad de líneas base, vaya a **Gestión de Microsoft 365** > **Líneas base**.

Supervisión de líneas base de inquilinos

Puede supervisar las líneas base de todos los inquilinos de Microsoft 365 que se hayan incorporado.

Pasos para supervisar las líneas base de inquilinos

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Líneas base**.
2. [Opcional] Seleccione un inquilino en el menú desplegable **Inquilino**. También puede filtrar la lista según el nombre de la categoría.

© Acronis International GmbH, 2003-2025

3. En la lista de líneas base, puede:
   - Examinar el estado (**Aprobada** o **Desviada**) de todas las líneas base aplicadas al inquilino seleccionado.
   - Verificar si la opción de autocorrección está habilitada.
   - Vea más detalles acerca de una línea base. Haga clic en la fila de la línea base correspondiente para:
     - Vea la descripción de la línea base. Para obtener más información sobre cada una de las líneas base disponibles, consulte "Líneas base de inquilinos" (p. 1356).
     - Ver los valores actuales y necesarios de la configuración de línea base.
     - Defina la corrección automática de la línea base. Haga clic en **Habilitar corrección automática** o **Deshabilitar corrección automática**, según sea necesario.
     - Corregir la desviación de línea base. Tenga en cuenta que esta opción requiere el modo de producto avanzado. Para obtener más información, consulte "Corrección de línea base de inquilinos de forma manual" (p. 1359).

Líneas base de inquilinos

La siguiente tabla enumera las líneas base de inquilinos de Microsoft 365 actualmente admitidas.

Categoría	Línea base	Descripción
Control	Registro de auditoría de buzones de correo	Habilitar los registros de auditoría de buzones de correo para toda la organización. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: aplicación de restricciones impuestas para dispositivos sin gestionar	Bloquear o limitar el acceso al contenido de SharePoint, OneDrive y Exchange desde dispositivos sin gestionar. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: bloquear la autenticación heredada	Bloquear el acceso a través de métodos de autenticación heredados inseguros. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: imponer	Imponer la autenticación multifactor. Para obtener más información, consulte la documentación de Microsoft.

© Acronis International GmbH, 2003-2025

Categoría	Línea base	Descripción
	autenticación multifactor	
Autenticación y autorización	Política de acceso condicional: sin sesiones de navegador persistentes	Evitar sesiones persistentes en el navegador. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: requerir aplicaciones de cliente aprobadas	Exigir una aplicación de cliente aprobada o una política de protección de aplicaciones al usar dispositivos móviles. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: requerir un dispositivo que cumpla los requisitos o que esté unido a Azure AD híbrido	Exigir a los usuarios administradores que realicen acciones desde un dispositivo que cumpla los requisitos o que esté unido a Azure AD híbrido. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: asegurar el registro de información de seguridad	Garantizar que todos los usuarios se registren de forma segura para la autenticación multifactor (MFA) y el restablecimiento de contraseña de autoservicio (SSPR) a través de dispositivos compatibles o condiciones específicas durante el registro. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de acceso condicional: autenticación multifactor basada en riesgos de inicio de sesión	Proteger a los usuarios de iniciar sesión mediante la autenticación multifactor en sesiones de riesgo. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Caja de seguridad del	Exigir a los ingenieros de soporte de Microsoft que obtengan la aprobación del cliente antes de acceder a sus datos durante los

© Acronis International GmbH, 2003-2025

Categoría	Línea base	Descripción
	cliente	casos de soporte. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Política de contraseñas	Especifica la duración de la validez de una contraseña antes de que deba cambiarse. También especifica el número de días antes de que un usuario reciba una notificación de que su contraseña va a caducar. Para obtener más información, consulte la documentación de Microsoft.
Autenticación y autorización	Requerir autenticación moderna en SharePoint	Requerir el uso de solo protocolos de autenticación modernos para el acceso global a SharePoint deshabilitando los protocolos de autenticación heredados. Para obtener más información, consulte la documentación de Microsoft.
Seguridad del correo electrónico	Reenvío automático: bloquear	Regla de transporte para bloquear el reenvío automático. Para obtener más información, consulte la documentación de Microsoft.
Seguridad del correo electrónico	Reenvío automático de correo	Deshabilitar el reenvío automático a dominios externos de forma predeterminada para toda la organización (los atacantes o actores maliciosos pueden reenviar automáticamente todo el correo a otro buzón y violar el cumplimiento si el reenvío automático es a un dominio externo). Para obtener más información, consulte la documentación de Microsoft.
Seguridad del correo electrónico	Política de filtro de tipos de archivos de malware	Bloquear los tipos de archivos maliciosos conocidos y personalizados para que no se adjunten a los correos electrónicos con el filtro de tipos de archivos adjuntos comunes. Esto ayuda a evitar que los archivos infectados con malware infecten un host. Para obtener más información, consulte la documentación de Microsoft.
Seguridad del correo electrónico	Política estándar de protección contra el phishing	Política antiphishing predeterminada para los buzones de Exchange, incluida la inteligencia antispoofing. Para obtener más información, consulte la documentación de Microsoft.
Intune	Octiga Windows 10 o posterior: política de cumplimiento	Política de cumplimiento para dispositivos Windows 10 (o posterior) gestionados por Octiga. Para obtener más información, consulte la documentación de Microsoft.
Acceso remoto	Autenticación moderna	Habilitar la autenticación moderna para toda la organización. Para obtener más información, consulte la documentación de Microsoft.
Acceso remoto	Acceso SMTP	Deshabilitar el acceso SMTP para toda la organización. SMTP se considera un protocolo de correo electrónico heredado poco seguro. Para obtener más información, consulte la documentación de Microsoft.

© Acronis International GmbH, 2003-2025

Categoría	Línea base	Descripción
Compartir	Caducidad de enlaces anónimos	Garantizar que los enlaces anónimos caduquen después de un cierto número de días. Para obtener más información, consulte la documentación de Microsoft.
Compartir	Volver a compartir para usuarios externos (invitados)	Evitar que los usuarios invitados que tienen acceso compartido a un elemento (donde el elemento se compartió mediante uso compartido de invitados y no a través de un vínculo anónimo) vuelvan a compartir el elemento con otros. El ajuste "Evitar que los usuarios externos vuelvan a compartir" garantiza un acceso limitado a los elementos compartidos. Para obtener más información, consulte la documentación de Microsoft.
Compartir	SharePoint bloquea la descarga de archivos infectados	Bloquear la descarga de archivos de SharePoint infectados. Para obtener más información, consulte la documentación de Microsoft.

Corrección de línea base de inquilinos de forma manual

Puede corregir las desviaciones en las líneas base del inquilino al hacer cumplir la configuración de línea base requerida en el inquilino.

Importante
La opción corrección automática debe estar habilitada para corregir automáticamente las desviaciones de línea base de inquilinos. Sin embargo, no es necesario para la corrección manual. Para obtener más información, consulte "Habilitación o deshabilitación de la corrección automática de las desviaciones de línea base" (p. 1360).

Pasos para corregir las desviaciones de línea base de inquilinos

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Líneas base**.
2. Seleccione la fila de inquilino correspondiente.
   Se muestra el panel de detalles de línea base.
3. Haga clic en **Solucionar**.
   Si está trabajando en el modo de producto gratuito, se le pedirá que cambie al modo de producto avanzado.

© Acronis International GmbH, 2003-2025

Nota

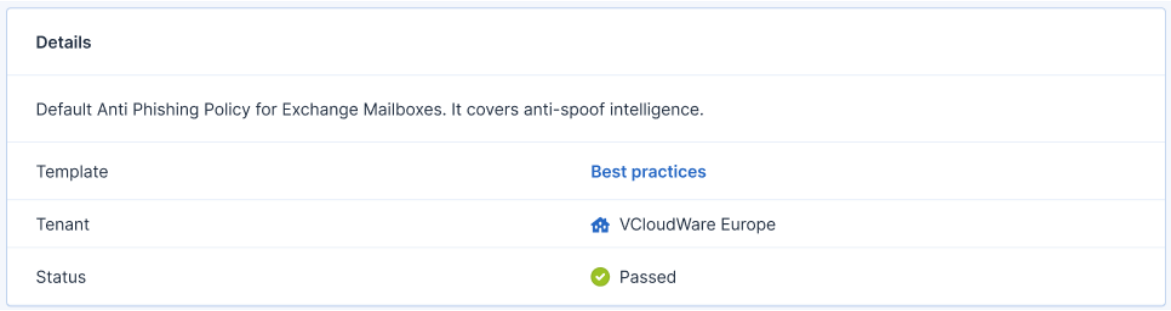
En licencias basadas en servicios, el modo gratuito requiere que la cuota de servicio **Protección estándar** > **Licencias de Microsoft 365** se aplique a todas las licencias de Microsoft 365 del cliente. El modo avanzado requiere que la cuota de servicio **RMM** > **Licencias de Microsoft 365** se aplique a todas las licencias de Microsoft 365 del cliente.

En licencias basadas en soluciones, la funcionalidad completa se activa con la licencia de **Seguridad y RMM** o **Protección definitiva**.

4. En el diálogo **Habilitar modo avanzado**, haga clic en **Habilitar**.

   Comienza el proceso de corrección.

   Cuando la corrección finaliza, el estado de línea base se actualiza a **Aprobada**, como se muestra a continuación.



Habilitación o deshabilitación de la corrección automática de las desviaciones de línea base

Puede configurar la corrección automática de desviaciones de línea base para determinados inquilinos de Microsoft 365.

Nota

La corrección automática está disponible solo en el modo avanzado. También es visible en el modo gratuito, pero cuando habilita la corrección automática, se le solicita que cambie al modo avanzado.

Pasos para habilitar o deshabilitar la corrección automática de las desviaciones de línea base

1. En la consola de Cyber Protect, vaya a **Gestión de M365** > **Líneas base**.
2. En el menú desplegable **Inquilino**, seleccione el inquilino correspondiente.

   También pued seleccionar el cliente correspondiente del menú desplegable **Todos los clientes** (ubicado sobre el menú de navegación).
3. Habilite o deshabilite las opciones de corrección automática según sea necesario:
   - Haga clic en **Habilitar corrección automática** para aplicar la corrección automática de las desviaciones a todas las líneas base.
   - Haga clic en **Deshabilitar corrección automática** para deshabilitar la corrección automática de las desviaciones para todas las líneas base.

© Acronis International GmbH, 2003-2025

4. [Opcional] Haga clic en una fila de línea base para modificar su configuración de corrección automática.

   Por ejemplo, puede habilitar la corrección automática para todas las líneas base, pero deshabilitarla para una o más líneas base específicas.

   Nota
   El sistema comprueba el estado de la(s) línea(s) base tres veces al día (cada ocho horas) y corrige automáticamente cualquier desviación (si la corrección automática está habilitada).

Gestión de usuarios de Microsoft 365

Como administrador de partner, puede navegar y gestionar la lista de usuarios del inquilino de Microsoft 365.

Para ver la lista actual de usuarios incorporados en la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Usuarios**. Puede filtrar la lista según el inquilino, el riesgo de usuario, el tipo de usuario, el rol del usuario y la licencia del producto.

Nota
Después de que se haya completado la incorporación del inquilino de cliente, la lista de usuarios del inquilino de Microsoft 365 tardará unos minutos en importarse desde Microsoft 365.

En la pantalla usuarios, puede realizar la incorporación de nuevos usuarios (consulte "Incorporación de usuarios" (p. 1361)).

Para realizar acciones específicas en un usuario determinado, haga clic en la fila del usuario correspondiente. A continuación, puede:

- Restablezca su contraseña (consulte "Restablecimiento de contraseñas de usuario" (p. 1365)).
- Corregir los riesgos de usuario (consulte "Corrección de riesgos de usuario" (p. 1362)).
- Dar de baja al usuario (consulte "Dar de baja a usuarios" (p. 1365)).

Nota
Actualmente, solo puede editar los detalles del usuario y gestionar aplicaciones y licencias en Microsoft 365. Para obtener más información, consulte la documentación de Microsoft.

Incorporación de usuarios

Puede incorporar nuevos usuarios a un inquilino de Microsoft 365 a través del servicio de gestión de Microsoft 365.

Pasos para incorporar a un nuevo usuario

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Usuarios**.
2. Haga clic en **Incorporar usuario**.
3. En el cuadro de diálogo, indique los siguientes detalles del usuario:

© Acronis International GmbH, 2003-2025

- [Opcional] **Nombre**: el nombre del usuario.
- [Opcional] **Apellido**: el apellido del usuario.
- **Nombre que se muestra**: el nombre que se muestra a los destinatarios del correo electrónico.
- **Nombre de usuario**: el nombre de usuario al iniciar sesión.
- [Opcional] **Dominio**: seleccione el dominio de Microsoft 365 correspondiente en el menú desplegable.
- **Ubicación**: seleccione el país correspondiente en el menú desplegable.
- **Contraseña**: introduzca la contraseña necesaria para iniciar sesión.
- [Opcional] En la sección **Información de contacto**, introduzca la información pertinente.

4. [Opcional] Seleccione la casilla de verificación **Solicitar al usuario que cambie su contraseña cuando inicie sesión por primera vez** si desea que los usuarios cambien sus contraseñas al iniciar sesión por primera vez.
5. Haga clic en **Crear**.

Corrección de riesgos de usuario

Puede corregir un número de riesgos de seguridad relacionados con una cuenta de Microsoft 365 de un usuario específico. Tenga en cuenta que solo puede corregir un riesgo de usuario a la vez.

Los riesgos que puede corregir incluyen:

- Cuentas de administrador con un buzón de correo: elimine los privilegios de administrador de las cuentas donde se requiera el buzón de correo y cree una nueva cuenta de administrador independiente para el usuario.
- Cuentas de invitados, usuarios y administradores inactivas: identifique a los exempleados u otras cuentas sin usar y elimine las cuentas de administrador y otras que ya no sean necesarias.
- Cuentas con autenticación multifactor deshabilitado o sin registrar: evalúe qué cuentas de usuario corren riesgo según la configuración de autenticación multifactor y las líneas base necesarias.
- Cuentas de administrador anónimas: determine si los usuarios que requieren privilegios de administrador deben recibir una cuenta de administrador independiente (sin un buzón de correo).
- Cuentas con buzones de correo compartidos configurados incorrectamente: identifique los usuarios correspondientes que necesitan “Enviar como” o tener “Acceso total” a la cuenta compartida.

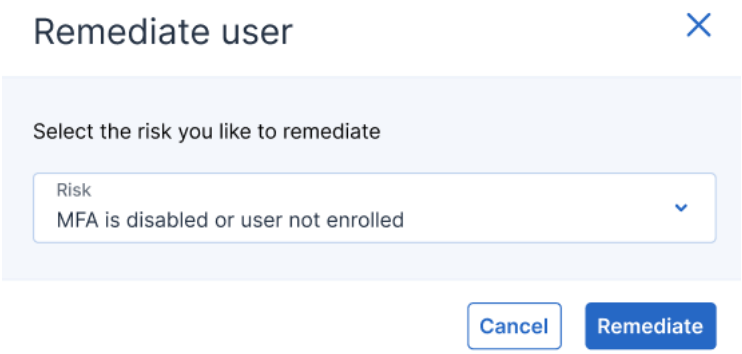
Nota
Para corregir los riesgos de usuario, debe habilitarse el modo de producto avanzado.

Pasos para corregir los riesgos de usuario

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Usuarios**.
2. Seleccione la casilla de verificación en la fila del usuario correspondiente y, a continuación, haga clic en **Corregir usuario**.
   Si está trabajando en el modo de producto gratuito, se le pedirá que cambie al modo de producto avanzado.

   Nota
   En licencias basadas en servicios, el modo gratuito requiere que la cuota de servicio **Protección estándar** > **Licencias de Microsoft 365** se aplique a todas las licencias de Microsoft 365 del cliente. El modo avanzado requiere que la cuota de servicio **RMM** > **Licencias de Microsoft 365** se aplique a todas las licencias de Microsoft 365 del cliente.
   En licencias basadas en soluciones, la funcionalidad completa se activa con la licencia de **Seguridad y RMM** o **Protección definitiva**.
3. En el diálogo **Habilitar modo avanzado**, haga clic en **Habilitar**.
4. En el menú desplegable **Riesgo**, seleccione el riesgo que desea corregir y, a continuación, haga clic en **Solucionar**.



La siguiente tabla enumera los riesgos y los pasos de corrección que se aplican al hacer clic en **Solucionar**.

Riesgo	Pasos de corrección
La autenticación multifactor está deshabilitada o el usuario no está registrado	La autenticación multifactor está habilitada para el usuario.

© Acronis International GmbH, 2003-2025

Riesgo	Pasos de corrección
Cuentas inactivas	Detiene cualquier nueva sesión iniciada para la cuenta de usuario o administrador inactiva seleccionada. Si el usuario o el administrador están conectados, se desconectarán automáticamente de todos los servicios de Microsoft en un plazo de 60 minutos.
Administradores inactivos	
Buzones de correo de administrador	Elimina los privilegios de administrador de la cuenta seleccionada y crea una cuenta de administrador nueva e independiente (sin licencia) para el usuario. El sistema también genera automáticamente un archivo CSV que enumera las cuentas de administrador creadas y sus contraseñas de un solo uso.
Administradores anónimos	Elimina la cuenta de administrador anónimo.
Buzones de correo compartidos	Convierte la cuenta de usuario en un

© Acronis International GmbH, 2003-2025

Riesgo	Pasos de corrección
	buzón compartido. A continuación, puede delegar "Enviar como" o "Acceso completo" a los usuarios correspondientes.
Invitados	Elimina la cuenta de usuario invitado inactiva.

5. En el cuadro de diálogo de confirmación, haga clic en **Confirmar**. A continuación, haga clic en **Cerrar**.

Restablecimiento de contraseñas de usuario

Puede restablecer la contraseña de Microsoft 365 de un usuario específico.

Pasos para restablecer la contraseña de un usuario de Microsoft 365

1. En la pantalla principal de usuarios, haga clic en la fila del usuario correspondiente.
2. Haga clic en **Restablecer contraseña**.
3. En el diálogo que se muestra, introduzca la nueva contraseña del usuario.
4. Si desea obligar al usuario a cambiar su contraseña, seleccione **Requerir que el usuario cambie su contraseña cuando inicie sesión por primera vez**.
5. Haga clic en **Guardar**.
6. En el cuadro de diálogo de confirmación, haga clic en **Cerrar**.

Dar de baja a usuarios

Puede dar de baja usuarios de un inquilino de Microsoft 365 a través del servicio de gestión de Microsoft 365.

Pasos para dar de baja a usuarios

1. En la consola de Cyber Protect, vaya a **Gestión de Microsoft 365** > **Usuarios**.
2. Seleccione la casilla de verificación en la columna del extremo izquierdo del usuario que desea dar de baja y, a continuación, haga clic en **Dar de baja al usuario**.
   Si está trabajando en el modo de producto gratuito, se le pedirá que cambie al modo de producto avanzado.

© Acronis International GmbH, 2003-2025

Nota

En licencias basadas en servicios, el modo gratuito requiere que la cuota de servicio **Protección estándar** > **Licencias de Microsoft 365** se aplique a todas las licencias de Microsoft 365 del cliente. El modo avanzado requiere que la cuota de servicio **RMM** > **Licencias de Microsoft 365** se aplique a todas las licencias de Microsoft 365 del cliente.

En licencias basadas en soluciones, la funcionalidad completa se activa con la licencia de **Seguridad y RMM** o **Protección definitiva**.

3. En el cuadro de diálogo Habilitar modo avanzado, haga clic en **Habilitar**.
4. Modifique la configuración de Microsoft 365 del usuario en las siguientes secciones, según sea necesario:
   - **Configuraciones del usuario**
   - **Asignar delegados de buzones de correo**
   - **Acción de respuesta automática**
   - **Conservación por juicios**
5. Haga clic en **Guardar**.
6. En el cuadro de diálogo de confirmación, haga clic en **Cerrar**.
   Se da de baja al usuario del inquilino de Microsoft 365 correspondiente.

© Acronis International GmbH, 2003-2025

Gestión del inventario de hardware

Cuando habilita la función de inventario de hardware, puede ver todos los componentes de hardware que están disponibles en:

- los dispositivos físicos Windows y macOS con una licencia compatible con la característica del inventario de hardware.
- las máquinas virtuales Windows y macOS que funcionen en las siguientes plataformas de virtualización:

  VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo y Virtuozzo Hybrid Infrastructure.

  Para obtener más información sobre las versiones compatibles de las plataformas de virtualización, consulte "Plataformas de virtualización compatibles" (p. 511).

Nota
La característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.

La característica del inventario de hardware es compatible solo con los dispositivos en los que está instalado un agente de protección.

Para obtener datos del inventario de hardware, puede ejecutar análisis automáticos o manuales en los dispositivos.

Puede utilizar los datos del inventario de hardware para:

- Descubrir todos los recursos de hardware de la organización.
- Buscar en el inventario de hardware de todos los dispositivos de su organización.
- Comparar los componentes de hardware en varios dispositivos.
- Muestra información detallada acerca de un componente de hardware.

Habilitar o deshabilitar el análisis de inventario de hardware

Cuando se habilita el análisis de inventario de hardware en dispositivos físicos y máquinas virtuales, el sistema recopila automáticamente los datos de hardware cada 12 horas.

La función de análisis de inventario de hardware viene habilitada de forma predeterminada, pero puede modificar la configuración cuando sea necesario.

Nota
Solo los inquilinos de cliente pueden habilitar o deshabilitar el análisis de inventario de hardware. Los inquilinos unidad pueden ver los ajustes del análisis de inventario de hardware, pero no pueden modificarlos.

Habilitar

© Acronis International GmbH, 2003-2025

Pasos para habilitar el análisis de inventario de hardware

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Gestión**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Análisis del inventario de hardware**.

Deshabilitar

Pasos para deshabilitar el análisis de inventario de hardware

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Gestión**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para deshabilitar el módulo **Análisis del inventario de hardware**.

Inicio manual de un análisis de inventario de hardware

Puede iniciar manualmente un análisis de inventario de hardware para un único dispositivo y ver los datos actuales de los componentes de hardware del dispositivo.

Nota
El análisis del inventario de hardware de las máquinas virtuales solo es compatible cuando la fecha y la hora actual de la máquina virtual corresponde a la fecha y la hora actual en UTC. Para asegurarse de que la máquina virtual utiliza la configuración de hora correcta, desactive la opción **Sincronización de hora** de la máquina virtual, establezca la fecha, la hora y la zona horaria actuales y reinicie **Acronis Agent Core Service** y **Acronis Managed Machine Service**.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- Los dispositivos tienen una licencia compatible con la función de inventario de hardware.

  Nota
  Tenga en cuenta que la función de inventario de hardware para las máquinas virtuales no es compatible con las ediciones (heredadas) de Cyber Protect.

- Un agente de protección está instalado en el dispositivo.
- [Si el dispositivo es una máquina virtual] La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Gestión del inventario de hardware" (p. 1367).

Pasos para iniciar un análisis de inventario de hardware en un único dispositivo

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desea analizar y, a continuación, pulse en **Inventario**.
3. En la pestaña **Hardware**, haga clic en **Analizar ahora**.

Búsqueda en el inventario de hardware

Puede ver y explorar los datos de todos los componentes de hardware que están disponibles en todos los dispositivos de su organización.

Requisitos previos

- Los dispositivos deben tener un sistema operativo Windows o macOS.
- Los dispositivos tienen una licencia compatible con la función de inventario de hardware.

> **Nota**
> La característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.

- Un agente de protección está instalado en el dispositivo.
- El análisis de inventario de hardware de los dispositivos se ha realizado correctamente.
- [Si el dispositivo es una máquina virtual] La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Gestión del inventario de hardware" (p. 1367).

Pasos para ver todos los componentes de hardware que están disponibles en los dispositivos de Windows y macOS

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. En el campo desplegable **Vista:**, seleccione **Hardware**.

> **Nota**
> Vista es un conjunto de columnas que determina los datos que se ven en la pantalla. Las vistas predefinidas son **Estándar** y **Hardware**. Puede crear y guardar vistas personalizadas que incluyan distintos conjuntos de columnas y que resulten más prácticas para sus necesidades.

En la siguiente tabla se describen los datos que aparecen en la vista **Hardware**.

Columna	Descripción
Nombre	Nombre de dispositivo.
Estado del análisis de hardware	Estado del análisis de hardware. • **Completado**. • **Sin iniciar**. • **No compatible**. Este estado se muestra para

© Acronis International GmbH, 2003-2025

Columna	Descripción
	las cargas de trabajo para las que no se admite la funcionalidad de inventario de hardware. Por ejemplo, máquinas virtuales, dispositivos móviles y dispositivos Linux. • **Actualizar agente**. Este estado se muestra cuando se ha instalado una versión obsoleta del agente en el dispositivo. Hacer clic en esta acción redirigirá a la página **Configuración** > **Agentes**, donde los administradores pueden actualizar el agente. • **Actualizar licencia**. Al pulsar en este estado se abre un cuadro de diálogo donde los administradores pueden cambiar la licencia actual por otra de las licencias que están disponibles para el inquilino.
Procesador	Modelos de todos los procesadores del dispositivo.
Núcleos de procesador	Número de núcleos de todos los procesadores del dispositivo.
Almacenamiento en disco	El almacenamiento utilizado y el almacenamiento total de todos los discos del dispositivo.
Memoria	La capacidad de RAM del dispositivo.
Fecha del análisis	La fecha y la hora del último análisis de inventario de hardware.
Placa base	La placa base del dispositivo.
Número de serie de la placa base	El número de serie de la placa base.
Número de serie	Número de serie del sistema del dispositivo.
Versión del BIOS	La versión del BIOS del sistema.
Organización	Organización a la que pertenece el dispositivo.
Propietario	Propietario del dispositivo.
Dominio	Dominio del dispositivo.
Sistema operativo	Sistema operativo del dispositivo.
Compilación del sistema operativo	Compilación del sistema operativo del dispositivo.

© Acronis International GmbH, 2003-2025

3. [Opcional] Para añadir columnas a la tabla, haga clic en el icono de engranaje y seleccione aquellas columnas que desee incluir en la tabla.
4. [Opcional] Para disminuir la cantidad de información que aparece en la pantalla, utilice uno o más filtros.
   a. Haga clic en **Buscar**.
   b. Haga clic en la flecha y, a continuación, haga clic en **Hardware**.
   c. Seleccione un filtro o una combinación de varios filtros.
      En la siguiente tabla se describen los filtros de **Hardware**.

Filtro	Descripción
Modelo de procesador	Es posible seleccionar varias opciones. Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con el modelo de procesador especificado.
Núcleos de procesador	Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con el número de núcleos de procesador especificado.
Tamaño total del disco	Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con el tamaño total de disco especificado.
Capacidad de memoria	Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con la capacidad de memoria especificada.

   d. Haga clic en **Aplicar**.
5. [Opcional] Para ordenar los datos de forma ascendente, haga clic en el nombre de una columna.

Visualización del hardware de un solo dispositivo

Puede ver información detallada acerca de la placa base, procesadores, memoria, gráficos, unidades de almacenamiento, redes y sistema de un dispositivo específico.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- El dispositivo tiene una licencia compatible con la función de inventario de hardware.

> **Nota**
> La característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.

- Un agente de protección está instalado en el dispositivo.
- El análisis de inventario de hardware del dispositivo se ha realizado correctamente.
- [Si el dispositivo es una máquina virtual] La máquina se ejecuta en una de las plataformas de

© Acronis International GmbH, 2003-2025

virtualización compatibles. Para obtener más información, consulte "Gestión del inventario de hardware" (p. 1367).

Pasos para ver información detallada acerca del hardware de un dispositivo específico

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. En el campo desplegable **Vista:**, seleccione **Hardware**.
3. Busque el dispositivo que desee inspeccionar empleando uno de los métodos que se describen a continuación.
   - Buscar el dispositivo mediante la opción **Filtro**:
     a. Haga clic en **Filtro**.
     b. Seleccione un filtro o una combinación de varios parámetros de filtro para buscar el dispositivo.
     c. Haga clic en **Aplicar**.
   - Buscar el dispositivo mediante la opción **Buscar**:
     a. Haga clic en **Buscar**.
     b. Escriba el nombre completo del dispositivo o parte del mismo y haga clic en **Introducir**.
4. Haga clic en la fila donde aparece el dispositivo, y haga clic en **Inventario**.
5. Haga clic en la pestaña **Hardware**.
   Se muestran los datos de hardware siguientes.

Componente de hardware	Información que se muestra
Placa base	Nombre, fabricante, modelo y número de serie de la placa base del dispositivo.
Procesadores	Fabricante, modelo, velocidad máxima del reloj y número de núcleos de cada procesador del dispositivo.
Memoria	Capacidad, fabricante y número de serie de la memoria del dispositivo.
Gráficos	Fabricante y modelo de las GPU del dispositivo.
Unidades de almacenamiento	Modelo, tipo de medio, espacio disponible y tamaño de las unidades de almacenamiento del dispositivo.
Red	Dirección MAC, dirección IP y tipo de adaptadores de red del dispositivo.
Sistema	ID del producto, fecha de instalación original, tiempo de arranque del sistema, fabricante del sistema, modelo del sistema, número de serie, versión de la BIOS, dispositivo de arranque,

© Acronis International GmbH, 2003-2025

Componente de hardware	Información que se muestra
	configuración regional del sistema y zona horaria del sistema.

© Acronis International GmbH, 2003-2025

Gestión de software

Nota
Para acceder a esta funcionalidad, debe tener uno de los siguientes roles de Cyber Protection: administrador de la empresa, administrador de cibernética o administrador de solo lectura.

Las funciones de gestión de software de Cyber Protection abarcan todo el ciclo de vida del software.

- Despliegue de software mediante DeployPilot: añada paquetes de software al repositorio de software y despliegue rápidamente software en recursos informáticos remotos.
- Exploración de inventario: ejecute exploraciones de inventario automáticas o manuales en los dispositivos y obtenga una visibilidad completa sobre el software que está instalado en ellos.
- Evaluación de vulnerabilidades: ejecute análisis de vulnerabilidades para identificar vulnerabilidades en los sistemas operativos y el software que están instalados en los dispositivos.
- Gestión de parches: gestione parches (actualizaciones) para los sistemas operativos y el software que están instalados en sus dispositivos y mantenga los sistemas actualizados.

Gestión del inventario de software

La disponibilidad de esta función depende de la licencia que se asigne a su carga de trabajo.

La función le permite ver todas las aplicaciones de software que están instaladas en todos los dispositivos Windows y macOS.

Para obtener datos del inventario de software, puede ejecutar análisis automáticos o manuales en los dispositivos.

Puede utilizar los datos del inventario de software para:

- buscar y comparar información acerca de todas las aplicaciones instaladas en los dispositivos de la empresa
- determinar si es necesario actualizar una aplicación
- determinar si es necesario eliminar una aplicación sin usar
- comprobar que la versión de software de varios dispositivos de la compañía sea la misma
- supervisar los cambios en el estado del software entre análisis consecutivos.

Habilitar o deshabilitar el análisis del inventario de software

Cuando se habilita el análisis de inventario de software en los dispositivos, el sistema recopila automáticamente los datos de software cada 12 horas.

La función de análisis de inventario de software viene habilitada de forma predeterminada para todos los dispositivos que tienen la licencia necesaria, pero puede modificar la configuración siempre que lo desee.

© Acronis International GmbH, 2003-2025

Nota
Solo los inquilinos de cliente pueden habilitar o deshabilitar el análisis de inventario de software. Los inquilinos unidad pueden ver los ajustes del análisis de inventario de software, pero no pueden modificarlos.

Habilitar

Pasos para habilitar el escaneo de inventario de software

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Gestión**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Análisis del inventario de software**.

Deshabilitar

Pasos para deshabilitar el escaneo de inventario de software

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Gestión**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para deshabilitar el módulo **Análisis del inventario de software**.

Inicio manual de un análisis de inventario de software

Puede iniciar manualmente un análisis de inventario de software desde la pantalla **Inventario de software** o desde la pestaña **Software** en la pantalla **Inventario**.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- El dispositivo tiene la licencia requerida.

Desde inventario de software

Pasos para iniciar un análisis de inventario de software desde la pantalla Inventario de software

1. En la consola de Cyber Protect, vaya a **Gestión del software**.
2. Haga clic en **Inventario de software**.
3. En el menú desplegable **Agrupar por:**, seleccione **Dispositivos**.
4. Busque el dispositivo que desea analizar y, a continuación, haga clic en **Analizar ahora**.

Desde software

© Acronis International GmbH, 2003-2025

Pasos para iniciar un análisis de inventario de software desde la pestaña Software en la pantalla Inventario

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desea analizar y, a continuación, pulse en **Inventario**.
3. En la pestaña **Software**, haga clic en **Analizar ahora**.

Búsqueda en el inventario de software

Puede ver y navegar por los datos de todas las aplicaciones de software que están disponibles en todos los dispositivos de su organización.

Requisitos previos

- Los dispositivos deben tener un sistema operativo Windows o macOS.
- Los dispositivos tienen la licencia requerida.
- Al menos un análisis de inventario de software en los dispositivos se completó correctamente.

Pasos para ver todas las aplicaciones de software que están disponibles en todos los dispositivos de Windows y macOS

1. En la consola de Cyber Protect, vaya a **Gestión del software**.
2. Haga clic en **Inventario de software**.
   De forma predeterminada, los datos se agrupan por dispositivo. En la siguiente tabla se describen los datos que aparecen en la pantalla **Inventario de software**.

Columna	Descripción
Nombre	Nombre de la aplicación.
Versión	Versión de la aplicación.
Estado	Estado de la aplicación. • **Nueva**. • **Actualización realizada**. • **Eliminada**. • **No hay cambios**.
Proveedor	Proveedor de la aplicación.
Fecha de instalación	La fecha y la hora en las que se instaló la aplicación.
Última ejecución	Solo para dispositivos con macOS. La fecha y la hora en las que la aplicación estuvo activa por última vez.
Ubicación	Directorio en el que se ha instalado la aplicación.

© Acronis International GmbH, 2003-2025

Columna	Descripción
Usuario	Usuario para quien se instaló la aplicación.
Tipo de sistema	Solo para dispositivos con Windows. Tipo de bits de la aplicación. • **X86** para aplicaciones de 32 bits. • **X64** para aplicaciones de 64 bits.

3. Para agrupar los datos por aplicación, en el campo desplegable **Agrupar por:** seleccione **Aplicaciones**.
4. Para disminuir la cantidad de información que aparece en la pantalla, utilice un filtro o una combinación de filtros.
   a. Haga clic en **Filtro**.
   b. Seleccione un filtro o una combinación de varios filtros.
      En la siguiente tabla se describen los datos de la pantalla **Inventario de software**.

Filtro	Descripción
Nombre de dispositivo	Nombre de dispositivo. Es posible seleccionar varias opciones. Use este filtro si desea comparar el software de dispositivos específicos.
Aplicación	Nombre de la aplicación. Es posible seleccionar varias opciones. Con este filtro, puede comparar los datos de una aplicación concreta de dispositivos específicos o de todos los dispositivos.
Proveedor	Proveedor de la aplicación. Es posible seleccionar varias opciones. Use este filtro si desea ver todas las aplicaciones de un proveedor concreto de dispositivos específicos o de todos los dispositivos.
Estado	Estado de la aplicación. Es posible seleccionar varias opciones. Use este filtro si desea ver todas las aplicaciones con el estado seleccionado de dispositivos específicos o de todos los dispositivos.
Fecha de instalación	Fecha en la que se ha instalado la aplicación. Use este filtro si desea ver todas las aplicaciones instaladas en una fecha específica de dispositivos específicos o de todos los dispositivos.
Fecha del análisis	Fecha del análisis de inventario de software. Use este filtro si desea ver la información acerca del software de dispositivos específicos o de todos los dispositivos analizados en esa fecha.

   c. Haga clic en **Aplicar**.

© Acronis International GmbH, 2003-2025

5. Para buscar en toda la lista de inventario de software, use la paginación que aparece en la parte inferior izquierda de la pantalla.

- Haga clic en el número de la página que desea abrir.
- En la lista desplegable, seleccione el número de página de la página que desea abrir.

Visualización del inventario de software de un solo dispositivo

Puede ver una lista de todas las aplicaciones de software instaladas en un solo dispositivo e información detallada acerca de las aplicaciones, como el estado, la versión, proveedor, fecha de instalación, última ejecución y ubicación.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- El dispositivo tiene la licencia requerida.
- Al menos un análisis de inventario de software en el dispositivo finalizó correctamente.

Desde inventario de software

Pasos para ver el inventario de software de un único dispositivo desde la pantalla Inventario de software

1. En la consola de Cyber Protect, vaya a **Gestión del software**.
2. Haga clic en **Inventario de software**.
3. En el menú desplegable **Agrupar por:**, seleccione **Dispositivos**.
4. Busque el dispositivo que desea inspeccionar, utilizando una de las siguientes opciones.
   - Utilice **Filtro**:
     a. Haga clic en **Filtro**.
     b. En el campo **Nombre de dispositivo**, seleccione el nombre de dispositivo que desea ver.
     c. Haga clic en **Aplicar**.
   - Utilice **Buscar**:
     a. Haga clic en **Buscar**.
     b. Escriba el nombre completo del dispositivo o parte del mismo.

Desde Dispositivos

Pasos para visualizar el inventario de software de un solo dispositivo desde la pantalla Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desea ver y luego en **Inventario**.
3. Haga clic en la pestaña **Software**.

© Acronis International GmbH, 2003-2025

Acceso a vulnerabilidades y gestión de parches

La **evaluación de vulnerabilidades** es un proceso que consiste en identificar, cuantificar y priorizar las vulnerabilidades encontradas en el sistema. Con el módulo de evaluación de vulnerabilidades, podrá analizar los equipos en busca de vulnerabilidades y asegurarse de que todos los sistemas operativos y las aplicaciones instaladas estén actualizados y funcionen correctamente.

El análisis de evaluación de vulnerabilidades es compatible con equipos con los siguientes sistemas operativos:

- Windows. Para obtener más información, consulte "Productos de Microsoft y de terceros compatibles con la evaluación de vulnerabilidades" (p. 1380).
- macOS. Para obtener más información, consulte "Productos de Apple y de terceros compatibles con la evaluación de vulnerabilidades" (p. 1381).
- Equipos Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Para obtener más información, consulte "Productos de Linux compatibles para la evaluación de vulnerabilidades" (p. 1382).

Utilice la función de **gestión de parches** para gestionar los parches (actualizaciones) de las aplicaciones y los sistemas operativos instalados en sus equipos y mantener actualizados sus sistemas. Con el módulo de gestión de parches, podrá aprobar manual o automáticamente la instalación de actualizaciones en sus equipos.

La gestión de parches es compatible con equipos con sistemas operativos Windows. Para obtener más información, consulte "Productos de Microsoft y de terceros compatibles con la evaluación de vulnerabilidades" (p. 1380).

Evaluación de vulnerabilidades

El proceso de evaluación de vulnerabilidades está formado por los siguientes pasos:

1. Cree un plan de protección con el módulo de evaluación de vulnerabilidades habilitado, especifique los ajustes de la evaluación de vulnerabilidades y asigne el plan a los equipos.
2. El sistema, si está planificado o se le pide, envía un comando para que se ejecute la evaluación de vulnerabilidades en los agentes de protección instalados en los equipos.
3. Los agentes reciben el comando, empiezan analizar equipos en busca de vulnerabilidades y generan la actividad de análisis.
4. Cuando haya terminado la evaluación de vulnerabilidades, los agentes generan los resultados y los envían al servicio de supervisión.
5. El servicio de supervisión procesa los datos de los agentes y muestra los resultados en los widgets de evaluación de vulnerabilidades y en la lista de vulnerabilidades encontradas.
6. Cuando tenga una lista de vulnerabilidades encontradas, podrá procesarla y decidir cuáles se deben solucionar.

Puede comprobar los resultados del análisis de la evaluación de vulnerabilidades en los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

© Acronis International GmbH, 2003-2025

Productos de Microsoft y de terceros compatibles con la evaluación de vulnerabilidades

Los siguientes productos de Microsoft y de terceros para sistemas operativos Windows son compatibles con la evaluación de vulnerabilidades y la administración de parches:

Productos de Microsoft compatibles

Sistemas operativos de escritorio

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 (Enterprise, Professional, Ultimate)

Sistemas operativos de servidor

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office y componentes relacionados

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Componentes de Windows

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio y aplicaciones
- Componentes del sistema operativo

© Acronis International GmbH, 2003-2025

Aplicaciones del servidor

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2016

Productos de terceros compatibles con Windows

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Cyber Protect es compatible con la evaluación de vulnerabilidades y la gestión de parches de una amplia gama de aplicaciones de terceros, incluyendo herramientas de colaboración y clientes VPN, que son de vital importancia en escenarios de trabajo remotos, como por ejemplo los siguientes:

- Microsoft Teams
- Zoom
- Slack
- Webex
- NordVPN
- TeamViewer

Para obtener la lista completa de productos de terceros compatibles con Windows, consulte la Lista de productos de terceros compatibles con la gestión de parches (62853).

Productos de Apple y de terceros compatibles con la evaluación de vulnerabilidades

Los siguientes productos de Apple y de terceros para macOS son compatibles con la evaluación de vulnerabilidades:

Productos de Apple compatibles

macOS

© Acronis International GmbH, 2003-2025

- macOS 10.13.x y posterior

Aplicaciones integradas de macOS

- Safari, iTunes y otros.

Productos de terceros compatibles para macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Thunderbird
- VLC media player

Para obtener la lista completa de productos de terceros compatibles con macOS, consulte la Lista de productos de terceros compatibles con la gestión de parches (62853).

Productos de Linux compatibles para la evaluación de vulnerabilidades

Distribuciones Linux y versiones de este sistema operativo que son compatibles con la evaluación de vulnerabilidades (EV):

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Configuración de la evaluación de vulnerabilidades

Para obtener más información sobre cómo crear un plan de protección con el módulo de **Evaluación de vulnerabilidades**, consulte "Creación de un plan de protección". El análisis de la evaluación de vulnerabilidades se puede llevar a cabo según la planificación o cuando se desee (mediante la acción **Ejecutar ahora** de un plan de protección).

Puede especificar los ajustes siguientes en el módulo de **Evaluación de vulnerabilidades**.

Qué analizar

Seleccione los productos de software que quiera analizar para detectar vulnerabilidades:

© Acronis International GmbH, 2003-2025

- Equipos Windows:
  - **Productos de Microsoft**: esta opción es parte del plan de protección estándar.
  - **Productos de terceros para Windows**: la disponibilidad de esta opción depende de la licencia. Para obtener más información sobre los productos de terceros compatibles con el SO Windows, consulte Lista de productos de terceros compatibles con administración de parches.
- Equipos macOS:
  - **Productos de Apple**
  - **Productos de terceros para macOS**
- Equipos Linux:
  - **Analizar paquetes de Linux**

Planificación

Defina la planificación que se deberá seguir para llevar a cabo el análisis de la evaluación de vulnerabilidades en los equipos seleccionados:

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario inicie sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario cierre sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación. • **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes:

© Acronis International GmbH, 2003-2025

Campo	Descripción
	• **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.
Especifique una cuenta de usuario que al cerrar sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el

© Acronis International GmbH, 2003-2025

Campo	Descripción
	retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo** • **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.

Evaluación de vulnerabilidades para equipos Windows

Puede analizar equipos Windows y productos de terceros para Windows para buscar vulnerabilidades.

Nota
La disponibilidad de esta función depende de la licencia que se asigne a su carga de trabajo y puede incurrir en costes adicionales.

Pasos para configurar la evaluación de vulnerabilidades para equipos Windows

1. En la consola de Cyber Protect, cree un plan de protección y habilite el módulo **Evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione una o ambas opciones.
     - **Productos de Microsoft**: esta opción es parte de las funciones de protección estándar.
     - **Productos de terceros para Windows**: esta opción es parte de RMM (modo de licencia basado en servicios) o Seguridad y RMM (modo de licencia basado en soluciones).
   - **Planificación**: define la planificación para ejecutar la evaluación de vulnerabilidades.

   Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1382).
3. Asigne el plan a los equipos Windows.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

© Acronis International GmbH, 2003-2025

Evaluación de vulnerabilidades para equipos Linux

Puede escanear equipos Linux en busca de vulnerabilidades a nivel de aplicación y núcleo.

Para configurar la evaluación de vulnerabilidades en equipos Linux

1. En la consola de Cyber Protect, cree un plan de protección y habilite el módulo **Evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione **Analizar paquetes de Linux**.
   - **Planificación**: define la planificación para ejecutar la evaluación de vulnerabilidades.

   Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1382).
3. Asigne el plan a los equipos de Linux.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

Evaluación de vulnerabilidades para dispositivos macOS

Puede analizar los dispositivos macOS para buscar vulnerabilidades a nivel del sistema operativo y de las aplicaciones.

Pasos para configurar la evaluación de vulnerabilidades para dispositivos macOS

1. En la consola de Cyber Protect, cree un plan de protección y habilite el módulo **Evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione **Productos de Apple**, **productos de terceros para macOS** o ambos.
   - **Planificación**: define la planificación para ejecutar la evaluación de vulnerabilidades.

   Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1382).
3. Asigne el plan a los dispositivos de macOS.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

© Acronis International GmbH, 2003-2025

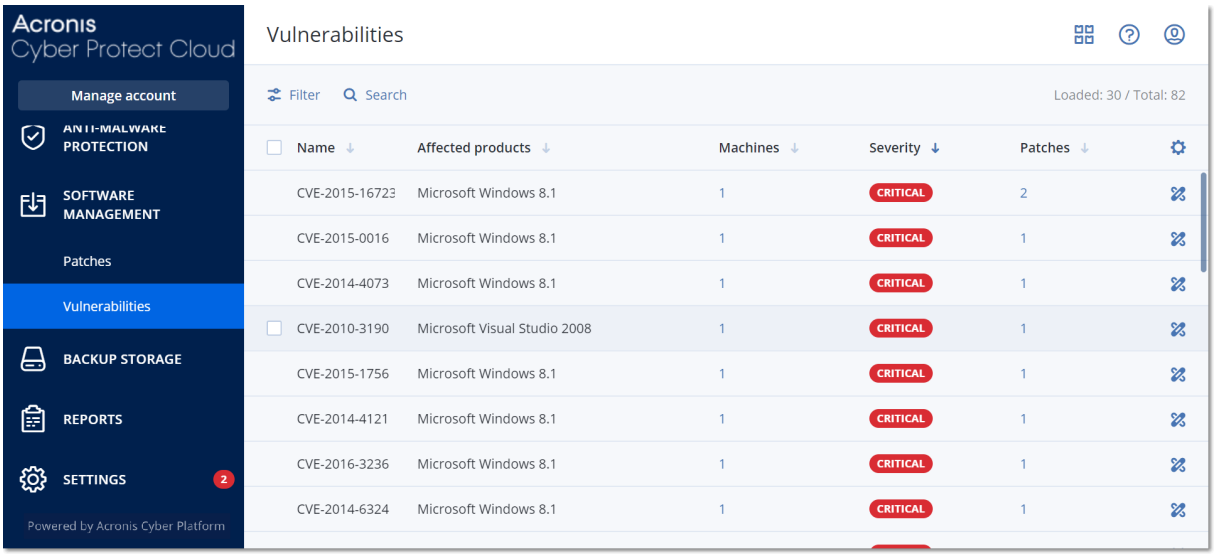
Gestión de vulnerabilidades encontradas

Si la evaluación de vulnerabilidades se ha llevado a cabo al menos una vez y se detecta alguna vulnerabilidad, las podrá encontrar en **Gestión del software** > **Vulnerabilidades**. En la lista de vulnerabilidades se muestran tanto aquellas en las que hay que instalar parches como para las que no hay ningún parche sugerido. Puede usar el filtro para mostrar únicamente las vulnerabilidades con parches.

Nombre	Descripción
Nombre	Nombre de la vulnerabilidad.
Productos afectados	Productos de software en los que se han encontrado vulnerabilidades.
Equipos	Número de equipos afectados.
Gravedad	La gravedad de la vulnerabilidad encontrada. Se pueden asignar los siguientes niveles según el sistema Common Vulnerability Scoring System (CVSS): • **Crítico**: 9-10 CVSS • **Alto**: 7-9 CVSS • **Medio**: 3-7 CVSS • **Bajo**: 0-3 CVSS • **Ninguno**
Parches	Número de parches adecuado.
Fecha de publicación	La fecha y la hora en las que se publicó la vulnerabilidad en Vulnerabilidades y exposiciones comunes (CVE).
Fecha de la detección	Fecha en la que se detectó por primera vez una vulnerabilidad existente en equipos.

Si hace clic en su nombre en la lista, encontrará la descripción de las vulnerabilidades encontradas.

© Acronis International GmbH, 2003-2025



Pasos para iniciar el proceso de resolución de vulnerabilidades

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Seleccione la vulnerabilidad en la lista y, a continuación, haga clic en **Instalar parches**. Se abrirá el asistente de solución de vulnerabilidades.
3. Seleccione los parches que se van a instalar en los equipos seleccionados y haga clic en **Siguiente**.
4. Seleccione los equipos en los cuales desea instalar los parches.
5. Seleccione las opciones de reinicio.

   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya

© Acronis International GmbH, 2003-2025

Opción	Descripción
automáticamente después de:	iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

6. Haga clic en **Instalar parches**.

   Como resultado, los parches seleccionados se instalan en los equipos indicados.

© Acronis International GmbH, 2003-2025

Gestión de parches

Nota

- La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.
- Para habilitar el módulo de **Gestión de parches** en el plan de protección, el módulo de **Evaluación de vulnerabilidades** debe estar habilitado.

Para obtener más información sobre los productos de terceros compatibles para Windows, consulte Lista de productos de terceros compatibles con gestión de parches (62853).

Utilice la funcionalidad de gestión de parches para:

- instalar actualizaciones a nivel de aplicación y sistema operativo
- aprobar la instalación manual o automática de parches
- instalar parches cuando se desee o según una planificación
- definir de forma precisa qué parches instalar según distintos criterios: gravedad, categoría y estado de aprobación
- llevar a cabo copias de seguridad previas a las actualizaciones por si no se realizan correctamente
- definir la acción de reinicio después de la instalación de parches

Nota

Para trabajar con las actualizaciones de Windows, la función de gestión de parches requiere que las actualizaciones de Windows estén habilitadas en la carga de trabajo. La función de gestión de parches se basa en el servicio de actualización de Windows, que detecta qué actualizaciones faltan y las propone en función de la versión del sistema operativo en ejecución existente.

Importante

La función de gestión de parches admite las actualizaciones a Windows 11. Sin embargo, debe verificar que las cargas de trabajo de Windows 10 que planea actualizar estén debidamente preparadas para ello. Consulte este artículo de Microsoft para obtener más información.

Para las actualizaciones de productos de terceros para Windows, Cyber Protection utiliza tecnología de par a par con el fin de minimizar el tráfico del ancho de banda de red. Puede elegir uno o varios agentes dedicados que descargarán actualizaciones de internet y las distribuirán ente otros agentes de la red. Además, todos los agentes compartirán actualizaciones con el resto como agentes del mismo nivel.

El flujo de trabajo de gestión de parches

El flujo de trabajo de gestión de parches incluye pasos para configurar y aplicar un plan de protección, ejecutar un análisis de evaluación de vulnerabilidades, configurar los ajustes de parches,

© Acronis International GmbH, 2003-2025

aprobar parches y, por último, instalar los parches que se hayan aprobado. Los pasos exactos del flujo de trabajo son los siguientes.

1. Configure un plan de protección que tenga los módulos **Evaluación de vulnerabilidades** y **Gestión de parches** habilitados.
2. Configure los ajustes de la evaluación de vulnerabilidades. Para obtener más información sobre esta configuración, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1382).
3. Configure los ajustes de la gestión de parches. Para obtener más información sobre esta configuración, consulte "Configuración de gestión de parches en el plan de protección" (p. 1391)
4. Aplique el plan de protección a uno o más equipos.
5. Espere a que se complete el análisis de evaluación de vulnerabilidades. El análisis comenzará automáticamente según la planificación configurada en el plan de protección. También puede iniciar el análisis bajo demanda manualmente haciendo clic en el icono **Ejecutar ahora** en el módulo **Evaluación de vulnerabilidades** del plan de protección.
6. Apruebe los parches. Puede definir la configuración de la aprobación automática de parches, que incluye la instalación automática de los parches en equipos de prueba. Para obtener más información, consulte "Aprobación automática de parches" (p. 1401). También puede aprobar los parches manualmente cambiando su estado de aprobación a **Aprobado**. Para obtener más información, consulte "Aprobar parches manualmente" (p. 1406).
7. Instale los parches. Los parches aprobados se pueden instalar automáticamente según la planificación configurada en el plan de protección. También puede instalar parches bajo demanda manualmente. Para obtener más información, consulte "Instalar parches bajo demanda" (p. 1406).

Puede revisar los resultados de la instalación de parches en el widget **Supervisión** > **Información general** > **Historial de instalación de parches**.

Configuración de gestión de parches en el plan de protección

En el módulo **Gestión de parches** del plan de protección, puede configurar los siguientes ajustes de gestión de parches:

- Qué actualizaciones se deben instalar para productos de Microsoft y terceros en sistemas operativos de Windows.
- Cuándo ejecutar la instalación automática de parches.
- Si se debe ejecutar una copia de seguridad antes de la actualización.

Para obtener más información sobre cómo crear un plan de protección y habilitar el módulo **Gestión de parches**, consulte "Creación de un plan de protección" (p. 250).

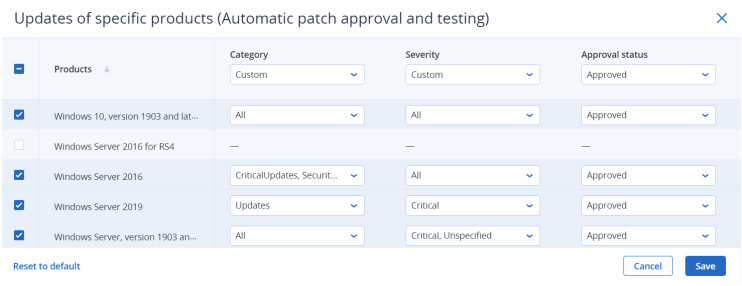
Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

© Acronis International GmbH, 2003-2025

Productos de Microsoft

Para instalar las actualizaciones de Microsoft en los equipos seleccionados

1. Active la opción **Actualizar productos de Microsoft** en el plan de protección.
2. Seleccione la opción de instalación:

Opción	Descripción
Todas las actualizaciones	Utilice esta opción si desea instalar todas las actualizaciones aprobadas.
Solo actualizaciones de seguridad y críticas	Utilice esta opción si desea instalar todas las actualizaciones críticas y de seguridad aprobadas.
Actualizaciones de productos específicos (aprobación y comprobación automática de parches)	Utilice esta opción si desea definir ajustes personalizados para diferentes productos. Si desea actualizar productos específicos, para cada producto puede definir qué actualizaciones instalar por categoría, gravedad o estado de aprobación. Seleccione esta opción si desea configurar las pruebas y la aprobación automática de pruebas de los parches. **Importante** La función de gestión de parches admite las actualizaciones a Windows 11. Sin embargo, debe verificar que las cargas de trabajo de Windows 10 que planea actualizar estén debidamente preparadas para ello. Consulte este artículo de Microsoft para obtener más información. 

En el caso de los productos de Microsoft, la distribución de parches usar el servicio de la API de Windows. Los parches y las actualizaciones no se descargan ni se almacenan internamente ni en agentes de distribución. Se descargan de Microsoft CDN. Por lo tanto, el agente no puede descargar ni distribuir parches aunque tenga asignado el rol de actualizador.

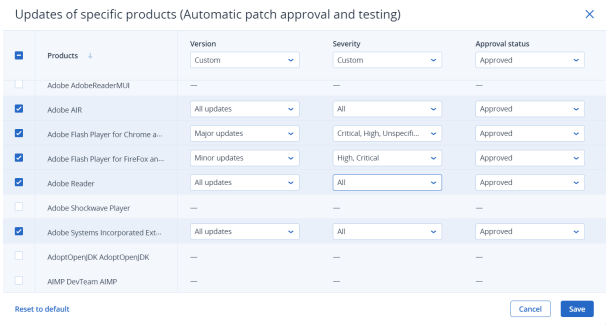
© Acronis International GmbH, 2003-2025

Productos de terceros a Windows

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Para instalar las actualizaciones de terceros en el sistema operativo Windows en los equipos seleccionados

1. Active la opción **Productos de terceros para Windows** en el plan de protección.
2. Seleccione las opciones de instalación:

Opción	Descripción
Todas las actualizaciones	Utilice esta opción si desea instalar todas las actualizaciones aprobadas. *
Solo actualizaciones importantes	Utilice esta opción si desea instalar todas las actualizaciones importantes aprobadas.
Solo actualizaciones menores	Utilice esta opción si desea instalar actualizaciones menores aprobadas.
Actualizaciones de productos específicos (aprobación y comprobación automática de parches)	Utilice esta opción si desea definir ajustes personalizados para diferentes productos. Si desea actualizar productos específicos, para cada producto puede definir qué actualizaciones instalar por categoría, gravedad o estado de aprobación. Seleccione esta opción si desea configurar las pruebas y la aprobación automática de pruebas de los parches. 
Instale las últimas versiones solo para las aplicaciones con vulnerabilidades detectadas	Marque esta casilla de verificación si desea instalar las últimas actualizaciones solo para las aplicaciones en las que se hayan detectado vulnerabilidades.

En el caso de los productos Windows de terceros, los parches de distribuyen directamente a las cargas de trabajo gestionadas desde una base de datos interna de Acronis. Si se asigna el rol de actualizador a un agente, este se utilizará para descargar y distribuir los parches.

© Acronis International GmbH, 2003-2025

Planificación

Defina la planificación y las condiciones que se seguirán para instalar las actualizaciones en los equipos seleccionados.

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, el inicio de sesión de cualquier usuario iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, cuando cualquier usuario cierre sesión se iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación. • **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes: • **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Configurar el	El campo se muestra si, en **Planificar la ejecución de tareas con los**

© Acronis International GmbH, 2003-2025

Campo	Descripción
periodo de mantenimiento para parches	**siguientes eventos**, ha seleccionado **Planificar por hora**. Seleccione esta configuración si desea que la instalación de parches se ejecute solo durante el intervalo de tiempo que especifique. Si no se completa el proceso de instalación de parches antes de la hora de finalización definida en el periodo de mantenimiento para parches, se detendrá automáticamente.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.
Especifique una cuenta de usuario que al cerrar sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar**

© Acronis International GmbH, 2003-2025

Campo	Descripción
	el equipo • **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.

Opciones de reinicio

Configure si desea que los recursos informáticos se reinicien después de la instalación de los parches.

La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe

© Acronis International GmbH, 2003-2025

Opción	Descripción
	reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

Copia de seguridad anterior a la actualización

Realizar una copia de seguridad antes de instalar actualizaciones de software: el sistema creará una copia de seguridad incremental del equipo antes de instalar cualquier actualización en él. Si anteriormente no se había creado ninguna copia de seguridad, se creará una copia de seguridad completa del equipo. Con esta opción podrá evitar situaciones en las que la instalación de actualizaciones no se realice correctamente y tenga que volver al estado anterior. Para que la opción **Copia de seguridad anterior a la actualización** funcione, los equipos correspondientes deben tener el módulo de copias de seguridad y el de gestión de parches habilitados en un plan de protección, y contar con los elementos que se van a incluir en la copia de seguridad, ya sea todo el equipo o los volúmenes de inicio del sistema de arranque. Si selecciona elementos inapropiados para la copia de seguridad, el sistema no le permitirá habilitar la opción **Copia de seguridad anterior a la actualización**.

© Acronis International GmbH, 2003-2025

Ver la lista de parches disponibles

Cuando se completa una evaluación de vulnerabilidades, puede ver información sobre los parches disponibles en **Gestión del software** > **Parches**.

Para ver los detalles de un parche de específico, haga clic en él en la lista de parches.

En la siguiente tabla se describe la información del parche que puede ver en la pantalla.

Columna	Descripción
Estado de aprobación	El estado de aprobación se necesita principalmente para aquellas situaciones en las que las aprobaciones se realizan automáticamente. Puede para definir uno de los siguientes estados para un parche: • **Aprobado**: el parche se ha instalado al menos en un equipo y se ha validado correctamente. • **Rechazado**: el parche no es seguro y puede dañar el sistema de un equipo. • **Aprobación pendiente**: el estado del parche no está claro y hay que validarlo
Acuerdo de licencia	• Acepto • No acepto. Si no acepta el acuerdo de licencia, el estado del parche pasa a ser **Rechazado** y no se instalará.
Gravedad	Nivel de gravedad del parche: • **Crítico** • **Alto** • **Medio** • **Bajo** • **Ninguno**
Proveedor	Proveedor del parche.
Producto afectado	Producto en el que se puede aplicar el parche.
Versiones instaladas	Versiones del producto que ya están instaladas.
Versión	Versión del parche.
Estabilidad	Puntuación de estabilidad del parche que indica si es seguro instalar el parche. Puede utilizar esta información para estimar el impacto potencial de un parche antes de su instalación y si un parche es estable o puede exponer a la organización a vulnerabilidades. Un parche puede tener una de las siguientes puntuaciones de estabilidad: • **Estable**: indica que el parche no tiene problemas ni preocupaciones informados en función del análisis de sentimientos y otras fuentes de datos y que el parche es conocido (hay suficientes datos sobre este parche en particular). Puede instalar este parche con confianza sin riesgo significativo.

© Acronis International GmbH, 2003-2025

	• **Problemas menores**: indica que el parche tiene algunos problemas informados, como problemas en la funcionalidad o la interfaz de usuario del producto, pero son menores, no críticos o tienen soluciones alternativas claras. Por lo general, puede continuar con la instalación del parche en la mayoría de los entornos, pero debe revisar primero los problemas. • **Precaución**: destaca que el parche tiene problemas significativos o generalizados informados, como causar inestabilidad del sistema, romper la funcionalidad o introducir vulnerabilidades de seguridad. En este caso, debe retrasar la instalación del parche, probarlo a fondo en un entorno controlado o esperar las actualizaciones del proveedor. • **Problemas críticos**: indica que el parche tiene problemas graves de alto impacto que pueden causar interrupciones importantes, como bloqueos del sistema, pérdida de datos o fallos críticos de la aplicación. Debe evitar instalar este parche hasta que el proveedor publique una solución o una guía sobre cómo actuar. Al hacer clic en los valores de esta columna, puede ver la siguiente información adicional sobre el parche: descripción general del parche, riesgos potenciales, estadísticas y parámetros, configuraciones específicas, información y recomendaciones, y experiencia del usuario. La información de **Estabilidad** se recopila de diversas fuentes externas mediante motores de búsqueda de IA.
Categoría	Categoría a la que pertenece el parche: • **Actualización crítica**: correcciones de amplia distribución para tratar problemas específicos asociados a errores críticos no relacionados con aspectos de seguridad. • **Actualización de la seguridad**: revisiones de amplia distribución para tratar problemas específicos asociados a errores de seguridad. • **Actualización de la definición**: actualizaciones aplicadas a virus u otros archivos de definiciones. • **Paquete acumulativo de actualizaciones**: conjuntos acumulativos de revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones que se recopilan para facilitar su implementación. Un paquete acumulativo está orientado normalmente a un área específica, como la seguridad, o a un componente de un producto, como Servicios de Internet Information Server (IIS). • **Paquete de servicio**: conjuntos acumulativos de todas las revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones creadas desde el lanzamiento del producto. Los paquetes de servicios también pueden contener un número limitado de funciones o cambios de diseño solicitados por el cliente. • **Herramienta**: utilidades o funciones que ayudan a llevar a cabo una tarea o un conjunto de tareas. • **Paquete de funciones**: lanzamientos de nuevas funciones que se suelen incluir en la última versión de los productos.

© Acronis International GmbH, 2003-2025

	• **Actualización**: correcciones que se emplean muchísimo para tratar problemas específicos asociados a errores que no son críticos ni están relacionados con aspectos de seguridad. • **Aplicación**: parches para una aplicación.
Fecha de publicación	Fecha en la que se publicó el parche.
Notificado por última vez	La fecha de la última vez que se notificó el parche
Instalado por primera vez	La fecha de la primera instalación correcta del parche en un equipo
KB de Microsoft	Si el parche es para un producto de Microsoft, el campo muestra el ID del artículo de la Base de conocimientos
Equipos	Número de equipos afectados.
Vulnerabilidades	Número de vulnerabilidades. Si hace clic en esta opción, se le redirigirá a la lista de vulnerabilidades.
Tamaño	Tamaño medio del parche.
Idioma	Idioma que admite el parche.
Sitio del proveedor	Sitio oficial del proveedor.

Configurar el tiempo de los parches en la lista

Para mantener la lista de parches actualizada, configure el tiempo que permanece cada parche en la lista desde la pantalla **Parches**. Esta configuración define el tiempo durante el cual el parche disponible detectado se conservará en la lista de parches. Se eliminará el parche de la lista una vez que se haya instalado correctamente en todos los equipos en los que faltaba o cuando transcurra el tiempo en la lista indicado.

Pasos para configurar el tiempo de los parches en la lista

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Haga clic en **Configuración**.
3. En **Tiempo en la lista**, seleccione la opción adecuada.

Opción	Descripción
Siempre	El parche se mantiene siempre en la lista.
7 días	El parche se eliminará de la lista siete días después de su primera instalación. Por ejemplo, supongamos que tiene dos equipos en los que se deben instalar parches. Uno de ellos está en línea y el otro fuera de línea. El parche se ha

© Acronis International GmbH, 2003-2025

Opción	Descripción
	instalado en el primer equipo. Cuando pasen siete días, el parche se eliminará, aunque no esté instalado en el segundo equipo porque estaba fuera de línea.
30 días	El parche se eliminará de la lista treinta días después de su primera instalación.

Aprobación automática de parches

Con la aprobación automática de parches, el proceso de instalación de actualizaciones en los equipos le resultará más sencillo. Esta función evita que la instalación de parches se retrase debido al proceso manual de aprobación de parches. Las actualizaciones y correcciones importantes se instalan con mayor rapidez, lo que aumenta la fiabilidad del sistema.

Puede usar la aprobación automática de parches en situaciones de prueba para instalar los parches automáticamente. Si los parches se instalan correctamente en los equipos de prueba, también lo harán automáticamente en los equipos de producción. Para obtener más información sobre esta situación, consulte "Caso de uso de prueba y aprobación automática de parches" (p. 1402).

También puede usar la aprobación automática de parches para instalar los parches automáticamente en el entorno de producción y saltarse la fase de prueba. Para obtener más información sobre esta situación, consulte "Caso de uso de aprobación automática de parches sin prueba" (p. 1405).

Importante
La función de gestión de parches admite las actualizaciones a Windows 11. Sin embargo, debe verificar que las cargas de trabajo de Windows 10 que planea actualizar estén debidamente preparadas para ello. Consulte este artículo de Microsoft para obtener más información.

Configuración de la aprobación automática de parches

Puede configurar la aprobación automática de parches para evitar que la instalación de parches se retrase debido al proceso manual de aprobación de parches.

Pasos para configurar la aprobación automática de parches

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Haga clic en **Configuración**.
3. Habilite la **Aprobación automática de parches**.
4. Establezca los ajustes de la aprobación automática de parches.

© Acronis International GmbH, 2003-2025

a. Seleccione la opción de aprobación automática de parches.

Opción	Descripción
Prueba y aprobación automática de parches	El estado de aprobación del parche cambiará a **Aprobado** cuando transcurra el número especificado de días desde la instalación correcta del parche. Le recomendamos que utilice esta configuración si quiere instalar primero los parches en un equipo de prueba para asegurarse de que todo funciona correctamente y, a continuación, instalarlos en su entorno de producción.
Aprobación automática de parches sin prueba	El estado de aprobación del parche cambiará a **Aprobado** cuando transcurra el número especificado de días desde que se encontró el parche.

b. Seleccione el número de días que deben transcurrir desde que se cumpla la condición de la opción de aprobación automática de parches. Después de este periodo, el estado de aprobación de los parches cambiará automáticamente de **Aprobación pendiente** a **Aprobado**.

5. Seleccione **Aceptar automáticamente los acuerdos de licencia**.
6. Haga clic en **Aplicar**.

Caso de uso de prueba y aprobación automática de parches

Si quiere probar los nuevos parches en un equipo de prueba antes de instalarlos en sus equipos de producción, puede configurar dos planes de protección, uno para la instalación de parches de prueba y otro para la instalación de parches ya probados en equipos de producción. De ese modo, se asegurará de que los parches que instale en el entorno de producción sean seguros y de que los equipos de producción funcionen correctamente después de la instalación del parche.

El caso de uso consiste en los pasos siguientes:

1. Establezca los ajustes de la aprobación automática de parches. Seleccione la opción **Prueba y aprobación automática de parches**. Para obtener más información, consulte "Configuración de la aprobación automática de parches" (p. 1401).
2. Configure un plan de protección para pruebas (por ejemplo, "Instalación de parches en entornos de prueba") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de prueba. Especifique la siguiente condición con respecto a la instalación de parches: el estado de aprobación del parche debe ser **Aprobación pendiente**. Este paso es necesario para validar los parches y comprobar si los equipos funcionan correctamente después de su instalación. Para obtener más información, consulte "Configurar el plan de protección Instalación de parches en entornos de prueba" (p. 1403).
3. Configure un plan de protección para el entorno de producción (por ejemplo, "Instalación de parches en entornos de producción") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de producción. Especifique la siguiente condición con respecto a la instalación de parches: el estado del parche debe ser **Aprobado**. Para obtener más información,

© Acronis International GmbH, 2003-2025

consulte "Configurar el plan de protección Instalación de parches en entornos de producción" (p. 1404).

4. Ejecute el plan Instalación de parches en entornos de prueba y compruebe los resultados. Deje el estado de aprobación de los equipos que no tienen ningún problema como **Aprobación pendiente** y cambie el de aquellos que no funcionan correctamente a **Rechazado**. Una vez transcurrido el número de días establecido en **Aprobación automática de parches**, el estado de aprobación de los parches cambiará automáticamente de **Aprobación pendiente** a **Aprobado**. Cuando ejecute el plan Instalación de parches en entornos de producción, solo se instalarán los parches con el estado **Aprobado** en los equipos de producción. Para obtener más información, consulte "Ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros" (p. 1405).
5. Ejecute el plan Instalación de parches en entornos de producción.

Configurar el plan de protección Instalación de parches en entornos de prueba

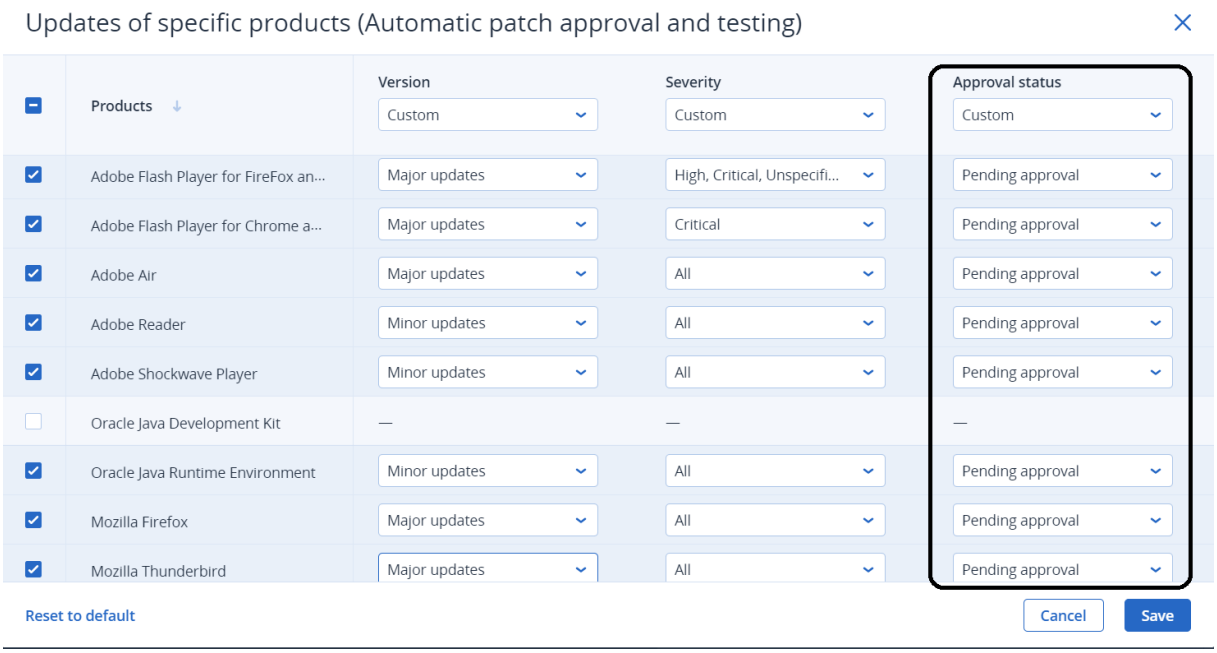
Puede configurar un plan de protección con ajustes de instalación de parches para sus equipos en el entorno de prueba.

Pasos para configurar el plan de protección Instalación de parches en entornos de prueba

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Haga clic en **Crear plan**.
3. Habilite el módulo **Gestión de parches**.
4. Defina qué actualizaciones desea instalar para productos de Microsoft y terceros, establezca una planificación y realice una copia de seguridad previa a la actualización. Para obtener más información sobre esta configuración, consulte "Configuración de gestión de parches en el plan de protección" (p. 1391).

Importante
Seleccione el estado de aprobación **Aprobación pendiente** para todos aquellos productos que se vayan a actualizar. De ese modo, el agente instalará únicamente los parches cuyo estado sea **Aprobación pendiente** en los equipos seleccionados del entorno de prueba.

© Acronis International GmbH, 2003-2025



Configurar el plan de protección Instalación de parches en entornos de producción

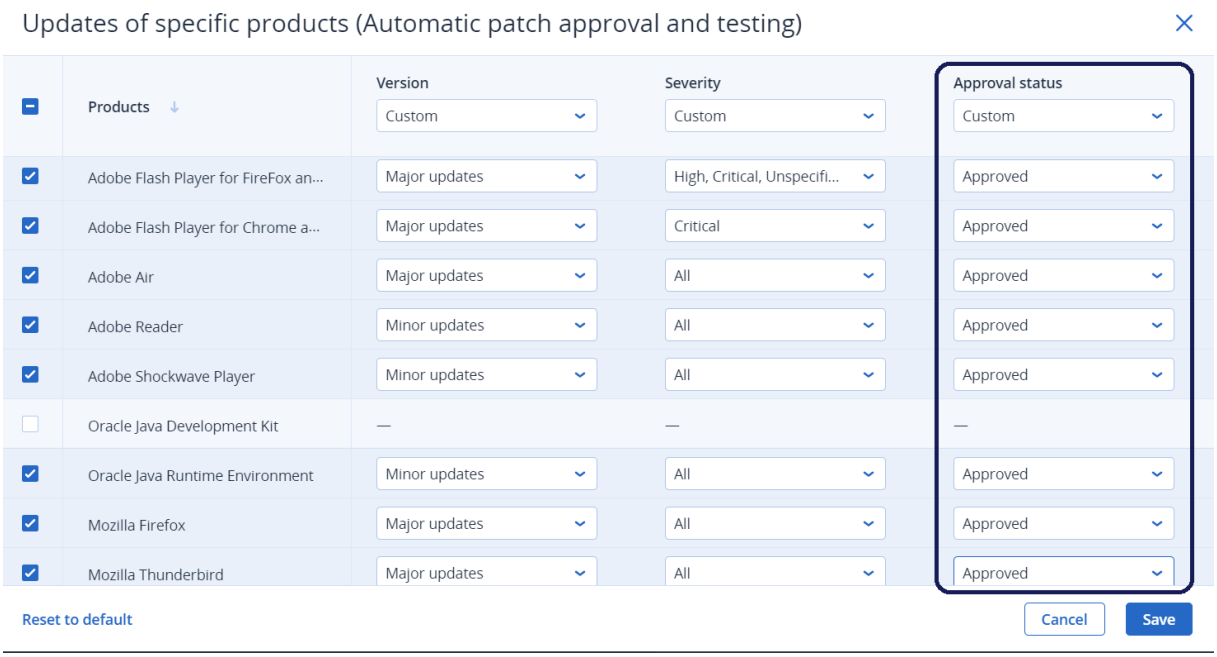
Puede configurar un plan de protección con ajustes de instalación de parches para sus equipos en el entorno de producción.

Pasos para configurar el plan de protección Instalación de parches en entornos de producción

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de protección**.
2. Haga clic en **Crear plan**.
3. Habilite el módulo **Gestión de parches**.
4. Defina qué actualizaciones desea instalar para productos de Microsoft y terceros, establezca una planificación y realice una copia de seguridad previa a la actualización. Para obtener más información sobre esta configuración, consulte "Configuración de gestión de parches en el plan de protección" (p. 1391).

Importante
Defina la opción **Estado de aprobación** como **Aprobado** para todos aquellos productos que se vayan a actualizar. De ese modo, el agente instalará únicamente los parches cuyo estado sea **Aprobado** en los equipos seleccionados del entorno de producción.

© Acronis International GmbH, 2003-2025



Ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros

Una vez que se hayan instalado los parches en los equipos del entorno de prueba, puede comprobar si todo funciona correctamente. Puede dejar el estado de aprobación de los equipos que no tienen ningún problema como **Aprobación pendiente** y cambiar el de aquellos que no funcionan correctamente a **Rechazado**.

Pasos para ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros

1. Ejecute el plan de protección Instalación de parches en entornos de prueba (según la planificación o manualmente).
2. Según el resultado, podrá ver cuáles de los parches instalados son seguros.
3. Vaya a **Gestión del software** > **Parches** y establezca el **Estado de aprobación** como **Rechazado** para aquellos parches que no sean seguros.

Caso de uso de aprobación automática de parches sin prueba

Si quiere instalar automáticamente los nuevos parches en los equipos de producción lo antes posible, sin instalarlos primero en los equipos de prueba, puede configurar solo un plan de protección.

El caso de uso consiste en los pasos siguientes:

1. Establezca los ajustes de la aprobación automática de parches. Selecciona la opción **Aprobación automática de parches sin prueba**. Para obtener más información, consulte "Configuración de la aprobación automática de parches" (p. 1401).

© Acronis International GmbH, 2003-2025

2. Configure un plan de protección para el entorno de producción (por ejemplo, "Instalación de parches en entornos de producción") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de producción. Especifique la siguiente condición con respecto a la instalación de parches: el estado del parche debe ser **Aprobado**. Para obtener más información, consulte "Configurar el plan de protección Instalación de parches en entornos de producción" (p. 1404).
3. Ejecute el plan Instalación de parches en entornos de producción.

Aprobar parches manualmente

Puede aprobar un parche manualmente para acelerar su instalación al omitir la fase de prueba.

Requisitos previos

- Debe aplicarse un plan de protección con el módulo **Gestión de parches** habilitado a al menos un equipo de Windows.
- Debe haber parches aún sin instalar en el equipo o los equipos en los que se ha aplicado el plan de protección.

Pasos para probar parches manualmente

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Seleccione los parches que quiera instalar y acepte los acuerdos de licencia.
3. Establezca el **Estado de aprobación** de los parches en **Aprobado**.
   El estado de aprobación de los parches se establecerá en **Aprobado**. Los parches se instalarán automáticamente en los equipos según la planificación definida en el plan de protección. Si quiere instalar los parches de forma inmediata, siga el procedimiento que se describe en "Instalar parches bajo demanda" (p. 1406).

Instalar parches bajo demanda

Puede instalar parches bajo demanda manualmente si no quiere esperar a que llegue la hora de instalación planificada.

Puede iniciar la instalación manual del parche desde tres pantallas: **Parches**, **Vulnerabilidades** y **Todos los dispositivos**.

Importante
La función de gestión de parches admite las actualizaciones a Windows 11. Sin embargo, debe verificar que las cargas de trabajo de Windows 10 que planea actualizar estén debidamente preparadas para ello. Consulte este artículo de Microsoft para obtener más información.

Pasos para instalar un parche manualmente

Desde Parches

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Acepte los acuerdos de licencia para los parches que quiera instalar.
3. En el asistente **Instalar parches**, seleccione los parches que quiera instalar y haga clic en **Instalar**.
4. Seleccione los equipos en los cuales desea instalar los parches.
5. Seleccione las opciones de reinicio.

   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos.

© Acronis International GmbH, 2003-2025

Opción	Descripción
	Nota El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

6. Haga clic en **Instalar parches**.

Desde Vulnerabilidades

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Lleva a cabo el proceso de solución tal y como se describe en "Gestión de vulnerabilidades encontradas" (p. 1387).

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo en el que desea instalar los parches.
3. Haga clic en **Parche**.
4. Seleccione los parches que quiera instalar y haga clic en **Siguiente**.
5. Seleccione las opciones de reinicio.

   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de

© Acronis International GmbH, 2003-2025

Opción	Descripción
	verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**.

© Acronis International GmbH, 2003-2025

Opción	Descripción
iniciado sesión en el dispositivo, reinícielo inmediatamente	Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

6. Haga clic en **Instalar parches**.

Trabajar con repositorios de software y paquetes de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Con el despliegue de software mediante DeployPilot, puede:

- Realizar instalaciones de software en dispositivos remotos.
- Actualizar las aplicaciones personalizadas que no son compatibles con la función de evaluación de vulnerabilidades y gestión de parches. Para que esta función sea compatible, el instalador cargado debe estar preconfigurado para admitir actualizaciones.

Paquetes de software

Los paquetes de software son archivos de instalación (.msi o .exe) que puede utilizar para desplegar (instalar o desinstalar) software en recursos informáticos de Windows de forma remota. Para comprobar las versiones de Windows compatibles, consulte "Versiones de Windows compatibles" (p. 1411).

Un paquete de software se define por la versión del software y algunas configuraciones personalizadas, como el idioma y el tipo de arquitectura.

Repositorios de software

Los repositorios de software son depósitos donde se almacenan los paquetes de software.

Hay dos repositorios de software: **Biblioteca** y **Mis paquetes**.

Biblioteca

El repositorio de la **Biblioteca** contiene 40 de las aplicaciones de software más utilizadas. El contenido de este repositorio está predefinido y es mantenido por el sistema. Puede ver la lista completa de estas aplicaciones en este artículo de la base de conocimientos.

© Acronis International GmbH, 2003-2025

No puede editar ni eliminar paquetes de este repositorio. Además, no puede desplegar un paquete directamente desde aquí. Para desplegar un paquete, primero debe agregarlo al repositorio **Mis paquetes**.

Mis paquetes

El repositorio **Mis paquetes** contiene todos los paquetes de software que puede desplegar e incluir en los planes de despliegue de software. Inicialmente, este repositorio está vacío, incluso si hay paquetes en el repositorio **Biblioteca**. Puede agregar paquetes a **Mis paquetes** de las siguientes formas:

- Agregando un paquete desde el repositorio **Biblioteca**. Consulte "Cómo agregar paquetes de software desde la biblioteca" (p. 1414) para obtener más información.
- Cargando manualmente un paquete de software. Consulte "Cargando paquetes de software" (p. 1415) para obtener más información.

Después de agregar un paquete a **Mis paquetes**, puede desplegarlo mediante una acción de despliegue rápido o incluyéndolo en un plan de despliegue de software. Consulte "Instalación de software" (p. 1420), "Desinstalación de software" (p. 1423) y "Crear un plan de despliegue de software" (p. 1427) para obtener más información.

Nota
DeployPilot distingue entre los paquetes que se agregaron desde el repositorio de la **Biblioteca** y los paquetes cargados manualmente. Para los paquetes que se agregaron desde el repositorio de la **Biblioteca**, DeployPilot comprueba antes del despliegue si el software ya está instalado en el dispositivo y, si es así, evita la reinstalación innecesaria.

La capacidad máxima de almacenamiento del repositorio **Mis paquetes** es de 5 GB para inquilinos-clientes y de 20 GB para inquilinos de partner.

Versiones de Windows compatibles

El despliegue de software mediante DeployPilot es compatible con equipos que tienen los siguientes sistemas operativos:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 (Enterprise, Professional y Ultimate)
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

© Acronis International GmbH, 2003-2025

- Windows Server 2012
- Windows Server 2008 R2

Búsqueda en los repositorios de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede buscar un paquete de software específico en los repositorios de software y ver detalles sobre este paquete.

Requisitos previos

Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa, administrador de cibernética o administrador de solo lectura.

Pasos para buscar un paquete de software

En la biblioteca

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Biblioteca**.
   En la pantalla **Biblioteca**, puede ver una lista con 40 de las aplicaciones de software más utilizadas y la siguiente información para cada aplicación:

Campo	Descripción
Nombre	Nombre del software
Versión más reciente	La versión más reciente de la aplicación que está disponible en el repositorio.
Proveedor	Nombre del proveedor de software.
Tipo de licencia	Tipo de licencia: propietaria o de código abierto.

2. [Opcional] Para buscar un paquete de software por nombre, haga clic en **Buscar** e introduzca el nombre.
   La lista de paquetes se filtra dinámicamente según el texto que introduzca en el campo.
3. [Opcional] Para filtrar la lista de paquetes, haga clic en **Filtro**, especifique los valores y, a continuación, haga clic en **Aplicar**.
   La siguiente tabla proporciona más detalles acerca de los filtros que están disponibles en esta página.

Filtro	Descripción
Proveedor	Use este filtro si conoce el nombre del proveedor de software y desea ver solo el software de este proveedor.
Tipo de licencia	Use este filtro si desea clasificar los resultados según el tipo de

© Acronis International GmbH, 2003-2025

Filtro	Descripción
	licencia: propietaria o de código abierto.
Período de lanzamiento más reciente	Use este filtro si desea clasificar los resultados y ver solo los paquetes de software que se lanzaron durante un período especificado.

4. Para ver todos los detalles de un paquete, haga clic en la fila correspondiente de la lista.

En Mis paquetes

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Mis paquetes**.
   En la pantalla **Mis paquetes**, se muestran los paquetes que puede desplegar en sus recursos informáticos gestionados y la siguiente información para cada paquete:

Campo	Descripción
Nombre	Nombre del software
Versión	Versión del software.
Proveedor	Nombre del proveedor de software.
Comprobación de firma digital	Estado de la comprobación de la firma digital.
Sistema operativo	Sistema operativo en el que se puede desplegar el paquete.
Última edición realizada por	Nombre de usuario del usuario que editó el paquete por última vez.
Tipo de sistema	Tipo de arquitectura del sistema operativo en el que se desplegará el paquete de software.
Tamaño del paquete	Tamaño del paquete de software.

2. [Opcional] Para buscar un paquete de software por nombre, haga clic en **Buscar** e introduzca el nombre.
   La lista de paquetes se filtra dinámicamente según el texto que introduzca en el campo.
3. [Opcional] Para filtrar la lista de paquetes, haga clic en **Filtro**, especifique los valores y, a continuación, haga clic en **Aplicar**.
   La siguiente tabla proporciona más detalles acerca de los filtros que están disponibles en esta página.

Filtro	Descripción
Proveedor	Use este filtro si conoce el nombre del proveedor de software y desea ver solo el software de este proveedor.
Última edición	Use este filtro si desea filtrar los resultados y ver solo los paquetes que

© Acronis International GmbH, 2003-2025

Filtro	Descripción
realizada por	fueron editados por un usuario determinado.
Tipo de sistema	Use este filtro si desea clasificar los resultados según el tipo de arquitectura del sistema.
Idioma	Use este filtro si desea clasificar los resultados según el idioma del software.
Período de lanzamiento	Use este filtro si desea clasificar los resultados y ver solo los paquetes de software que se lanzaron durante un período especificado.

4. Para ver todos los detalles de un paquete, haga clic en la fila correspondiente de la lista.

Cómo agregar paquetes de software desde la biblioteca

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

El repositorio **Biblioteca** contiene 40 de las aplicaciones de software más utilizadas. Para poder desplegar un paquete desde la biblioteca, primero debe agregarlo a sus paquetes.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para añadir un paquete de la biblioteca a mis paquetes

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Biblioteca**.
2. En la fila del paquete de software que desea agregar a sus paquetes, haga clic en **Agregar**.
3. En el asistente **Agregar a mis paquetes**, seleccione la configuración del software.

Configuración	Descripción
Versión	Versión del software.
Idioma	Idioma del software.
Tipo de arquitectura	Tipo de arquitectura del sistema operativo en el que se desplegará el paquete de software.

4. Seleccione **Acepto los términos y condiciones de la EULA** y haga clic en **Agregar**.
   El paquete se agrega a sus paquetes. Puede verlo en la página **Mis paquetes**.

© Acronis International GmbH, 2003-2025

Cargando paquetes de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

En la página **Mis paquetes**, puede cargar paquetes de software en los siguientes formatos: .msi o .exe.

Importante
Si planea utilizar el paquete para actualizar instalaciones existentes, asegúrese de que el paquete que va a cargar sea compatible con las actualizaciones.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para cargar un paquete de software

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Mis paquetes**.
2. Haga clic en **Agregar paquete**.
3. En la pestaña **Cargar paquete**, haga lo siguiente:
   a. Haga clic en **Cargar**, seleccione el paquete de software que desea cargar y, a continuación, haga clic en **Abrir**.
   b. Dependiendo de si desea utilizar Copilot para rellenar automáticamente los detalles del paquete y la información requerida, como el comando y los argumentos de instalación y desinstalación, marque o desmarque el interruptor **Probar Copilot**.
   c. Haga clic en **Siguiente**.
4. En la pestaña **Detalles del paquete**, haga lo siguiente:
   - Si utilizó Copilot para rellenar automáticamente los detalles del paquete, revíselos y asegúrese de que son correctos y, a continuación, haga clic en **Siguiente**.

     Nota
     Puede corregir manualmente los detalles del paquete que fueron completados por Copilot o hacer clic en **Revertir cambios** para eliminar todos los detalles del paquete.

   - Si no utilizó Copilot para rellenar automáticamente los detalles del paquete, introduzca los detalles y, a continuación, haga clic en **Siguiente**.

Campo	Descripción
Nombre del	Nombre del software. Este campo es obligatorio.

© Acronis International GmbH, 2003-2025

Campo	Descripción
software	
Proveedor/editor	Nombre del proveedor de software. Este campo es obligatorio.
Descripción del software	Descripción adicional del software. Este campo es opcional.
Tipo de licencia	Tipo de licencia del software. • **Propiedad**. Las licencias en propiedad están controladas y son propiedad de los proveedores de software. Este es el valor predeterminado. • **Código abierto**. Estas son las licencias para el software de código abierto que son gratuitas para la distribución pública.
Versión	Versión del software. Este campo es obligatorio.
Tipo de arquitectura	Tipo de arquitectura del sistema operativo en el que se desplegará el paquete de software. Este campo es obligatorio.
Idioma	Idioma del software. Este campo es opcional.
Fecha de publicación	Fecha de lanzamiento del software. Este campo es obligatorio.

5. En la pestaña **Comandos de Instalación / Desinstalación**, realice lo siguiente:
   - Si utilizó Copilot para rellenar automáticamente los comandos y argumentos de instalación y desinstalación, revise los detalles, asegúrese de que son correctos y, a continuación, haga clic en **Siguiente**.
   - Si no utilizó Copilot para completar automáticamente la información del paquete, haga lo siguiente:
     a. [Opcional] En la sección **Opciones de instalación**, en el campo **Argumentos de comando**, introduzca los argumentos del comando de instalación.
     b. [Opcional] En los campos **Códigos de retorno de reinicio** y **Códigos de retorno correctos**, especifique los códigos de retorno que indican el resultado del proceso de instalación.
     c. En la sección **Opciones de desinstalación**, seleccione el método de desinstalación:

Método de desinstalación	Descripción
Línea de comando	Si selecciona este método, debe proporcionar el comando y los argumentos de desinstalación silenciosa correctos. De lo contrario, la desinstalación podría dejar de responder.
Nombre del software o del	Si selecciona este método, el sistema utilizará el nombre del software, el nombre del proveedor o el modelo de RegEx que

© Acronis International GmbH, 2003-2025

Método de desinstalación	Descripción
proveedor	proporcione para ubicar y ejecutar automáticamente el comando de desinstalación. Utilice este método si no está seguro del comando de desinstalación para la aplicación.

d. [Si ha seleccionado **Nombre del software o del proveedor**] En el campo **Nombre del software**, introduzca el nombre del software.

e. [Si ha seleccionado **Nombre del software o del proveedor**] En el campo **Nombre del proveedor**, introduzca el nombre del proveedor del software.

f. [Si ha seleccionado **Línea de comando**] En el campo **Ruta de desinstalación**, introduzca la ruta de desinstalación y el comando.

La ruta de desinstalación es la ruta al directorio de un ordenador donde se encuentra el ejecutable de desinstalación del programa de software. La ruta de desinstalación es esencial para asegurar que el software se puede eliminar de forma limpia y completa del sistema.

g. En el campo **Argumentos de comando**, introduzca los argumentos del comando de desinstalación.

h. [Opcional] En los **Códigos de retorno de reinicio**, introduzca los códigos de retorno.

i. [Opcional] En los campos de **Códigos de retorno correctos**, introduzca los códigos de retorno.

j. Haga clic en **Siguiente**.

Para obtener más información sobre los comandos y argumentos de instalación y desinstalación, consulte "Comandos y argumentos de instalación y desinstalación" (p. 1418).

6. En la pestaña **Resumen**, revise los detalles del paquete de software, seleccione **He revisado los detalles del paquete y confirmo que quiero agregarlo a Mis paquetes** y **Acepto los términos y condiciones del EULA**, y luego haga clic en **Siguiente**.
7. En la pestaña **Comprobación de firma digital**:
   - Si desea realizar una comprobación de firma digital del paquete, seleccione **Habilitar comprobación de firma digital**.

     Nota
     Le recomendamos que siempre realice una comprobación de la firma digital. Esto garantiza que el paquete personalizado que se cargará es compatible y está firmado digitalmente, y minimiza el riesgo de desplegar software no verificado o manipulado.

   - Si desea omitir la comprobación, desactive **Habilitar comprobación de firma digital**.
8. Haga clic en **Agregar paquete**.

© Acronis International GmbH, 2003-2025

Comandos y argumentos de instalación y desinstalación

Al proporcionar argumentos de instalación y desinstalación durante la carga manual de paquetes de software, puede garantizar un despliegue de software eficaz y sin problemas en toda su organización.

Nota
Puede utilizar Copilot para rellenar automáticamente los argumentos de instalación y desinstalación.

Comandos de instalación

Argumentos del comando

Los argumentos de línea de comandos son parámetros o etiquetas que puede especificar para el proceso de instalación. Entre los ejemplos más comunes se incluyen:

- Instalación silenciosa (instala el software sin mostrar ninguna interfaz de usuario):
  `/s` o `/quiet`
- Sin reinicio (evita que el sistema se reinicie automáticamente después de que se complete el proceso de instalación):
  `/norestart`
- Archivo de registro (crea un archivo de registro para realizar un seguimiento del proceso de instalación):
  `/l* log.txt`

Comandos de desinstalación

Ruta de desinstalación

La ruta de desinstalación proporciona la ruta de archivo y el comando necesarios para desinstalar el software. Por ejemplo:

```
%ProgramFiles%\7-Zip\Uninstall.exe
```

Argumentos del comando

Los argumentos de línea de comandos son parámetros o etiquetas que puede especificar para el proceso de desinstalación. Entre los ejemplos más comunes se incluyen:

- Desinstalación silenciosa (desinstala el software sin mostrar ninguna interfaz de usuario):
  `/s` o `/quiet`
- Sin reinicio (evita que el sistema se reinicie automáticamente después de que se complete el proceso de desinstalación):
  `/norestart`

© Acronis International GmbH, 2003-2025

- Archivo de registro (crea un archivo de registro para realizar un seguimiento del proceso de desinstalación):

  ```
  /l* log.txt
  ```

Edición de paquetes de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Solo puede editar los paquetes de software que haya cargado manualmente.

Requisitos previos

Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para editar un paquete de software

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Mis paquetes**.
2. Haga clic en el icono **...** para el paquete que desea editar, y después haga clic en **Editar**.
3. En el asistente **Editar paquete**, edite la configuración y haga clic en **Guardar**.

Eliminación de paquetes de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede eliminar los paquetes de software que ya no necesite.

Requisitos previos

Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para eliminar un paquete de software

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Mis paquetes**.
2. Para el paquete que desea editar, haga clic en el icono **...** y después en **Eliminar**.
3. Haga clic en **Eliminar** en la ventana de confirmación.

Si el paquete se cargó manualmente, se eliminará de forma permanente. Si el paquete se agregó desde la biblioteca, solo se eliminará de sus paquetes.

© Acronis International GmbH, 2003-2025

Instalación de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede instalar software de forma remota en sus recursos informáticos gestionados sin crear un plan de despliegue de software. Esta acción es compatible con hasta 15 paquetes de software y hasta 150 recursos informáticos de destino a la vez.

Requisitos previos

Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para instalar un paquete de software

Desde Mis paquetes

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Mis paquetes**.
2. Seleccione el software que quiera instalar y haga clic en **Instalar**.
3. En la ventana **Desplegar software**, haga clic en **Agregar recursos informáticos**.
4. Seleccione el recurso informático en el que desee instalar el paquete y, a continuación, haga clic en **Agregar**.
5. Para configurar las opciones de reinicio, haga lo siguiente:
   a. Haga clic en el campo **Opciones de reinicio**.
   b. En la pantalla **Opciones de reinicio**, configure si el sistema reiniciará los recursos informáticos después de la instalación de la instalación de software.
   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

c. Haga clic en **Listo**.

6. Haga clic en **Instalar ahora**.

© Acronis International GmbH, 2003-2025

Nota
Los paquetes que no superen la comprobación de la firma digital no se desplegarán.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en un recurso informático y, a continuación, en **Desplegar software**.
3. En la ventana **Desplegar software**, en el campo **Acción**, seleccione **Instalar**.
4. Haga clic en **Seleccionar software**, seleccione el software que desea instalar y, a continuación, haga clic en **Listo**.
5. Para configurar las opciones de reinicio, haga lo siguiente:
   a. Haga clic en el campo **Opciones de reinicio**.
   b. En la pantalla **Opciones de reinicio**, configure si el sistema reiniciará los recursos informáticos después de la instalación de la instalación de software.
   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde

© Acronis International GmbH, 2003-2025

Opción	Descripción
	repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

c. Haga clic en **Listo**.

6. Haga clic en **Desplegar ahora**.

Desinstalación de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede desinstalar el software de forma remota desde sus recursos informáticos gestionados sin crear un plan de despliegue de software.

Requisitos previos

Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

© Acronis International GmbH, 2003-2025

Pasos para desinstalar un paquete de software

Desde Mis paquetes

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Mis paquetes**.
2. Haga click en el paquete que quiera instalar y, a continuación, haga click en **Desinstalar**.
3. En la ventana **Desplegar software**, haga clic en **Agregar recursos informáticos**.
4. Seleccione uno o varios recursos informáticos en los que desee instalar el paquete y, a continuación, haga clic en **Agregar**.
5. Para configurar las opciones de reinicio, haga lo siguiente:
   a. Haga clic en el campo **Opciones de reinicio**.
   b. En la pantalla **Opciones de reinicio**, configure si el sistema reiniciará los recursos informáticos después de la desinstalación del software.
   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período

© Acronis International GmbH, 2003-2025

Opción	Descripción
	seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

c. Haga clic en **Listo**.

6. Haga clic en **Desinstalar ahora**.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en un recurso informático y, a continuación, en **Desplegar software**.
3. En la ventana **Desplegar software**, en el campo **Acción**, seleccione **Desinstalar**.
4. Haga clic en **Seleccionar software**, seleccione el software que desea desinstalar y, a continuación, haga clic en **Listo**.
5. Para configurar las opciones de reinicio, haga lo siguiente:
   a. Haga clic en el campo **Opciones de reinicio**.
   b. En la pantalla **Opciones de reinicio**, configure si el sistema reiniciará los recursos informáticos después de la desinstalación del software.
   La siguiente tabla proporciona más información sobre las opciones de reinicio.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático.

© Acronis International GmbH, 2003-2025

Opción	Descripción
	• 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

c. Haga clic en **Listo**.

6. Haga clic en **Desplegar ahora**.

Planes de implementación de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Con los planes de despliegue de software, puede automatizar el proceso de despliegue de software y garantizar que la distribución de software en sus recursos informáticos gestionados sea coherente. La funcionalidad incluye las siguientes funciones:

- Instalación o desinstalación remota de software.
- Planificaciones para la instalación o desinstalación automática de software.
- Acciones después de la instalación.

Crear un plan de despliegue de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede crear un plan de despliegue de software y, a continuación, asignarlo a uno o varios recursos informáticos. De este modo, se asegura de que distribuye e instala software aprobado en sus recursos informáticos gestionados y, al mismo tiempo, desinstala software que está obsoleto o que no está aprobado por su organización.

Cuando Active Protection está habilitada en el plan de protección que se aplica a los recursos informáticos, el despliegue de software está protegido por el motor antimalware. Antes de instalar un paquete en los recursos informáticos, el sistema ejecutará automáticamente un análisis antimalware. Esta capa de defensa proactiva protege contra inyecciones malintencionadas,

© Acronis International GmbH, 2003-2025

garantizando que el despliegue de software no introducirá vulnerabilidades en los sistemas. Esto es especialmente valioso en entornos donde la seguridad es crítica, y reduce el riesgo de tiempo de inactividad y de costosas respuestas ante incidentes.

Nota
Un plan de despliegue de software único solo admite una de las acciones de despliegue: instalar o desinstalar. Esto significa que debe crear planes separados: uno para la instalación de software y otro para su desinstalación.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para crear un plan de despliegue de software

Planes de despliegue de software

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de despliegue de software**.
2. Cree un plan mediante una de estas dos opciones:
   - Si no hay planes de despliegue de software en la lista, haga clic en **Crear**.
   - Si hay planes de despliegue de software en la lista, haga clic en **Crear plan**.
3. [Opcional] Pasos para añadir cargas de trabajo al plan:
   a. Haga clic en **Añadir cargas de trabajo**.
   b. Seleccione las cargas de trabajo y haga clic en **Agregar**.
4. Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Continuar**.
5. En el campo **Acción**, seleccione si el plan instalará o desinstalará el software.
6. En el campo **Software**, haga clic en **Seleccionar software**, seleccione una o varias aplicaciones de la lista y haga clic en **Listo**.
7. Para configurar las opciones de reinicio, haga lo siguiente:
   a. Haga clic en el campo **Opciones de reinicio**.
   b. En la pantalla **Opciones de reinicio**, configure si el sistema reiniciará los recursos informáticos después de la instalación o desinstalación del software.
   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de

© Acronis International GmbH, 2003-2025

Opción	Descripción
	instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

c. Haga clic en **Listo**.

8. Para crear una planificación para la ejecución del plan, haga lo siguiente:
   a. Haga clic en el campo **Planificación**.
   b. En la pantalla **Planificación**, en el campo **Planificar la ejecución de la tarea utilizando los siguientes eventos**, seleccione el evento que iniciará el plan.

Opción	Descripción
Ejecutar una vez	Si selecciona esta opción, debe configurar la fecha y la hora en las que se ejecutará el plan.
Planificar por hora	Si selecciona esta opción, puede configurar planes que se ejecutarán cada hora, día o mes. Si desea que esta planificación sea efectiva solo durante un período de tiempo específico, seleccione la casilla de verificación **Ejecutar dentro de un rango de fechas** y, a continuación, configure el período (en días) durante el cual se ejecutará el plan programado.
Cuando el usuario inicia sesión en el sistema	Si selecciona esta opción, el plan se ejecutará cuando un usuario específico o cualquier usuario inicie sesión en el recurso informático de destino.
Cuando el usuario cierra sesión en el sistema	Si selecciona esta opción, el plan se ejecutará cuando un usuario específico o cualquier usuario cierre la sesión del recurso informático de destino.
Al iniciarse el sistema	Si selecciona esta opción, el plan se ejecutará cuando se inicie el recurso informático de destino.
Cuando el sistema está apagado	Si selecciona esta opción, el plan se ejecutará cuando se apague el recurso informático de destino.
Cuando el	Si selecciona esta opción, el plan se ejecutará cuando el recurso

© Acronis International GmbH, 2003-2025

Opción	Descripción
sistema está en línea	informático de destino se ponga en línea.

c. En la sección **Condiciones de inicio**, seleccione todas las condiciones que deben cumplirse de forma simultánea para iniciar el plan.

Condición	Descripción
Ejecutar solo si la carga de trabajo está en línea	Esta condición se cumple cuando la carga de trabajo de destino se conecta a Internet.
El usuario está inactivo	Esta condición se cumple cuando se está ejecutando el protector de pantalla en el equipo o el equipo está bloqueado.
El usuario cerró la sesión	Si selecciona esta condición, puede posponer un plan programado hasta que el usuario de la carga de trabajo de destino cierre sesión.
Coincidir con intervalo	Si selecciona esta condición, debe definir el intervalo de tiempo en el que puede ejecutarse el plan.
Ahorrar batería	Si selecciona esta condición, podrá asegurarse de que el plan no se interrumpirá porque la batería sea baja. Las siguientes opciones están disponibles: • **No iniciar con alimentación por batería** El plan se iniciará únicamente si el equipo está conectado a una fuente de alimentación. • **Iniciar con alimentación por batería si su nivel es superior a** El plan se iniciará si el equipo está conectado a una fuente de alimentación o si el nivel de la batería es superior al valor especificado.
No iniciar con conexiones de uso medido	Si selecciona esta condición, el plan no se ejecutará si la carga de trabajo de destino accede a Internet a través de una conexión de uso medido.
No iniciar con conexiones a las siguientes redes Wi-Fi	Si selecciona esta condición, el plan no se ejecutará si la carga de trabajo de destino está conectada a cualquiera de las redes inalámbricas especificadas. Para utilizar esta condición, debe especificar el SSID de la red prohibida. La restricción se aplica a todas las redes de contengan el nombre especificado como una subcadena en su nombre, sin distinción de mayúsculas y minúsculas. Por ejemplo, si especifica `teléfono` como nombre de red, el plan no se iniciará cuando el dispositivo esté conectado a alguna de las siguientes redes: `Teléfono de Juan`, `wifi_teléfono` o `wifi_de_mi_teléfono`.

© Acronis International GmbH, 2003-2025

Condición	Descripción
Comprobar dirección IP del dispositivo	Si selecciona esta condición, el plan no se ejecutará si alguna de las direcciones IP de la carga de trabajo de destino está dentro o fuera del rango de direcciones IP especificado. Las siguientes opciones están disponibles: • **Iniciar si queda fuera del intervalo IP** • **Iniciar si queda dentro del intervalo IP** Solo se admiten direcciones IPv4.
Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos	Utilice esta opción para establecer el intervalo de tiempo tras el cual se ejecutará el plan, independientemente del resto de condiciones. El plan comenzará cuando se cumplan el resto de las condiciones o cuando termine este periodo, lo que suceda primero. Esta opción no está disponible si ha seleccionado la opción **Ejecutar una vez** para la programación.

d. Haga clic en **Listo**.

9. Haga clic en **Crear**.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en el recurso informático al que desee aplicar un plan de despliegue de software.
3. Haga clic en **Proteger** y, a continuación, en **Agregar plan**.
4. Haga clic en **Crear plan** y seleccione **Despliegue del software**.
5. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Continuar**.
6. En el campo **Acción**, seleccione si el plan instalará o desinstalará el software.
7. En el campo **Software**, haga clic en **Seleccionar software**, seleccione una o varias aplicaciones de la lista y haga clic en **Listo**.
8. Para configurar las opciones de reinicio, haga lo siguiente:
   a. Haga clic en el campo **Opciones de reinicio**.
   b. En la pantalla **Opciones de reinicio**, configure si el sistema reiniciará los recursos informáticos después de la instalación o desinstalación del software.
   La siguiente tabla proporciona más información sobre las opciones de reinicio.

Opción	Descripción
Reiniciar si es necesario	Si desea que la carga de trabajo se reinicie después de que el software se instale o desinstale, solo si el software lo requiere, marque esta casilla de verificación.
Reiniciar siempre	Si desea que la carga de trabajo se reinicie siempre después de

© Acronis International GmbH, 2003-2025

Opción	Descripción
	instalar o desinstalar el software, marque esta casilla de verificación.
No reiniciar	Si no desea que la carga de trabajo se reinicie después de instalar o desinstalar el software, marque esta casilla de verificación.
Planificar reinicio automático	Esta opción está disponible si ha seleccionado **Reiniciar si es necesario** o **Reiniciar siempre**. La opción permite el reinicio automático del recurso informático.
Si un usuario ha iniciado sesión en el dispositivo, este se reiniciará automáticamente después de:	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione el período después del cual el recurso informático se reiniciará automáticamente. Se notificará al usuario que haya iniciado sesión en el recurso informático sobre un reinicio automático pendiente y la hora a la que ocurrirá. De esta manera, los usuarios pueden guardar su trabajo y prepararse para el reinicio.
Notificaciones adicionales	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Seleccione esta opción si desea que se le recuerde repetidamente al usuario que ha iniciado sesión en el recurso informático que debe reiniciar antes de que pase el período seleccionado. El momento de las notificaciones depende del período seleccionado y se convierte en una cuenta regresiva a medida que se acerca la hora de reinicio. Esto garantiza que los usuarios estén informados y preparados para el reinicio. Las notificaciones se activan por una actualización o despliegue de software correcto y se envían en los siguientes momentos. **Nota** El momento de la primera notificación coincide con el período seleccionado. • 24 h antes del reinicio automático. • 8 h antes del reinicio automático. • 4 h antes del reinicio automático. • 1 h antes del reinicio automático. • 30 minutos antes de reiniciar. • 15 minutos antes de reiniciar. • 5 minutos antes del reinicio automático. No se puede cerrar ni descartar la última notificación al usuario.

© Acronis International GmbH, 2003-2025

Opción	Descripción
Si no hay ningún usuario que haya iniciado sesión en el dispositivo, reinícielo inmediatamente	Esta opción está disponible si ha seleccionado **Planificar reinicio automático**. Si selecciona esta opción y ningún usuario ha iniciado sesión en el recurso informático, este se reiniciará inmediatamente, sin esperar a que pase el período seleccionado antes del reinicio automático.

c. Haga clic en **Listo**.

9. Para crear una planificación para la ejecución del plan, haga lo siguiente:
   a. Haga clic en el campo **Planificación**.
   b. En la pantalla **Planificación**, en el campo **Planificar la ejecución de la tarea utilizando los siguientes eventos**, seleccione el evento que iniciará el plan.

Opción	Descripción
Ejecutar una vez	Si selecciona esta opción, debe configurar la fecha y la hora en las que se ejecutará el plan.
Planificar por hora	Si selecciona esta opción, puede configurar planes que se ejecutarán cada hora, día o mes. Si desea que esta planificación sea efectiva solo durante un período de tiempo específico, seleccione la casilla de verificación **Ejecutar dentro de un rango de fechas** y, a continuación, configure el período (en días) durante el cual se ejecutará el plan programado.
Cuando el usuario inicia sesión en el sistema	Si selecciona esta opción, el plan se ejecutará cuando un usuario específico o cualquier usuario inicie sesión en el recurso informático de destino.
Cuando el usuario cierra sesión en el sistema	Si selecciona esta opción, el plan se ejecutará cuando un usuario específico o cualquier usuario cierre la sesión del recurso informático de destino.
Al iniciarse el sistema	Si selecciona esta opción, el plan se ejecutará cuando se inicie el recurso informático de destino.
Cuando el sistema está apagado	Si selecciona esta opción, el plan se ejecutará cuando se apague el recurso informático de destino.
Cuando el	Si selecciona esta opción, el plan se ejecutará cuando el recurso

© Acronis International GmbH, 2003-2025

Opción	Descripción
sistema está en línea	informático de destino se ponga en línea.

c. En la sección **Condiciones de inicio**, seleccione todas las condiciones que deben cumplirse de forma simultánea para iniciar el plan.

Condición	Descripción
Ejecutar solo si la carga de trabajo está en línea	Esta condición se cumple cuando la carga de trabajo de destino se conecta a Internet.
El usuario está inactivo	Esta condición se cumple cuando se está ejecutando el protector de pantalla en el equipo o el equipo está bloqueado.
El usuario cerró la sesión	Si selecciona esta condición, puede posponer un plan programado hasta que el usuario de la carga de trabajo de destino cierre sesión.
Coincidir con intervalo	Si selecciona esta condición, debe definir el intervalo de tiempo en el que puede ejecutarse el plan.
Ahorrar batería	Si selecciona esta condición, podrá asegurarse de que el plan no se interrumpirá porque la batería sea baja. Las siguientes opciones están disponibles: • **No iniciar con alimentación por batería** El plan se iniciará únicamente si el equipo está conectado a una fuente de alimentación. • **Iniciar con alimentación por batería si su nivel es superior a** El plan se iniciará si el equipo está conectado a una fuente de alimentación o si el nivel de la batería es superior al valor especificado.
No iniciar con conexiones de uso medido	Si selecciona esta condición, el plan no se ejecutará si la carga de trabajo de destino accede a Internet a través de una conexión de uso medido.
No iniciar con conexiones a las siguientes redes Wi-Fi	Si selecciona esta condición, el plan no se ejecutará si la carga de trabajo de destino está conectada a cualquiera de las redes inalámbricas especificadas. Para utilizar esta condición, debe especificar el SSID de la red prohibida. La restricción se aplica a todas las redes de contengan el nombre especificado como una subcadena en su nombre, sin distinción de mayúsculas y minúsculas. Por ejemplo, si especifica `teléfono` como nombre de red, el plan no se iniciará cuando el dispositivo esté conectado a alguna de las siguientes redes: `Teléfono de Juan`, `wifi_teléfono` o `wifi_de_mi_teléfono`.

© Acronis International GmbH, 2003-2025

Condición	Descripción
Comprobar dirección IP del dispositivo	Si selecciona esta condición, el plan no se ejecutará si alguna de las direcciones IP de la carga de trabajo de destino está dentro o fuera del rango de direcciones IP especificado. Las siguientes opciones están disponibles: • **Iniciar si queda fuera del intervalo IP** • **Iniciar si queda dentro del intervalo IP** Solo se admiten direcciones IPv4.
Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos	Utilice esta opción para establecer el intervalo de tiempo tras el cual se ejecutará el plan, independientemente del resto de condiciones. El plan comenzará cuando se cumplan el resto de las condiciones o cuando termine este periodo, lo que suceda primero. Esta opción no está disponible si ha seleccionado la opción **Ejecutar una vez** para la programación.

d. Haga clic en **Listo**.

10. Haga clic en **Crear**.

Adición de un recurso informático a un plan de despliegue de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede agregar recursos informáticos a un plan de despliegue de software después de haberlo creado.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para añadir un recurso informático a un plan de despliegue de software

Planes de despliegue de software

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de despliegue de software**.
2. Haga clic en el plan de despliegue de software.
3. Según si el plan ya se ha aplicado a una carga de trabajo, haga lo siguiente:
   - Haga clic en **Añadir cargas de trabajo**, si el plan todavía no se ha aplicado a ninguna carga de trabajo.
   - Haga clic en **Gestionar cargas de trabajo**, si el plan se ha aplicado a alguna carga de trabajo.

© Acronis International GmbH, 2003-2025

4. Seleccione una carga de trabajo de la lista y haga clic en **Agregar**.
5. Haga clic en **Guardar**.
6. Haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en el recurso informático al que desee aplicar un plan de despliegue de software.
3. Haga clic en **Proteger** y, a continuación, en **Agregar plan**.
4. En **Seleccione un plan de la lista que figura a continuación**, seleccione **Despliegue de software** para ver solo los planes de despliegue de software.
5. Haga clic en **Aplicar**.
6. Haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Cómo quitar recursos informáticos de los planes de despliegue de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Puede eliminar recursos informáticos que se agregaron a un plan de despliegue de software.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Pasos para eliminar recursos informáticos de un plan de despliegue de software

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de despliegue de software**.
2. Haga clic en el plan de despliegue de software.
3. Haga clic en **Gestionar cargas de trabajo**.
4. Seleccione uno o varios recursos informáticos que desee eliminar del plan de despliegue de software y haga clic en **Eliminar**.
5. Haga clic en **Listo**.
6. Haga clic en **Guardar**.

Acciones adicionales con planes de despliegue de software

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

© Acronis International GmbH, 2003-2025

Desde la pantalla **Planes de implementación de software**, puede realizar las operaciones adicionales siguientes con los planes de implementación de software: ver detalles, editar, ver actividades, ver alertas, renombrar, clonar, exportar, importar, y eliminar.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Tiene uno de los siguientes roles de Cyber Protection: administrador de la empresa o administrador de cibernética.

Ver detalles

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para ver los detalles de un plan de despliegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Ver detalles**.

Editar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para editar un plan de despliegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Editar**.

Actividades

Pasos para ver las actividades relacionadas con un plan de despliegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Actividades**.
3. Haga clic en una actividad para ver más información sobre ella.

Alertas

Pasos para ver las alertas

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Alertas**.

Cambiar nombre

© Acronis International GmbH, 2003-2025

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para cambiar el nombre de un plan de despliegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Cambiar nombre**.
3. Escriba el nuevo nombre del plan y haga clic en **Continuar**.

Clonar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para clonar un plan de despliuegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Clonar**.
3. Haga clic en **Crear**.

Exportar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para exportar un plan de despliegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Exportar**.
   La configuración del plan se exporta en formato JSON al equipo local.

Importar

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Un archivo JSON con la configuración del plan está disponible en el equipo desde el que ha iniciado sesión en la consola.

Para importar un plan de despliegue de software

1. En la pantalla **Planes de implementación de software**, haga clic en **Importar plan**.
2. En la ventana que se abre, busque el archivo JSON.
3. Haga clic en el archivo y luego en **Abrir**.

© Acronis International GmbH, 2003-2025

El plan de despliegue del software aparece en la pantalla. Ahora puede aplicarlo a las cargas de trabajo.

Eliminar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar un plan de despliegue de software

1. En la pantalla **Planes de despliegue de software**, haga clic en el icono **Más acciones** del plan de despliegue de software.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

© Acronis International GmbH, 2003-2025

Conexión a cargas de trabajo para asistencia o escritorio remotos

La funcionalidad de asistencia y escritorio remotos es una manera conveniente de conectarse a las cargas de trabajo de su organización para obtener control o asistencia remotos.

A partir de diciembre de 2022, esta funcionalidad es compatible con los protocolos NEAR, RDP y Apple Screen Sharing. Para obtener más información, consulte "Protocolos de conexión remota" (p. 1446).

Puede utilizar la funcionalidad de escritorio remoto para ejecutar las siguientes tareas:

- Conectarse a cargas de trabajo remotas de Windows, macOS y Linux con NEAR en el modo de solo visualización.
- Conectarse a cargas de trabajo remotas de Windows con RDP.
- Conectarse a cargas de trabajo remotas de macOS mediante el uso compartido de pantalla de Apple en modo de solo visualización o en modo cortina.
- Conectarse a cargas de trabajo administradas y controlarlas de forma remota con conexiones remotas de la nube.
- Conectarse a cargas de trabajo no administradas y controlarlas de forma remota con conexiones remotas directas.
- Conectarse a cargas de trabajo remotas no administradas con Acronis Asistencia rápida.
- Conectarse a cargas de trabajo remotas con métodos de autenticación diferentes: con credenciales de carga de trabajo remotas, solicitando permiso para observar y controlar o con un código de acceso (para Asistencia rápida).
- Observar varios monitores al mismo tiempo en la vista múltiple.
- Grabar sesiones remotas (al estar conectado a través de NEAR).
- Ver el informe de historial de sesiones.

Puede utilizar la funcionalidad de asistencia remota para ejecutar las siguientes tareas:

- Conectarse a cargas de trabajo remotas de Windows, macOS y Linux con NEAR en el modo de control.
- Conectarse a cargas de trabajo remotas de macOS mediante el uso compartido de pantalla de Apple en modo de control.
- Proporcionar asistencia remota para las cargas de trabajo con conexiones remotas de la nube.
- Transferir archivos entre las cargas de trabajo locales y remotas.
- Realizar acciones de administración básicas en la carga de trabajo remota: reiniciar, apagar, pausar, vaciar papelera de reciclaje y cerrar la sesión del usuario remoto.
- Supervisar la carga de trabajo remota con capturas de pantalla periódicas del escritorio.

© Acronis International GmbH, 2003-2025

Importante
Para activar la funcionalidad completa de escritorio y asistencia remotos en una carga de trabajo administrada, debe configurar y aplicar un plan de administración remota a la carga de trabajo. Aunque puede aplicar solo un plan de administración remota a una carga de trabajo, según sus necesidades, puede configurar planes de administración remota diferentes y aplicarlos a diferentes cargas de trabajo.

De esta forma, puede controlar la disponibilidad de las funciones en los planes de administración remota para que correspondan a las licencias que se asignan a sus cargas de trabajo.

Para obtener más información acerca de los planes de administración remota y trabajar con ellos, consulte "Planes de administración remota" (p. 1450).

Nota
La funcionalidad de asistencia y escritorio remotos requiere:

- una instalación única de Cliente de Connect en el recurso informático de gestión (host). Cuando intente realizar una acción remota (control remoto o asistencia remota) en un recurso informático de destino por primera vez, el sistema le pedirá que descargue el cliente. Alternativamente, puede descargar Cliente de Connect desde la ventana **Descargas** en la consola de Protección. Para obtener más información sobre los ajustes que puede configurar, consulte "Configuración de los ajustes de Cliente de Connect" (p. 1492).
- instalación del Agente de Connect en las cargas de trabajo gestionadas. El Agente de Connect es un módulo que forma parte del agente de Protección, a partir de la versión 15.0.31266.
- para las cargas de trabajo remotas de macOS, se deben conceder los permisos de sistema necesarios para el Agente de Connect. Para obtener más información, consulte "Instalación de agentes de protección en macOS" (p. 72).
- ejecución de la aplicación Acronis Asistencia rápida en las cargas de trabajo sin gestionar. Puede descargar Acronis Asistencia rápida desde el sitio web.

Para obtener más información sobre las plataformas compatibles con cada componente de asistencia y escritorio remotos, consulte "Sistemas operativos compatibles con escritorio remoto y asistencia" (p. 1445).

Funciones de asistencia y escritorio remotos

La siguiente tabla proporciona más información sobre las funciones compatibles de la funcionalidad de escritorio remoto y asistencia según la licencia.

© Acronis International GmbH, 2003-2025

Característica	Protección estándar (modo de licencia basado en servicios)	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Asistencia remota a través de RDP para Windows	No	No
Compartir una conexión remota con usuarios	No	No
Conexiones remotas		
Acciones remotas	Sí	Sí
Selección de una sesión para conectarse a Windows, macOS o Linux	No	Sí
Conexión directa mediante RDP y el uso compartido de pantalla de Apple	No	Sí
Control de varias ventanas	No	Sí
Modos de conexión: control, solo visualización y cortina	No	Sí
Compatibilidad con credenciales comunes para conexiones remotas	Sí	Sí
Conexiones simultáneas por técnico		
a través de RDP	Sí	Sí
a través de NEAR	No	Sí
Transferencia y uso compartido de archivos		
de Windows a Windows, macOS o Linux	No	Sí
de macOS a Windows, macOS o Linux	No	Sí
de Linux a Windows, macOS o Linux	No	Sí
Conexión mediante la aplicación Asistencia rápida		

© Acronis International GmbH, 2003-2025

Característica	Protección estándar (modo de licencia basado en servicios)	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
de Windows a Windows, macOS o Linux	No	Sí
de macOS a Windows, macOS o Linux	No	Sí
de Linux a Windows, macOS o Linux	No	Sí
Conexiones remotas mediante protocolos		
Conexión remota a través de NEAR		
de Windows a Windows, macOS o Linux	No	Sí
de macOS a Windows, macOS o Linux	No	Sí
de Linux a Windows, macOS o Linux	No	Sí
Conexión remota a través de RDP (cliente de escritorio)		
de Windows a Windows	Sí	Sí
de macOS a Windows	Sí	Sí
de Linux a Windows	Sí	Sí
Conexión remota a través de RDP (cliente web)		
de Windows a Windows	Sí	Sí
de macOS a Windows	Sí	Sí
de Linux a Windows	Sí	Sí
Conexión remota a través del uso compartido de pantalla de Apple		
de Windows, macOS o Linux a macOS	No	Sí
Administración de sesiones		
Grabación de sesiones	No	Sí

© Acronis International GmbH, 2003-2025

Característica	Protección estándar (modo de licencia basado en servicios)	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Informes y supervisión		
Historial de sesiones y búsqueda	No	Sí
Transmisión de captura de pantalla	No	Sí
Intercambio de archivos a través del portapapeles	No	Sí

Sistemas operativos compatibles con escritorio remoto y asistencia

La siguiente tabla enumera los sistemas operativos compatibles para cada componente de la funcionalidad de asistencia y escritorio remotos.

Componente del escritorio remoto	Plataformas compatibles
Cliente de Connect	• Windows 7 o posterior • macOS 10.13 o posterior • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Agente de Connect	• Windows 7 o posterior • Windows Server 2008 R2 o posterior • macOS 10.13 o posterior • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco

© Acronis International GmbH, 2003-2025

Componente del escritorio remoto	Plataformas compatibles
	Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Asistencia rápida	• Windows 7 o posterior • Windows Server 2008 R2 o posterior • macOS 10.13 o posterior • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protocolos de conexión remota

La funcionalidad de escritorio remoto utiliza los siguientes protocolos para las conexiones remotas.

NEAR

NEAR es un protocolo altamente seguro desarrollado por Acronis que tiene las siguientes características:

- ### H.264

  NEAR implementa tres modos de calidad: **Suave**, **Equilibrado** y **Nítido**. En el modo **Suave**, NEAR utiliza la codificación H.264 de hardware en macOS y Windows para codificar la imagen de escritorio y recurrir al codificador de software si el codificador de hardware no está disponible. El tamaño de la imagen actualmente está limitado a la resolución Full HD (1920x1080).

- ### Códec adaptable

  En los modos de calidad **Equilibrado** y **Nítido**, NEAR utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264.

  En el modo **Equilibrado**, la calidad de la imagen se ajusta automáticamente según sus condiciones de red actuales y mantiene la velocidad de frotogramas actual.

  En el modo **Nítido**, la imagen tiene la máxima calidad, pero podría tener una velocidad de fotogramas reducida si su red, procesador o tarjeta de vídeo se sobrecargan.

© Acronis International GmbH, 2003-2025

El códec adaptable utiliza OpenCL en Windows y macOS cuando está disponible en sus controladores gráficos.

- ### Transferencia de sonido

  NEAR es capaz de capturar el sonido del equipo remoto y transferirlo al host. Para obtener más información acerca de habilitar el redireccionamiento del sonido remoto en Windows, macOS y Linux, consulte "Redireccionamiento de sonido remoto" (p. 1447).

- ### Diferentes opciones de inicio de sesión

  Puede utilizar los siguientes métodos para iniciar sesión en la carga de trabajo remota.

  Código de acceso: el usuario que ha iniciado sesión en la carga de trabajo remota ejecuta Asistencia rápida y le dice el código de acceso. Con este método, siempre se conecta a la sesión del usuario conectado en ese momento.

  Credenciales de la carga de trabajo: inicie sesión en la carga de trabajo remota con las credenciales del administrador que están registradas en la carga de trabajo.

  Solicitar permiso para observar o controlar: el usuario que ha iniciado sesión en la carga de trabajo remota le pedirá que permita o deniegue la conexión.

- ### Seguridad

  Sus datos siempre están cifrados de dos formas con cifrado AES en NEAR.

RDP

El protocolo de escritorio remoto (RDP) es un protocolo propio desarrollado por Microsoft que permite la conexión con el ordenador de Windows sobre una conexión de red.

Uso compartido de pantalla de Apple

El uso compartido de pantalla de Apple es un cliente VNC de Apple incluido como parte de macOS versión 10.5 y posteriores.

Redireccionamiento de sonido remoto

Cliente de Connect es compatible con la transmisión de audio a través del protocolo de conexión NEAR. Para obtener más información sobre NEAR, consulte "Protocolos de conexión remota" (p. 1446).

Redireccionamiento del sonido desde una carga de trabajo remota de Windows

Para las cargas de trabajo de Windows, el sonido remoto debería transmitirse automáticamente. Asegúrese de que hay dispositivos de salida de sonido (altavoces o auriculares) conectados a la carga de trabajo remota.

© Acronis International GmbH, 2003-2025

Redireccionamiento del sonido desde una carga de trabajo remota de macOS

Para habilitar el redireccionamiento de sonido desde una carga de trabajo macOS, asegúrese de que:

- La carga de trabajo tiene instalado el agente de Protección.
- La carga de trabajo tiene instalado un controlador de captura del sonido.
- La carga de trabajo utiliza el protocolo NEAR para las conexiones remotas.

Nota
En macOS 10.15 Catalina, se debe otorgar el permiso de micrófono al Agente de Connect. Para obtener más información sobre el permiso de micrófono al Agente de Connect, consulte "Conceder los permisos de sistema necesarios para el Agente de Connect" (p. 58).

El agente funciona con los siguientes controladores de captura de sonido: Soundflower o Blackhole.

El proceso de instalación en las versiones más recientes se describe en la página de wikis de Blackhole: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Nota
actualmente, Cliente de Connect es compatible solo con la versión de dos canales de Blackhole.

De manera alternativa, si Homebrew está instalado en la carga de trabajo, puede instalar Blackhole mediante la ejecución de este comando:

```
brew install --cask blackhole-2ch
```

Nota
Si bien el sonido de una carga de trabajo remota de macOS se redirecciona, el usuario que ha iniciado sesión en la carga de trabajo remota no escuchará el sonido.

Redireccionamiento del sonido desde una carga de trabajo remota de Linux

El redireccionamiento de sonido remoto debería funcionar automáticamente con la mayoría de las distribuciones de Linux. Si el redireccionamiento de sonido remoto no funciona de forma predeterminada, instale el controlador PulseAudio mediante la ejecución del siguiente comando:

```
sudo apt-get install pulseaudio
```

Conexiones a cargas de trabajo remotas para asistencia o escritorio remotos

La funcionalidad de asistencia y escritorio remotos ofrece diversas formas de establecer conexiones directas remotas o en la nube con sus cargas de trabajo.

© Acronis International GmbH, 2003-2025

Las conexiones directas se establecen a través de TCP/IP en la red del área local (LAN) entre Cliente de Connect y la carga de trabajo remota que no tiene un agente instalado. No requiere acceso a Internet.

Las conexiones de la nube se establecen entre Cliente de Connect y el agente o Asistencia rápida en la carga de trabajo a través de Acronis Cloud.

La siguiente tabla proporciona más información sobre las opciones de conexión de la nube.

Conexión en la nube	Opción de conexión en la nube	Modo Ver	Acción remota compatible	Disponible para
a través de NEAR	de Cliente de Connect a Agente de Connect de Cliente de Connect a Asistencia rápida	Control Solo visualización	Escritorio remoto Asistencia remota	cargas de trabajo administradas
a través de RDP	de Cliente de Connect a Agente de Connect desde el cliente web a Agente de Connect	Control	Escritorio remoto	cargas de trabajo administradas
a través del uso compartido de pantalla de Apple	de Cliente de Connect a Agente de Connect	Control Solo visualización Cortina	Escritorio remoto Asistencia remota	cargas de trabajo administradas

La siguiente tabla proporciona más información sobre las opciones de conexión directa.

Conexión directa	Opción de conexión directa	Acción remota compatible	Disponible para
a través de RDP	desde Cliente de Connect al servidor RDP	Escritorio remoto	cargas de trabajo no administradas
a través del uso compartido de pantalla de Apple	de Cliente de Connect al servidor del uso compartido de pantalla de Apple	Escritorio remoto Asistencia remota	cargas de trabajo no administradas

© Acronis International GmbH, 2003-2025

Planes de administración remota

Los planes de administración remota son planes que aplica al agente de Protección para habilitar y configurar la funcionalidad de escritorio y asistencia remotos en sus cargas de trabajo administradas.

Si no se aplica ningún plan de administración remota a una carga de trabajo, la funcionalidad de escritorio y asistencia remotos se limitará a las acciones remotas (reiniciar, apagar, pausar, vaciar papelera de reciclaje y cerrar la sesión del usuario remoto).

Nota
La disponibilidad de la función y los ajustes que puede configurar en el plan de administración remota dependen de la licencia que se asigne a la carga de trabajo.

Creación de un plan de administración remota

Puede crear un plan de administración remota y asignarlo a una carga de trabajo para configurar la funcionalidad de asistencia y escritorio remotos en la carga de trabajo administrada.

Nota
La disponibilidad de la configuración del plan de administración remota depende de la licencia que se asigne a la carga de trabajo.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Si el dispositivo gestionado está unido a Entra ID (anteriormente Azure AD) y desea conectarse a él mediante el protocolo NEAR, consulte este artículo de la base de conocimientos.

Pasos para crear un plan de administración remota

Desde planes de administración remota

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de administración remota**.
2. Cree un plan de administración remota mediante una de estas dos opciones:
   - Si no hay planes de administración remota en la lista, haga clic en **Crear**.
   - Si hay planes de administración remota en la lista, haga clic en **Crear plan**.
3. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Continuar**.
4. Haga clic en **Protocolos de conexión** y active los protocolos que desee que estén disponibles en este plan de administración remota para las conexiones remotas: NEAR, RDP o el uso compartido de pantalla de Apple.
5. [Opcional] Para el protocolo NEAR, en la sección **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración

© Acronis International GmbH, 2003-2025

correspondiente y haga clic en **Listo**.

Configuración	Descripción	Disponible para
Bloquee la carga de trabajo cuando el usuario desconecte de la sesión de la consola	Si selecciona este ajuste, la carga de trabajo se bloqueará cuando se desconecte de la sesión de la consola.	Windows, macOS
Permitir que solo un usuario a la vez se conecte con NEAR o transfiera archivos	Si selecciona esta configuración, las conexiones que utilizan NEAR y la transferencia de archivos no serán posibles mientras haya una conexión remota activa a la carga de trabajo.	Windows, macOS, Linux
Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador	Si selecciona esta configuración, el administrador podrá conectarse a cualquier sesión de usuario estándar en la carga de trabajo. Si **Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador** y **Permitir la creación de sesiones del sistema** están desactivadas, solo podrá conectarse a sesiones de administrador activas en las cargas de trabajo remotas de macOS.	Windows, macOS
Permitir la creación de sesiones del sistema	Si selecciona esta configuración, cuando establezca conexiones remotas, el administrador se conectará en una sesión nueva y no en una de las sesiones activas existentes.	macOS
Permitir la sincronización del portapapeles	Si selecciona esta configuración, podrá transferir datos entre su	Windows, macOS, Linux

© Acronis International GmbH, 2003-2025

Configuración	Descripción	Disponible para
	portapapeles y el portapapeles de la carga de trabajo remota. Por ejemplo, podrá copiar texto de un archivo en la carga de trabajo remota y pegarlo en un archivo de su carga de trabajo, y viceversa.	

6. Haga clic en **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción
Mostrar si la carga de trabajo se controla de forma remota	Si selecciona esta configuración, se mostrará una notificación en el escritorio de la carga de trabajo remota cuando haya una conexión de escritorio remoto activa con la carga de trabajo.
Pedir permiso al usuario para realizar capturas de pantalla de la carga de trabajo	Si selecciona esta configuración, el usuario de la carga de trabajo remota será notificado cuando el administrador solicite la transmisión de capturas de pantalla desde la carga de trabajo.

7. Haga clic en **Gestión de la carga de trabajo**, seleccione las funciones que desee que estén disponibles en las cargas de trabajo remotas y, a continuación, haga clic en **Listo**.

Configuración	Descripción	Disponible el
Transferencia de archivos	Permite la transferencia de archivos entre cargas de trabajo locales y remotas.	Windows, macOS, Linux
Transmisión de captura de pantalla	Habilite la transmisión de capturas de pantalla del escritorio de la carga de trabajo remota para la consola de Cyber Protect.	Windows, macOS, Linux
Seguimiento de geolocalización	Permite el seguimiento de la ubicación del recurso informático cuando los servicios de ubicación están habilitados en la configuración del sistema	Windows, macOS, Linux

© Acronis International GmbH, 2003-2025

Configuración	Descripción	Disponible el
	operativo del mismo.	
Chat	Permite el chat en vivo entre un técnico que ha iniciado sesión en la consola de Cyber Protect y un usuario que ha iniciado sesión en la carga de trabajo remota.	Windows, macOS

8. Haga clic en **Configuración de pantalla**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Nota
La **Configuración de pantalla** solo está disponible para las conexiones a través de NEAR.

Configuración	Descripción	Disponible el
Use la deduplicación del escritorio para capturarlo	La duplicación del escritorio es uno de los métodos de captura de pantalla de Windows. En algunos entornos, puede ser inestable. Si no utiliza la deduplicación del escritorio, utilizará el método básico (BitBlt) en su lugar. Es mucho más lento, pero más estable.	Windows
Use la aceleración de OpenCL	La aceleración de OpenCL puede acelerar el códec adaptable, que se encarga del modo de calidad **Equilibrado**, mediante la ejecución de algunos cálculos en la unidad de procesamiento gráfico (GPU). Para ello, es necesario instalar el controlador de OpenCL en el Linux remoto. El códec adaptable utiliza OpenCL en macOS y Windows cuando está disponible en sus controladores gráficos.	Linux

© Acronis International GmbH, 2003-2025

Configuración	Descripción	Disponible el
Use la codificación H.264 de hardware	NEAR es compatible con tres modos de calidad: **Suave**, **Equilibrado** y **Nítido**. El modo **Suave** utiliza la codificación H.264 para codificar la imagen del escritorio. El modo **Equilibrado** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La calidad de la imagen se ajusta automáticamente según sus condiciones de red actuales y mantiene la velocidad de fotogramas actual. El modo **Nítido** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La imagen siempre tiene la máxima calidad, pero podría tener una velocidad de fotogramas reducida por segundos si su red, procesador o tarjeta de vídeo se sobrecargan.	Windows, macOS

9. Haga clic en **Caja de herramientas**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción	Disponible el
Mostrar los últimos usuarios que han iniciado sesión	Si selecciona este ajuste, la información sobre los usuarios que iniciaron sesión por última vez en las cargas de trabajo será visible en los detalles de la carga de trabajo.	Windows, macOS, Linux

© Acronis International GmbH, 2003-2025

Configuración	Descripción	Disponible el
	Para obtener más información sobre los últimos usuarios que iniciaron sesión, consulte "Viendo el último usuario que ha iniciado sesión" (p. 467).	
Interfaz de línea de comandos remota	Este ajuste habilita el acceso remoto a la interfaz de línea de comandos del dispositivo gestionado.	Windows, macOS

10. [Opcional] Pasos para añadir cargas de trabajo al plan:
    a. Haga clic en **Añadir cargas de trabajo**.
    b. Seleccione las cargas de trabajo y haga clic en **Agregar**.
    c. Si hay problemas de compatibilidad que desea resolver, siga el procedimiento descrito en "Resolver problemas de compatibilidad" (p. 258).
11. Haga clic en **Crear**.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que quiera aplicar un plan de administración remota.
3. Haga clic en **Proteger** y, a continuación, en **Agregar plan**.
4. Haga clic en **Crear plan** y seleccione **Administración remota**.
5. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Continuar**.
6. Haga clic en **Protocolos de conexión** y active los protocolos que desee que estén disponibles en este plan de administración remota para las conexiones remotas: NEAR, RDP o el uso compartido de pantalla de Apple.
7. [Opcional] Para el protocolo NEAR, en la sección **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción	Disponible para
Bloquee la carga de trabajo cuando el usuario desconecte de la sesión de la consola	Si selecciona este ajuste, la carga de trabajo se bloqueará cuando se desconecte de la sesión de la consola.	Windows, macOS

© Acronis International GmbH, 2003-2025

Configuración	Descripción	Disponible para
Permitir que solo un usuario a la vez se conecte con NEAR o transfiera archivos	Si selecciona esta configuración, las conexiones que utilizan NEAR y la transferencia de archivos no serán posibles mientras haya una conexión remota activa a la carga de trabajo.	Windows, macOS, Linux
Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador	Si selecciona esta configuración, el administrador podrá conectarse a cualquier sesión de usuario estándar en la carga de trabajo. Si **Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador** y **Permitir la creación de sesiones del sistema** están desactivadas, solo podrá conectarse a sesiones de administrador activas en las cargas de trabajo remotas de macOS.	Windows, macOS
Permitir la creación de sesiones del sistema	Si selecciona esta configuración, cuando establezca conexiones remotas, el administrador se conectará en una sesión nueva y no en una de las sesiones activas existentes.	macOS
Permitir la sincronización del portapapeles	Si selecciona esta configuración, podrá transferir datos entre su portapapeles y el portapapeles de la carga de trabajo remota. Por ejemplo, podrá copiar texto de un archivo en la carga de trabajo remota y pegarlo en un archivo de su carga de trabajo, y viceversa.	Windows, macOS, Linux

© Acronis International GmbH, 2003-2025

8. Haga clic en **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción
Mostrar si la carga de trabajo se controla de forma remota	Si selecciona esta configuración, se mostrará una notificación en el escritorio de la carga de trabajo remota cuando haya una conexión de escritorio remoto activa con la carga de trabajo.
Pedir permiso al usuario para realizar capturas de pantalla de la carga de trabajo	Si selecciona esta configuración, el usuario de la carga de trabajo remota será notificado cuando el administrador solicite la transmisión de capturas de pantalla desde la carga de trabajo.

9. Haga clic en **Gestión de la carga de trabajo**, seleccione las funciones que desee que estén disponibles en las cargas de trabajo remotas y, a continuación, haga clic en **Listo**.

Configuración	Descripción	Disponible el
Transferencia de archivos	Permite la transferencia de archivos entre cargas de trabajo locales y remotas.	Windows, macOS, Linux
Transmisión de captura de pantalla	Habilite la transmisión de capturas de pantalla del escritorio de la carga de trabajo remota para la consola de Cyber Protect.	Windows, macOS, Linux
Seguimiento de geolocalización	Permite el seguimiento de la ubicación del recurso informático cuando los servicios de ubicación están habilitados en la configuración del sistema operativo del mismo.	Windows, macOS, Linux
Chat	Permite el chat en vivo entre un técnico que ha iniciado sesión en la consola de Cyber Protect y un usuario que ha iniciado sesión en la carga de trabajo remota.	Windows, macOS

10. Haga clic en **Configuración de pantalla**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

© Acronis International GmbH, 2003-2025

Nota
La **Configuración de pantalla** solo está disponible para las conexiones a través de NEAR.

Configuración	Descripción	Disponible el
Use la deduplicación del escritorio para capturarlo	La duplicación del escritorio es uno de los métodos de captura de pantalla de Windows. En algunos entornos, puede ser inestable. Si no utiliza la deduplicación del escritorio, utilizará el método básico (BitBlt) en su lugar. Es mucho más lento, pero más estable.	Windows
Use la aceleración de OpenCL	La aceleración de OpenCL puede acelerar el códec adaptable, que se encarga del modo de calidad **Equilibrado**, mediante la ejecución de algunos cálculos en la unidad de procesamiento gráfico (GPU). Para ello, es necesario instalar el controlador de OpenCL en el Linux remoto. El códec adaptable utiliza OpenCL en macOS y Windows cuando está disponible en sus controladores gráficos.	Linux
Use la codificación H.264 de hardware	NEAR es compatible con tres modos de calidad: **Suave**, **Equilibrado** y **Nítido**. El modo **Suave** utiliza la codificación H.264 para codificar la imagen del escritorio. El modo **Equilibrado** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264.	Windows, macOS

© Acronis International GmbH, 2003-2025

Configuración	Descripción	Disponible el
	La calidad de la imagen se ajusta automáticamente según sus condiciones de red actuales y mantiene la velocidad de fotogramas actual. El modo **Nítido** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La imagen siempre tiene la máxima calidad, pero podría tener una velocidad de fotogramas reducida por segundos si su red, procesador o tarjeta de vídeo se sobrecargan.	

11. Haga clic en **Caja de herramientas**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción	Disponible el
Mostrar los últimos usuarios que han iniciado sesión	Si selecciona este ajuste, la información sobre los usuarios que iniciaron sesión por última vez en las cargas de trabajo será visible en los detalles de la carga de trabajo. Para obtener más información sobre los últimos usuarios que iniciaron sesión, consulte "Viendo el último usuario que ha iniciado sesión" (p. 467).	Windows, macOS, Linux
Interfaz de línea de comandos remota	Este ajuste habilita el acceso remoto a la interfaz de línea de comandos del dispositivo gestionado.	Windows, macOS

12. Haga clic en **Crear**.

© Acronis International GmbH, 2003-2025

Adición de una carga de trabajo a un plan de administración remota

Puede agregar cargas de trabajo a un plan de administración remota después de haberlo creado.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para añadir una carga de trabajo a un plan de administración remota

Desde planes de administración remota

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de administración remota**.
2. Haga clic en el plan de administración remota.
3. Según si el plan ya se ha aplicado a una carga de trabajo, haga lo siguiente:
   - Haga clic en **Añadir cargas de trabajo**, si el plan todavía no se ha aplicado a ninguna carga de trabajo.
   - Haga clic en **Gestionar cargas de trabajo**, si el plan se ha aplicado a alguna carga de trabajo.
4. Seleccione una carga de trabajo de la lista y haga clic en **Agregar**.
5. Haga clic en **Guardar**.
6. Haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que quiera aplicar un plan de administración remota.
3. Haga clic en **Proteger** y, a continuación, en **Agregar plan**.
4. En **Seleccione un plan de la lista que figura a continuación**, seleccione **Administración remota** para ver solo los planes de administración remota.
5. Haga clic en **Aplicar**.
6. Haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Eliminación de cargas de trabajo de un plan de administración remota

Según sus necesidades, puede eliminar cargas de trabajo de un plan de administración remota.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar cargas de trabajo de un plan de administración remota

1. En la consola de Cyber Protect, vaya a **Gestión** > **Planes de administración remota**.
2. Haga clic en el plan de administración remota.

© Acronis International GmbH, 2003-2025

3. Haga clic en **Gestionar cargas de trabajo**.
4. Seleccione una o varias cargas de trabajo que quiera eliminar del plan de administración remota y haga clic en **Eliminar**.
5. Haga clic en **Listo**.
6. Haga clic en **Guardar**.

Acciones adicionales con planes de administración remota

Desde la pantalla **Planes de administración remota**, puede realizar las siguientes acciones adicionales con los planes de administración remota: ver detalles, editar, ver las actividades, ver las alertas, renombrar, habilitar, deshabilitar, clonar, exportar, establecer como favorito, establecer como predeterminado y eliminar.

Ver detalles

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para ver los detalles de un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Ver detalles**.

Editar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para editar un plan

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Editar**.
3. Edite los ajustes y haga clic en **Guardar**.

Actividades

Pasos para ver las actividades relacionadas con un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Actividades**.
3. Haga clic en una actividad para ver más información sobre ella.

Alertas

Pasos para ver las alertas

© Acronis International GmbH, 2003-2025

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Alertas**.

Cambiar nombre

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para cambiar el nombre de un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Cambiar nombre**.
3. Escriba el nuevo nombre del plan y haga clic en **Continuar**.

Habilitar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para habilitar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Habilitar**.

Deshabilitar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para deshabilitar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Deshabilitar**.

Clonar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para clonar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.

© Acronis International GmbH, 2003-2025

2. Haga clic en **Clonar**.
3. Haga clic en **Crear**.

Exportar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para exportar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Exportar**.
   La configuración del plan se exporta en un formato JSON al equipo local.

Importar

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Un archivo JSON con la configuración del plan está disponible en el equipo desde el que ha iniciado sesión en la consola.

Para importar un plan de administración remota

1. En la pantalla de **Planes de administración remota**, **Importar plan**.
2. En la ventana que se abre, busque el archivo JSON.
3. Haga clic en el archivo y luego en **Abrir**.
   El plan de administración remota aparece en la pantalla. Ahora puede aplicarlo a las cargas de trabajo.

Establecer como predeterminado

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para establecer un plan de administración remota como predeterminado

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Establecer como predeterminado**.
3. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla **Planes de administración remota**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Establecer como favorito

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

© Acronis International GmbH, 2003-2025

Para establecer un plan de administración remota como favorito

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Agregar a favoritos**.
   En la pantalla de **Planes de administración remota**, aparece un icono de estrella junto al nombre del plan.

Eliminar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

Credenciales de la carga de trabajo

Puede añadir credenciales de administrador o que no sean de administrador de las cargas de trabajo remotas (nombre de usuario y contraseña o contraseña de VNC), guardarlas en el almacén de credenciales de la nube y utilizarlas para la autenticación automática cuando se conecte a las cargas de trabajo que administra. De este modo, en lugar de introducir esas credenciales de forma manual cada vez durante el paso de autenticación de la conexión, puede guardarlas en el almacén de credenciales una vez y asignarlas a varias cargas de trabajo, y Cliente de Connect utilizará esas credenciales cada vez que usted quiera conectarse a las cargas de trabajo de forma remota.

Nota
Las credenciales que se almacenan en el almacén de credenciales no se comparten entre los distintos niveles de inquilino. Se comparten solo en el mismo nivel de inquilino y para el mismo inquilino cliente o inquilino partner.

Esto significa que si un inquilino cliente tiene varios administradores, verán y compartirán las credenciales del almacén de credenciales. Sin embargo, los administradores de partners o de clientes de otros inquilinos no podrán ver o utilizar esas credenciales.

Agregar credenciales

Puede agregar credenciales y utilizarlas para las conexiones remotas a varias cargas de trabajo.

Pasos para agregar credenciales a una carga de trabajo y guardarlas en el Almacén de credenciales

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo para la que desee agregar credenciales.
3. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
4. Haga clic en **Agregar credenciales**.
5. En el **Almacén de credenciales**, haga clic en **Agregar credenciales**.
6. Introduzca las credenciales.

Campo	Descripción
Nombre de las credenciales	Identificador de las credenciales que se mostrarán en el almacén de credenciales.
Nombre de usuario	Nombre de usuario que se utilizará para las conexiones remotas a la carga de trabajo de destino.
Contraseña	La contraseña se utilizará para las conexiones remotas a la carga de trabajo de destino.
Contraseña de VNC	Este campo solo está disponible para el uso compartido de pantalla de Apple.

7. Haga clic en **Guardar**.

Asignación de credenciales a una carga de trabajo

Después de agregar credenciales, puede utilizarlas para autenticarse automáticamente cuando se conecte a una carga de trabajo que gestione.

Nota
El uso de cuentas de Microsoft Entra ID (anteriormente Azure AD) con el protocolo NEAR requiere una configuración adicional. Consulte este artículo de la base de conocimientos.

Pasos para asignar las credenciales guardadas a una carga de trabajo para la autenticación automática

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. En la pestaña del protocolo soportado (NEAR, RDP o el uso compartido de pantalla de Apple), haga clic en **Agregar credenciales**.
4. En el **Almacén de credenciales**, seleccione las credenciales de la lista y haga clic en **Seleccionar credenciales**.

© Acronis International GmbH, 2003-2025

Eliminar credenciales

Puede eliminar credenciales que ya no se necesiten.

Pasos para eliminar credenciales de el almacén de credenciales

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. En la pestaña del protocolo admitido (NEAR, RDP o el uso compartido de pantalla de Apple), haga clic en **Eliminar**.
4. Haga clic en **Eliminar** en la ventana de confirmación.

Anular la asignación de credenciales de una carga de trabajo

Puede anular la asignación de credenciales de una carga de trabajo, pero conservarlas en el almacén de credenciales.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. En la pestaña del protocolo admitido (NEAR, RDP o el uso compartido de pantalla de Apple), haga clic en **Anular asignación**.
4. Haga clic en **Anular asignación** en la ventana de confirmación.

Trabajar con cargas de trabajo gestionadas

Las cargas de trabajo gestionadas son cargas de trabajo en las que se ha instalado el agente de Protección.

Puede realizar las siguientes acciones en las cargas de trabajo remotas gestionadas:

- conectarse a la asistencia remota o al escritorio remoto mediante NEAR en modo de **Control** o **Solo visualización**
- conectarse al escritorio remoto con RDP en el modo de **Control**
- conectarse a la asistencia remota o al escritorio remoto mediante uso compartido de pantalla de Apple en modo de **Control**, **Solo visualización** o **Cortina**
- conectarse al escritorio remoto a través del cliente web
- reiniciar, apagar, pausar, vaciar papelera de reciclaje y cierre la sesión del usuario remoto de las cargas de trabajo remotas

© Acronis International GmbH, 2003-2025

- transferir archivos entre su carga de trabajo y las cargas de trabajo remotas
- supervisarlos con capturas de pantalla

Nota
Las conexiones del escritorio remoto a cargas de trabajo gestionadas requieren la instalación de un agente de Protección y la aplicación de un plan de administración remota en la carga de trabajo.

Ajuste de la configuración de RDP

Puede configurar los ajustes que se aplicarán automáticamente para las conexiones RDP de control remoto a la carga de trabajo administrada.

Pasos para configurar los ajustes RDP de una carga de trabajo

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. Configure los ajustes en la pestaña **RDP**.

Configuración	Descripción
Reproducción de audio	Estos ajustes habilitan o deshabilitan el redireccionamiento del sonido de la carga de trabajo remota en tu carga de trabajo local.
Grabación de audio	Estos ajustes determinan si la grabación de audio (cuando se hable al micrófono) se transferirá a la carga de trabajo remota.
Redirigir impresoras	Si selecciona este ajuste, las impresoras de su carga de trabajo estarán disponibles en la carga de trabajo remota. **Nota** El redireccionamiento de impresoras no es compatible con las conexiones a escritorios remotos a través de un cliente web.
Redirigir archivos	Estos ajustes definen si los archivos de la carga de trabajo local se compartirán a la carga de trabajo remota.
Profundidad del color	Estos ajustes determinan el número de colores en la imagen que transferirá RDP. Un valor más alto requiere más ancho de banda. **Color intenso**: 16 bits **Color real**: • 24 bits para conexiones RDP a través del cliente web • 32 bits para conexiones RDP a través de Cliente de Connect

4. Haga clic en el botón Cerrar.

© Acronis International GmbH, 2003-2025

Conexión a cargas de trabajo administradas para asistencia o escritorio remotos

Nota
La disponibilidad de los protocolos de conexión que puede utilizar para las conexiones remotas depende de la configuración del plan de administración remota y del sistema operativo de la carga de trabajo remota.

Requisitos previos

- [Para conexiones a través del uso compartido de pantalla de Apple] El uso compartido de pantalla de Apple está activado en la carga de trabajo de macOS.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para conectarse de forma remota a una carga de trabajo administrada para asistencia o escritorio remotos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo a la que desee conectarse.
3. Haga clic en **Escritorio remoto**.
   Por defecto, NEAR se selecciona como protocolo de conexión.
4. [Opcional] En la lista desplegable **Protocolo de conexión**, seleccione el protocolo de conexión que desee utilizar.
5. Haga clic en el modo de vista que quiera usar.

Protocolo	Conexiones remotas a	Modo Ver	Acción remota compatible
NEAR	Windows Linux macOS	**Control**: En este modo, podrá observar y ejecutar operaciones en la carga de trabajo remota. **Solo visualización**: en este modo, solo podrá observar la carga de trabajo remota.	Escritorio remoto Asistencia remota
RDP	Windows	**Control**: En este modo, podrá ver y ejecutar operaciones en la carga de trabajo remota.	Escritorio remoto

© Acronis International GmbH, 2003-2025

Protocolo	Conexiones remotas a	Modo Ver	Acción remota compatible
		Nota Si RDP está desactivado en la configuración del sistema operativo de la carga de trabajo, aparecerá una ventana emergente. Utilice esta ventana para habilitar RDP para la carga de trabajo para la sesión actual o en general: • Si desea habilitar RDP para esta carga de trabajo solo para la sesión actual, seleccione **Deshabilítelo una vez que termine la sesión** y, a continuación, haga clic en **Permitir**. • Si desea habilitar RDP para esta carga de trabajo, haga clic en **Permitir**.	
Uso compartido de pantalla de Apple	macOS	**Control**: En este modo, podrá observar y ejecutar operaciones en la carga de trabajo remota. **Solo visualización**: en este modo, solo podrá observar la carga de trabajo remota. **Cortina**: disponible solo para cargas de trabajo de macOS. Si se conecta a la carga de trabajo remota en el modo cortina, la pantalla de la carga de trabajo remota se atenuará, y el usuario remoto no podrá ver sus acciones en la carga de trabajo.	Escritorio remoto Asistencia remota

6. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.

     Nota
     El sistema sugiere automáticamente el plan más apropiado, dependiendo del protocolo que seleccionó en el paso anterior.

   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

© Acronis International GmbH, 2003-2025

Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

7. [Si la función correspondiente no está habilitada en el plan de administración remota que se aplica a la carga de trabajo] En la ventana **Actualizar plan de administración remota**, haga clic en **Actualizar**, habilite la función, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
8. [Si Cliente de Connect no está instalado en su carga de trabajo] En el cuadro de diálogo **Conectar a carga de trabajo**, haga clic en **Descargar Cliente de Connect**, descargue e instale el cliente en su carga de trabajo y, a continuación, pulse en **Conectar**.
9. [Si aparece un mensaje de confirmación emergente] Haga clic en **Abrir Cliente de Connect**.
10. En la ventana **Autenticación**, seleccione una opción de autenticación y facilite las credenciales necesarias.

Nota
Si tiene credenciales asignadas a la carga de trabajo, la autenticación se llevará a cabo automáticamente y se omitirá este paso. Para obtener más información, consulte "Asignación de credenciales a una carga de trabajo" (p. 1465).

Opción de autenticación	Descripción
Con las credenciales de la carga de trabajo remota	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador de la carga de trabajo remota. Esta opción está disponible para NEAR, RDP y el uso compartido de pantalla de Apple. Puede utilizar esta opción para autenticar la asistencia y el escritorio remotos.
Solicitar permiso para observar	Se le permitirá establecer la conexión remota en el modo de observación después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita. Esta opción está disponible para NEAR y el uso compartido de pantalla de Apple. Puede utilizar esta opción para autenticar la asistencia remota.
Solicitar permiso para controlar	Se le permitirá establecer la conexión remota en el modo de control después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita. Esta opción está disponible para NEAR y el uso compartido de pantalla de Apple. Puede utilizar esta opción para autenticar la asistencia remota.

11. Haga clic en **Conectar** y luego en la sesión que mostrar (si hay más de una sesión de usuario disponible en la carga de trabajo).

© Acronis International GmbH, 2003-2025

Cliente de Connect abrirá una ventana del visor nueva en la que podrá ver el escritorio de la carga de trabajo remota. El visor tiene una barra de herramientas con acciones adicionales que puede ejecutar en la carga de trabajo remota después de establecer la conexión remota. Para obtener más información, consulte "Uso de la barra de herramientas en la ventana del Visor" (p. 1488).

Conectar a una carga de trabajo gestionada a través del cliente web

Puede establecer una conexión a escritorio remoto para una carga de trabajo administrada a través del cliente web.

Nota
El redireccionamiento de impresoras no es compatible con las conexiones a escritorios remotos a través de un cliente web.

Requisitos previos

- Se ha habilitado RDP en la carga de trabajo administrada.
- Su buscador es compatible con HTML5.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para conectar a una carga de trabajo de forma remota a través de un cliente web

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que desee conectarse de forma remota y, a continuación, haga clic en **Escritorio remoto**>**Conectarse a través del cliente web**.
3. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
4. [Si la función correspondiente no está habilitada en el plan de administración remota que se aplica a la carga de trabajo] En la ventana **Actualizar plan de administración remota**, haga clic en **Actualizar**, habilite la función, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
5. Introduzca el nombre de usuario y la contraseña para acceder a la carga de trabajo y haga clic en **Conectar**.

© Acronis International GmbH, 2003-2025

Nota
Si tiene credenciales asignadas a la carga de trabajo, la autenticación se llevará a cabo automáticamente y se omitirá este paso. Para obtener más información, consulte "Asignación de credenciales a una carga de trabajo" (p. 1465).

Transferir archivos

Puede transferir fácilmente archivos entre la carga de trabajo local y una carga de trabajo gestionada.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para transferir archivos entre la carga de trabajo local y una carga de trabajo gestionada

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo con la que desee transferir archivos.
3. Haga clic en **Administrar** y luego en **Transferir archivos**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.

     Nota
     El sistema sugiere automáticamente el plan más apropiado.

   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
5. [Si **Permitir conexiones a través de NEAR** o **Transferencia de archivos** está deshabilitado en el plan de administración remota que se aplica a la carga de trabajo] En la ventana **Actualizar plan de administración remota**, haga clic en **Actualizar**, habilite la configuración, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
6. [Si Cliente de Connect no está instalado en su carga de trabajo] En el cuadro de diálogo **Conectar a carga de trabajo**, haga clic en **Descargar Cliente de Connect**, descargue e instale el cliente en su carga de trabajo y, a continuación, pulse en **Conectar**.
7. [Si aparece un mensaje de confirmación emergente] Haga clic en **Abrir Cliente de Connect**.
8. En la ventana **Autenticación**, seleccione una opción de autenticación y facilite las credenciales necesarias.

© Acronis International GmbH, 2003-2025

Opción de autenticación	Descripción
Con las credenciales de la carga de trabajo remota	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador de la carga de trabajo remota.
Solicitar permiso para transferir archivos	Se le permitirá transferir archivos después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita.

9. En la ventana **Transferencia de archivos**, examine los archivos, arrástrelos y suéltelos en el destino que desee.

Nota
Los archivos de la carga de trabajo local aparecen en el panel de la izquierda, y los archivos de la carga de trabajo remota aparecen en el panel de la derecha.
Cuando comienza una transferencia de archivos, aparece en el panel de **Tareas**.

10. [Opcional] Si desea eliminar las tareas completadas del panel de **Tareas**, haga clic en **Borrar completadas**.
11. Cuando se completen todas las transferencias, cierre la ventana.

Compartir contenido del portapapeles entre cargas de trabajo

Puede enviar el contenido del portapapeles de su carga de trabajo a una carga de trabajo remota u obtener el contenido del portapapeles de una carga de trabajo remota a través de NEAR. Por ejemplo, puede querer copiar un texto de un archivo en la carga de trabajo remota y pegarlo en un documento en su carga de trabajo, y viceversa.

Enviar portapapeles

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para enviar el contenido del portapapeles de su carga de trabajo a una carga de trabajo remota

1. Inicie una sesión de control remoto a una carga de trabajo gestionada a través de NEAR.
   Para obtener más información, consulte "Conexión a cargas de trabajo administradas para asistencia o escritorio remotos" (p. 1468).
2. [Opcional] Si desea que el contenido de su portapapeles y el de la carga de trabajo remota se sincronicen automáticamente, en la barra de herramientas **Visor**, haga clic en el icono **Otros** y después seleccione **Sincronización automática del portapapeles**.
3. Para compartir el contenido de su portapapeles con el de la carga de trabajo remota, haga lo siguiente.

© Acronis International GmbH, 2003-2025

- Si la **sincronización automática del portapapeles** está deshabilitada, realice los pasos correspondientes:
  a. En su carga de trabajo local, copie el texto o la imagen que desea enviar.
  b. En la barra de herramientas **Visor** de la carga de trabajo remota, haga clic en el icono **Otros**.
  c. Haga clic en **Enviar portapapeles**.
  d. Abra el archivo en el que desea pegar el contenido y, a continuación, péguelo.
- Si la **sincronización automática del portapapeles** está habilitada, realice los pasos correspondientes según el contenido que desee compartir.

Opción	Acciones
Si desea compartir uno o varios archivos en su portapapeles local	a. En su carga de trabajo local, copie el archivo o los archivos que desea enviar. b. Abra la ventana **Visor** de la carga de trabajo remota. c. En la ventana emergente de alerta que aparece, haga clic en **Enviar al ordenador remoto**. d. Pegue el contenido en la carga de trabajo remota.
Si desea compartir un texto de un archivo en su portapapeles local	a. En su carga de trabajo local, copie el texto que desea enviar. b. Abra la ventana **Visor** de la carga de trabajo remota. c. Abra el archivo en el que desea pegar el contenido. d. Pegue el contenido en el archivo.

Obtener portapapeles

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para obtener el contenido del portapapeles de una carga trabajo remota a su carga de trabajo

1. Inicie una sesión de control remoto a una carga de trabajo gestionada a través de NEAR. Para obtener más información, consulte "Conexión a cargas de trabajo administradas para asistencia o escritorio remotos" (p. 1468).
2. Si desea que el contenido de su portapapeles y el de la carga de trabajo remota se sincronicen automáticamente, en la barra de herramientas **Visor**, haga clic en el icono **Otros** y después seleccione **Sincronización automática del portapapeles**.
3. Para obtener el contenido del portapapeles de la carga de trabajo remota en su portapapeles, realice lo siguiente.

© Acronis International GmbH, 2003-2025

- Si la **sincronización automática del portapapeles** está deshabilitada, realice los pasos correspondientes.
  a. En la carga de trabajo remota, copie el texto o la imagen que desea compartir.
  b. En la barra de herramientas **Visor** de la carga de trabajo remota, haga clic en el icono **Otros**.
  c. Haga clic en **Obtener portapapeles**.
  d. En la carga de trabajo local, abra el archivo en el que desea pegar el contenido.
  e. Pegue el contenido en el archivo.
- Si la **Sincronización automática del portapapeles** está habilitada, realice los pasos correspondientes según el contenido que desee obtener.

Opción	Acciones
Si desea obtener uno o varios archivos del portapapeles de la carga de trabajo remota en el portapapeles local	a. En la carga de trabajo remota, copie el archivo o los archivos que desee obtener. b. En la alerta emergente que aparece, haga clic en **Recibir portapapeles**. c. En su carga de trabajo local, pegue el contenido.
Si desea obtener un texto del portapapeles de la carga de trabajo remota en el portapapeles local	a. En la carga de trabajo remota, copie el texto que desea obtener. b. En su carga de trabajo local, pegue el contenido en un archivo.

Llevar a cabo acciones de control en cargas de trabajo gestionadas

Puede gestionar una carga de trabajo remota mediante acciones de control básico sobre ella: vaciar papelera de reciclaje, suspender, reiniciar, apagar y cierre la sesión del usuario remoto.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Vaciar papelera de reciclaje

Pasos para vaciar la papelera de reciclaje en la carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Vaciar papelera de reciclaje**.

© Acronis International GmbH, 2003-2025

4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
5. Seleccione la sesión de usuario para la que desee llevar a cabo la acción y haga clic en **Vaciar papelera de reciclaje**.

Suspender

Pasos para suspender una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Suspender**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

Reiniciar

Pasos para reiniciar una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Reiniciar**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

© Acronis International GmbH, 2003-2025

Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

5. Dependiendo del sistema operativo que esté instalado en la carga de trabajo remota, realice una de las siguientes acciones:
   - Para cargas de trabajo de Windows, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se reinicie dicha carga de trabajo y, a continuación, seleccione al usuario y haga clic en **Reiniciar** de nuevo.
   - Para cargas de trabajo de macOS, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se reinicie la carga de trabajo y, a continuación, haga clic en **Reiniciar** de nuevo.
   - Para las cargas de trabajo de Linux, haga clic en **Reiniciar**.

Apagar

Pasos para apagar una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Apagar**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
5. Dependiendo del sistema operativo que esté instalado en la carga de trabajo remota, realice una de las siguientes acciones:
   - Para cargas de trabajo de Windows, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se apague la carga de trabajo, y, a continuación, seleccione al usuario y haga clic en **Apagar** de nuevo.
   - Para cargas de trabajo de macOS, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se apague la carga de trabajo y, a continuación, haga clic en **Apagar** de nuevo.
   - Para las cargas de trabajo de Linux, haga clic en **Apagar** de nuevo.

Cierre la sesión del usuario remoto

Pasos para cerrar la sesión de usuario de una carga de trabajo remota

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Cierre la sesión del usuario remoto**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
5. Seleccione el usuario del que desea cerrar sesión y, a continuación, haga clic en **Cerrar sesión**.

Conexión a línea de comandos remota

Puede conectarse de forma remota a la interfaz de línea de comandos de sus cargas de trabajo de Windows y macOS gestionadas y realizar tareas relacionadas con diagnósticos, solución de problemas, gestión de configuración, mantenimiento, automatización y programación de tareas.

Requisitos previos

- Tener el rol de Administrador de ciberseguridad.
- La autenticación de doble factor (2FA) está habilitada para su cuenta de Acronis Cyber Protect Cloud.

Windows

Pasos para conectarse de forma remota a la línea de comandos de un dispositivo Windows

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo para la que desea iniciar la línea de comandos remota.
3. En el menú **Acciones**, haga clic en **Gestionar** y luego en **Línea de comandos**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.

     Nota
     El sistema sugiere automáticamente el plan más apropiado.

   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

© Acronis International GmbH, 2003-2025

Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

5. En la nueva pestaña que se abre, seleccione la interfaz de línea de comandos que desea utilizar.
   Verá las siguientes opciones, según las herramientas de línea de comandos que estén disponibles en la carga de trabajo:
   - PowerShell 7 (64 bits)
   - PowerShell 7 (32 bits)
   - PowerShell 5 (64 bits)
   - PowerShell 5 (32 bits)
   - Símbolo del sistema (64 bits)
   - Símbolo del sistema (32 bits)
6. En el campo **Usuario**, seleccione la cuenta de usuario con la que desea iniciar la línea de comandos.

   Nota
   Si inicia la línea de comandos con la cuenta de sistema, sus acciones no serán visibles para el usuario de la carga de trabajo remota.
   Si inicia la línea de comandos con la cuenta de usuario que ha iniciado sesión, sus acciones serán visibles.

7. Dependiendo de si desea guardar la configuración para la siguiente sesión, marque o desmarque **Guardar configuración para la siguiente sesión**.
8. Haga clic en **Iniciar sesión**.
   Se abre la consola de la línea de comandos. Ahora puede realizar tareas en la consola.

   Nota
   Iniciar y finalizar una sesión de línea de comandos remota crea un registro en **Registro de auditoría**. El registro incluye detalles sobre el evento, como la fecha y la hora, el inquilino, el nombre de la carga de trabajo, la dirección IP y el iniciador.

macOS

Pasos para conectarse de forma remota a la línea de comandos de un dispositivo macOS

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo para la que desea iniciar la línea de comandos remota.
3. En el menú **Acciones**, haga clic en **Gestionar** y luego en **Terminal**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.

© Acronis International GmbH, 2003-2025

Nota
El sistema sugiere automáticamente el plan más apropiado.

- Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

  Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

5. En la nueva pestaña que se abre, seleccione la interfaz de línea de comandos que desea utilizar.

   Verá las siguientes opciones, según las herramientas de línea de comandos que estén disponibles en la carga de trabajo:

   - BASH
   - ZSH

6. En el campo **Usuario**, seleccione la cuenta de usuario con la que desea iniciar la línea de comandos.

   Nota
   Puede seleccionar entre las cuentas de usuario no relacionadas con servicios y que no estén ocultas disponibles. La cuenta de usuario que se registró primero (por fecha de registro) se selecciona de forma predeterminada.

7. Dependiendo de si desea guardar la configuración para la siguiente sesión, marque o desmarque **Guardar configuración para la siguiente sesión**.
8. Haga clic en **Iniciar sesión**.

   Se abre la consola de la línea de comandos. Ahora puede realizar tareas en la consola.

   Nota
   Iniciar y finalizar una sesión de línea de comandos remota crea un registro en **Registro de auditoría**. El registro incluye detalles sobre el evento, como la fecha y la hora, el inquilino, el nombre de la carga de trabajo, la dirección IP y el iniciador.

Acciones adicionales con la consola de línea de comandos remota

Después de acceder de forma remota a la línea de comandos de una carga de trabajo gestionada, puede realizar las siguientes acciones desde la consola: copiar contenido de la consola, pegar contenido en la consola, vaciar la consola y exportar el contenido de la consola.

Copiar

Puede copiar partes del contenido de la consola.

Pasos para copiar desde la consola

© Acronis International GmbH, 2003-2025

1. En la consola de línea de comandos, seleccione el texto que desea copiar.
2. Haga clic en **Copiar**.
   El texto seleccionado se copia.

Pegar

Puede pegar texto en la consola de línea de comandos remota.

Pasos para pegar

1. Abra la consola de línea de comandos remota.
2. En la consola de línea de comandos, haga clic en **Pegar**.
   El texto se pega en la consola.

Vaciar consola

Puede borrar el contenido de la consola de línea de comandos remota.

Pasos para vaciar la consola

1. Abra la consola de línea de comandos remota.
2. En la consola de línea de comandos, haga clic en **Vaciar consola**.
   La consola se vacía.

Exportar

Puede exportar el contenido completo de la consola de línea de comandos como un archivo TXT.

Pasos para exportar el contenido de la consola de línea de comandos

1. Abra la consola de línea de comandos remota.
2. En la consola de línea de comandos, haga clic en **Exportar**.
   El contenido de la consola se exporta y se guarda como un archivo TXT en la carpeta de descarga predeterminada de su equipo local.

Supervisión de cargas de trabajo mediante la transmisión de captura de pantalla

Puede supervisar el estado de una carga de trabajo con la función de transmisión de captura de pantalla.

Requisitos previos

- La versión del agente de protección está actualizada y es compatible con la función de transmisión de capturas de pantalla.
- La carga de trabajo está en línea.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Supervisar una carga de trabajo

© Acronis International GmbH, 2003-2025

Pasos para supervisar una carga de trabajo mediante la transmisión de captura de pantalla

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Transmisión de captura de pantalla**.
2. Haga clic en la carga de trabajo que quiera supervisar.
3. [Si no se aplica un plan de administración remota a la carga de trabajo] Haga clic en **Aplicar un plan de administración remota** y, a continuación, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
4. [Si la **Transmisión de captura de pantalla** está deshabilitada en el plan de administración remota que se aplica a la carga de trabajo] Haga clic en la ventana **Ir al plan de administración remota**, pulse en **Editar**, habilite **Transmisión de captura de pantalla**, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
5. [Si **Solicitar permiso para tomar capturas de pantalla** está habilitado en el plan de administración remota que se aplica a la carga de trabajo] Haga clic en **Solicitar la transmisión de captura de pantalla**.

   Verá la captura de pantalla después de que el usuario de la carga de trabajo remota apruebe la solicitud.
6. [Opcional] Seleccione la sesión de usuario.
7. [Opcional] Seleccione la pantalla.
8. [Opcional] Seleccione la tasa de actualización para hacer una nueva captura de pantalla del escritorio.
9. [Opcional] Seleccione la calidad de la imagen.
10. [Opcional] Para descargar la captura de pantalla, haga clic en el icono de descarga.

Hacer una captura de pantalla

Pasos para hacer una captura de pantalla de una carga de trabajo gestionada

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo de la que desee hacer una captura de pantalla.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Hacer captura del escritorio**.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] Haga clic en **Aplicar un plan de administración remota** y, a continuación, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en

© Acronis International GmbH, 2003-2025

Confirmar.

Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

5. [Si la **Transmisión de captura de pantalla** está deshabilitada en el plan de administración remota que se aplica a la carga de trabajo] Haga clic en la ventana **Ir al plan de administración remota**, pulse en **Editar**, habilite **Transmisión de captura de pantalla**, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
6. [Si **Solicitar permiso para tomar capturas de pantalla** está habilitado en el plan de administración remota que se aplica a la carga de trabajo] Haga clic en **Solicitar la transmisión de captura de pantalla**.

   Verá la captura de pantalla después de que el usuario de la carga de trabajo remota apruebe la solicitud.
7. [Opcional] Seleccione la sesión de usuario.
8. [Opcional] Seleccione la pantalla.
9. [Opcional] Seleccione la tasa de actualización para hacer una nueva captura de pantalla del escritorio.
10. [Opcional] Seleccione la calidad de la imagen.
11. [Opcional] Para descargar la captura de pantalla, haga clic en el icono de descarga.

Observar varias cargas de trabajo gestionadas de manera simultánea

Puede observar los escritorios de múltiples cargas de trabajo remotas simultáneamente en una única ventana. Esta funcionalidad requiere que NEAR o Apple Screen Sharing estén habilitados en los planes de administración remota que se aplican a las cargas de trabajo.

Nota
El número de escritorios que puede ver de manera simultánea en la ventana depende del tamaño de su monitor.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para observar varias cargas de trabajo de manera simultánea

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las cargas de trabajo que desea observar.
3. Haga clic en **Vista múltiple**.
4. [Si no se aplica un plan de administración remota a ninguna de las cargas de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:

© Acronis International GmbH, 2003-2025

- Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.

  Nota
  El sistema sugiere automáticamente el plan más apropiado.

- Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

  Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

5. [Si la función correspondiente no está habilitada en el plan de administración remota que se aplica a las cargas de trabajo] En la ventana **Actualizar plan de administración remota**, haga clic en **Actualizar**, habilite la función y, a continuación, inicie este procedimiento desde el paso 1.
6. [Si Cliente de Connect no está instalado en su carga de trabajo] En el cuadro de diálogo **Conectar a carga de trabajo**, haga clic en **Descargar Cliente de Connect**, descargue e instale el cliente en su carga de trabajo y, a continuación, pulse en **Conectar**.
7. [Si aparece un mensaje de confirmación emergente] Haga clic en **Abrir Cliente de Connect**.
8. En la ventana **Autenticación**, seleccione una opción de autenticación y facilite las credenciales necesarias.

Opción de autenticación	Descripción
Con las credenciales de la carga de trabajo remota	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador en la carga de trabajo remota.
Solicitar permiso para observar	Se le permitirá establecer la conexión remota en el modo de observación después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita.

9. Si desea utilizar el mismo método de autenticación y las credenciales cuando se conecte a todas las cargas de trabajo remotas que ha seleccionado en el paso 2, seleccione **Usar en otros equipos**.
10. Haga clic en **Conectar**.

    En la barra de herramientas de la ventana de vista múltiple, puede seleccionar un modo de visualización en el que conectarse a una carga de trabajo. Esta acción abrirá una ventana del Visor independiente para esa carga de trabajo.

© Acronis International GmbH, 2003-2025

Nota
Si alguna de las cargas de trabajo seleccionadas está fuera de línea o tiene una versión obsoleta del agente instalada, no se mostrará en la ventana de vista múltiple.
Todas las conexiones de vista múltiple a cargas de trabajo remotas están en el modo **Solo visualización**.

Trabajar con cargas de trabajo sin gestionar

Las cargas de trabajo sin gestionar son cargas de trabajo en las que no se ha instalado el agente de Protección.

Puede realizar las siguientes acciones en las cargas de trabajo remotas sin gestionar:

- conectarse a la asistencia remota mediante Acronis Asistencia rápida
- conectarse a la asistencia o el escritorio remotos mediante una dirección IP
- transferir archivos entre su carga de trabajo y la carga de trabajo remota mediante Asistencia rápida

Nota
Para conectarse de forma remota a cargas de trabajo no administradas con Asistencia rápida, asegúrese de que:

- La licencia requerida se asigna a su inquilino de cliente.
- La aplicación Asistencia rápida se ejecuta en la carga de trabajo remota a la que desee conectarse.

Conectar a cargas de trabajo no administradas a través de Acronis Asistencia rápida

Puede utilizar la función Asistencia rápida para conectarse de forma remota bajo demanda a las cargas de trabajo no gestionadas y proporcionar ayuda a tiempo.

Requisitos previos

- La licencia requerida se asigna a su inquilino de cliente.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.
- El usuario remoto ha facilitado el ID de la carga de trabajo y el código de acceso de Asistencia rápida.
- El usuario remoto ha descargado y ejecutado Acronis Asistencia rápida.

Pasos para conectarse a una carga de trabajo para asistencia remota mediante Asistencia rápida

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Asistencia rápida**.
3. En la ventana **Asistencia rápida**, introduzca el ID de carga de trabajo que le proporcionó el usuario final y, a continuación, seleccione **Conectar**.
4. Haga clic en **Conectar**.
5. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, seleccione **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
6. En la ventana **Autenticación**, introduzca el código de acceso.
7. Cliente de Connect abrirá una ventana del visor nueva en la que podrá ver el escritorio de la carga de trabajo remota. El visor tiene una barra de herramientas con acciones adicionales que puede ejecutar en la carga de trabajo remota después de establecer la conexión remota. Para obtener más información, consulte "Uso de la barra de herramientas en la ventana del Visor" (p. 1488).

Conectar a cargas de trabajo gestionadas mediante una dirección IP

Si hay una carga de trabajo no administrada en su LAN, puede conectarse a ella para obtener asistencia o control remotos mediante su dirección IP. Esta conexión no requiere acceso a Internet.

Requisitos previos

- La licencia requerida se asigna a su inquilino de cliente.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para conectarse a una carga de trabajo para asistencia o escritorio remotos mediante su dirección IP

1. En la consola de Cyber Protect, vaya a **Todos los dispositivos**.
2. Haga clic en **Asistencia rápida**.
3. Haga clic en la pestaña **Vía dirección IP**.
4. Introduzca la dirección IP y el puerto de la carga de trabajo.
5. Seleccione un protocolo de conexión RDP (cargas de trabajo de Windows) o el uso compartido de pantalla de Apple (para cargas de trabajo de macOS), según el sistema operativo de la carga de trabajo remota.

© Acronis International GmbH, 2003-2025

Nota
Las conexiones a través de RDP admiten la acción de escritorio remoto, y las conexiones a través del uso compartido de pantalla de Apple admiten tanto la acción de escritorio remoto como la de asistencia remota.

6. Haga clic en **Conectar**.
7. En la ventana **Autenticación**, facilite las credenciales necesarias.

Para las conexiones a través del uso compartido de pantalla de Apple, Cliente de Connect abrirá una nueva ventana de visualización en la que podrá ver el escritorio de la carga de trabajo remota. El visor tiene una barra de herramientas con acciones adicionales que podrá realizar en la carga de trabajo remota una vez se establezca la conexión remota. Para obtener más información, consulte "Uso de la barra de herramientas en la ventana del Visor" (p. 1488).

Transferir archivos mediante Acronis Asistencia rápida

Puede utilizar la función Asistencia rápida para transferir archivos entre su carga de trabajo y las cargas de trabajo sin gestionar.

Requisitos previos

- La licencia requerida se asigna a su inquilino de cliente.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.
- El usuario remoto ha descargado y ejecutado Acronis Asistencia rápida.
- El usuario remoto ha facilitado el ID del equipo de todo el contenido del equipo y el código de acceso de Asistencia rápida.

Pasos para transferir archivos a una carga de trabajo con Asistencia rápida

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Asistencia rápida**.
3. En la ventana **Asistencia rápida**, introduzca el ID de la carga de trabajo que el usuario final le proporcionó y seleccione **Transferencia de archivos**.
4. Haga clic en **Conectar**.
5. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, seleccione **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
6. En la ventana **Autenticación**, introduzca el código de acceso.

© Acronis International GmbH, 2003-2025

7. En la ventana **Transferencia de archivos**, examine los archivos, arrástrelos y suéltelos en el destino que desee.

   Nota
   Los archivos de la carga de trabajo local aparecen en el panel de la izquierda, y los archivos de la carga de trabajo remota aparecen en el panel de la derecha.
   Cuando comienza una transferencia de archivos, aparece en el panel de **Tareas**.

8. [Opcional] Si desea eliminar las tareas completadas del panel de **Tareas**, haga clic en **Borrar completadas**.
9. Cuando se completen todas las transferencias, cierre la ventana.

Uso de la barra de herramientas en la ventana del Visor

Después de conectarse a una carga de trabajo remota, puede utilizar la barra de herramientas de la ventana del visor para ejecutar rápidamente las distintas acciones.

Icono	Descripción
	**Tamaño real** Adapta el escritorio de la carga de trabajo remota para que un píxel del escritorio remoto se corresponda con un píxel de la ventana del visor.
	**Zoom para ajustar** Adapta el escritorio de la carga de trabajo remota para ajustarlo a la ventana del visor.
	**Bloquear** y **Desbloquear pantalla** Muestra un marcador de posición en la pantalla de la carga de trabajo remota para que el usuario remoto no vea sus acciones.
	**Hacer captura** Guarde la imagen de escritorio del servidor remoto en un archivo local.
	**Seleccione la pantalla** Seleccione la pantalla de la carga de trabajo remota que quiera ver y la resolución deseada. Disponible para conexiones a través del uso compartido de pantalla de Apple con macOS y conexiones NEAR con cualquier sistema operativo. Si el ordenador remoto tiene varios monitores, puede elegir entre los siguientes modos de visualización para varios monitores:

© Acronis International GmbH, 2003-2025

Icono	Descripción
	• **Combinado**: todas las pantallas remotas se muestran en una sola ventana. • **Dividido**: cada visualización remota se muestra en una ventana separada. Este modo es muy conveniente si tiene varias pantallas que están conectadas a su carga de trabajo local. En este caso, por ejemplo, puede organizarlas para ver una pantalla remota en cada pantalla local. Si cierra cualquiera de las pantallas de la carga de trabajo remota, se finalizará la conexión remota. Para ver las pantallas de la carga de trabajo remota, debe volver a conectarla. Disponible solo para conexiones NEAR
	**Calidad de la imagen** Ajusta la calidad de la imagen de la pantalla remota desde el blanco y negro a la mejor posible en las conexiones a través del uso compartido de pantalla de Apple.
	**Calidad de la imagen NEAR** Ajusta la calidad o la proporción de rendimiento de las conexiones NEAR. El lado izquierdo del control deslizante (Suave) da prioridad al rendimiento sobre la calidad de imagen, el derecho (Nítido) supone la mejor calidad de la pantalla del escritorio remoto, pero probablemente peor rendimiento.
	**Enviar Ctrl+Alt+Supr** Envía una secuencia Ctrl + Alt + Suprimir a la carga de trabajo remota. Disponible para cargas de trabajo de Windows y Linux.
	**Transferencia de archivos** Abre la ventana del administrador de archivos para intercambiar archivos entre la carga de trabajo remota y la local. Disponible para conexiones NEAR.
	**Anclar la barra de herramientas** Desactiva la ocultación automática de la barra de herramientas del visor. Disponible para cargas de trabajo de Windows.
	**Pantalla completa** Cambia al modo de pantalla completa y adapta la carga de trabajo remota para que llene la pantalla local por completo.

© Acronis International GmbH, 2003-2025

Icono	Descripción
	Disponible para cargas de trabajo de Windows.
	**Cerrar** Cierra la ventana del Visor y finaliza la sesión del control remoto. Disponible para cargas de trabajo de Windows.

Según el tipo de conexión, puede que haya opciones adicionales disponibles cuando haga clic en el icono **Otros**.

Opción	Descripción
Iniciar grabación/Detener la grabación	Grabe la sesión de escritorio remoto actual. Las grabaciones de la sesión se guardan como archivos .crec en la carga de trabajo local. Puede abrir archivos .crec con Acronis Cliente de Connect. Disponible para conexiones NEAR
Sincronización automática del portapapeles	Cuando active esta opción, el cliente sincronizará automáticamente su portapapeles local y el de la carga de trabajo remota. Disponible para conexiones NEAR
Enviar portapapeles	**Enviar portapapeles** reemplaza el contenido del portapapeles de la carga de trabajo remota con el contenido del portapapeles local. La opción está deshabilitada si la **Sincronización automática del portapapeles** está habilitada. Para obtener más información, consulte "Compartir contenido del portapapeles entre cargas de trabajo" (p. 1473). Disponible para conexiones NEAR
Obtener portapapeles	**Obtener portapapeles** transfiere el contenido del portapapeles de la carga de trabajo remota al portapapeles de la carga de trabajo local. La opción está deshabilitada si la **Sincronización automática del portapapeles** está habilitada. Para obtener más información, consulte "Compartir contenido del portapapeles entre cargas de trabajo" (p. 1473). Disponible para conexiones NEAR
Teclado inteligente/Teclas Raw/Teclas Raw con todos los accesos	Cambia el modo de entrada del teclado para la conexión actual. **Teclado inteligente**: el cliente transmite los códigos Unicode de los símbolos tecleados a nivel local al equipo remoto

© Acronis International GmbH, 2003-2025

Opción	Descripción
directos	**Teclas Raw**: el cliente utiliza los códigos raw de los botones del teclado que presiona. **Teclas Raw con todos los accesos directos**: el cliente deshabilita los accesos directos del sistema local para que se transmitan también al sistema operativo remoto.
Enfoque del teclado al mantener el ratón	Cuando se habilita, el cliente solo captura la entrada del teclado mientras el cursor del ratón local se sitúa encima de la ventana del Visor. Cuando se deshabilita, el cliente captura su teclado siempre que la ventana esté activa.
Mostrar información de conexión/Ocultar la información de conexión	Cuando se seleccione **Mostrar información de conexión**, aparecerá un pequeño panel de información sobre la pantalla del escritorio remoto, que mostrará la información más esencial sobre la conexión actual.
Sonido remoto	Permite que el cliente redirija el sonido desde el equipo remoto al local. Disponible para conexiones NEAR
Preferencias	Configure los ajustes de Cliente de Connect. Para obtener más información, consulte "Configuración de los ajustes de Cliente de Connect" (p. 1492).

Grabar y reproducir sesiones remotas

Puede grabar una sesión remota a través de NEAR en Acronis Cliente de Connect.

Para grabar una sesión remota

1. En la barra de herramientas del Visor en Cliente de Connect, haga clic en **Otro** y seleccione **Iniciar Grabación**.
2. Seleccione un nombre y una ubicación para el registro.

   Por defecto, se asignará un nombre al archivo con la fecha y hora actuales y se ubicará en la carpeta **Documentos** en el directorio principal del usuario actual. Mientras la grabación esté activa, en la barra de herramientas del **Visor** verá un círculo rojo parpadeante en la esquina superior derecha de la pantalla remota y el temporizador de grabación.
3. Para detener la grabación, haga clic en **Otro** y luego en **Detener la grabación**. En un Mac, también puede hacer clic en **Detener** en la barra de herramientas.

   Todos los archivos .crec creados por Acronis Cliente de Connect se abrirán por defecto con Acronis Cliente de Connect.

Para reproducir una grabación

© Acronis International GmbH, 2003-2025

1. Localice un archivo de grabación.
2. Ábralo.

   El reproductor de grabaciones de Acronis Cliente de Connect se abre. Tenga en cuenta que no es posible desplazarse por la grabación. Para encontrar un momento determinado de la grabación, espere hasta que el reproductor lo alcance.
3. [Opcional] Para ajustar la velocidad de reproducción, utilice los iconos **<<** y **>>** en la sección de controles de reproducción.

   La grabación se almacena como una secuencia de eventos transmitidos desde y hacia el servidor remoto durante una conexión. Esto asegura la mejor calidad posible de la grabación con un tamaño de archivo mínimo. Sin embargo, esto también significa que no es posible navegar por la grabación. En este momento tampoco es posible convertir las grabaciones a un formato de vídeo.

Configuración de los ajustes de Cliente de Connect

Después de instalar Cliente de Connect en su carga de trabajo, puede configurar los ajustes según sus preferencias.

Pasos para configurar los ajustes de Cliente de Connect

1. En el menú de inicio, busque **Cliente de Connect** e inícielo.
2. Configure los ajustes en la pestaña **General**.

Opción	Descripción
Escribir registros detallados	Seleccione esta opción para permitir a Cliente de Connect escribir registros detallados. Si está deshabilitado, el cliente solo escribirá información general en el archivo de registro.
Configuración del proxy	Seleccione si desea utilizar el proxy del sistema predeterminado o configurar un proxy SOCKSS personalizado.

3. Configure los ajustes en la pestaña **Visor**.

Opción	Descripción
Solicitar confirmación al cerrar un visor	Seleccione esta opción si desea que Cliente de Connect muestre un mensaje de confirmación cuando intente cerrar la ventana del Visor para evitar el cierre accidental.
Al minimizar	Seleccione si desea suspender la actividad del Visor al minimizar para reducir la carga de la CPU.
Al maximizar	Seleccione si desea habilitar el modo de pantalla completa al maximizar.
Transferencia de portapapeles	Habilite la visualización del indicador de transferencia del Portapapeles en la ventana del Visor cada vez que copie o pegue

© Acronis International GmbH, 2003-2025

Opción	Descripción
	texto e imágenes.
Modo teclado	Habilite la visualización del indicador de modo de Entrada en el título de la ventana del Visor cuando los eventos del ratón y el teclado se envíen al equipo remoto.
Portapapeles	Seleccione **Sincronizar automáticamente el portapapeles** para habilitar la sincronización automática del portapapeles cuando esté disponible.
Enviar eventos de teclado	Escoja si desea utilizar la entrada de su teclado local siempre que la ventana del Cliente de Connect esté activa o solo cuando el puntero del ratón local esté sobre ella.
Color en segundo plano del Visor	Cambie el color en segundo plano de la ventana del Visor.
Volver a conectar automáticamente	Seleccione **Habilitar para volver a conectar automáticamente** si desea que Cliente de Connect vuelva a establecer la conexión automáticamente si se ha interrumpido.
H.264	Puede deshabilitar los decodificadores de hardware.
Cerrar cuando esté inactiva	Seleccione el intervalo de tiempo de inactividad después del cual cerrar la ventana del Visor.

4. Configure los ajustes en la pestaña **Teclado**.

Opción	Descripción
Asignaciones de modificadores	Cambie el comportamiento de las claves del modificador con un menú emergente. Estos ajustes se almacenan de forma independiente para las conexiones NEAR, RDP y el uso compartido de pantalla de Apple.
Modo de entrada	Para cada tipo de conexión (seleccionada en el encabezado del panel), seleccione el modo de entrada predeterminado del teclado.

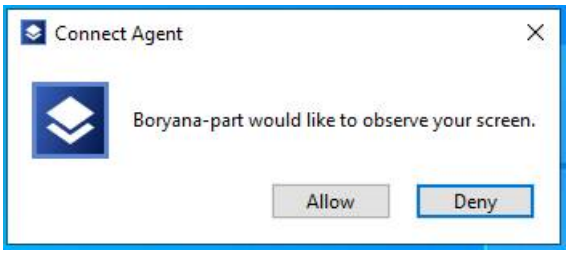
5. Haga clic en **Aceptar**.

Los notificadores del escritorio remoto

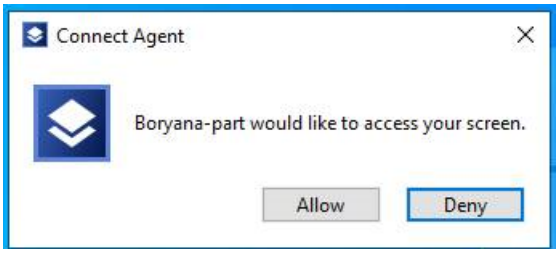
El Agente de Connect muestra cuadros de diálogo de acción (notificadores) en el escritorio de la carga de trabajo remota en los siguientes casos:

- cuando intenta conectarse a la carga de trabajo de forma remota pidiendo permiso para observar. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.

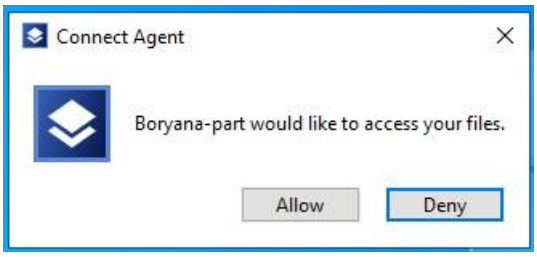
© Acronis International GmbH, 2003-2025



- cuando intenta conectarse a la carga de trabajo de forma remota pidiendo permiso para controlar. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.



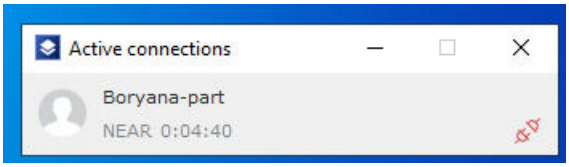
- cuando intenta intercambiar archivos entre su carga de trabajo y la carga de trabajo remota mediante la solicitud de permiso para transferir archivos. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.



Cuando establece una conexión a escritorio remoto con una carga de trabajo, el usuario que ha iniciado sesión en la carga de trabajo verá un notificador de conexión diferente que contiene la siguiente información:

- nombre del usuario que está conectado de forma remota
- protocolo de conexión que se utiliza para establecer la conexión remota
- duración de la conexión remota

El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede terminar la conexión en cualquier momento haciendo clic en el icono **Desconectar** o el icono **Cerrar**.



© Acronis International GmbH, 2003-2025

Seguimiento de geolocalización

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

Con el seguimiento de geolocalización, puede ver la ubicación física en tiempo real de sus dispositivos. Puede utilizar esta información para:

- Restringir el acceso a datos o sistemas confidenciales en función de la ubicación del dispositivo.
- Realice un seguimiento de dispositivos robados o perdidos.
- Mantenga registros precisos de dónde se utilizan los dispositivos en su organización.

Para empezar a seguir la ubicación de un dispositivo, debe habilitar los servicios de ubicación en la configuración de su sistema operativo y, a continuación, aplicar un plan de administración remota que tenga habilitada la opción de seguimiento de geolocalización. Para obtener más información, consulte "Creación de un plan de administración remota" (p. 1450) y "Habilitación de los servicios de ubicación en el sistema operativo" (p. 1496).

Dependiendo del sistema operativo del dispositivo, el seguimiento de geolocalización utiliza la geolocalización del sistema operativo o la geolocalización de IP.

La geolocalización del sistema operativo utiliza GPS, señales Wi-Fi, Bluetooth y datos de torres de telefonía móvil para determinar la ubicación precisa del dispositivo. La geolocalización de IP utiliza la dirección IP del dispositivo y la compara con las regiones geográficas conocidas de la base de datos GeoIP para determinar la ubicación del dispositivo.

El dispositivo informa de los datos de ubicación una vez cada 5 minutos para la geolocalización del sistema operativo y una vez cada 2 horas para la geolocalización de IP.

Para obtener más información sobre el método de seguimiento de geolocalización compatible por sistema operativo, consulte "Método de seguimiento de geolocalización compatible por sistema operativo" (p. 1495).

Método de seguimiento de geolocalización compatible por sistema operativo

El seguimiento geolocalización es compatible con los sistemas operativos Windows, macOS y Linux. Sin embargo, el método que se utiliza para rastrear los dispositivos puede diferir en los diferentes sistemas operativos. La siguiente tabla proporciona más detalles.

Sistema operativo	Método de seguimiento de geolocalización compatible
Windows	Geolocalización del sistema operativo. Este método se utiliza cuando los servicios de ubicación están habilitados en el dispositivo.

© Acronis International GmbH, 2003-2025

Sistema operativo	Método de seguimiento de geolocalización compatible
	Geolocalización de IP
macOS	Geolocalización del sistema operativo. Este método se utiliza cuando los servicios de ubicación están habilitados en el dispositivo. Geolocalización de IP
Linux	Geolocalización de IP

Habilitación de los servicios de ubicación en el sistema operativo

Para seguir la ubicación de un dispositivo, los servicios de ubicación deben estar habilitados en la configuración del sistema operativo del dispositivo.

Para los dispositivos macOS, puede habilitar los servicios de ubicación durante el programa de instalación del agente en el dispositivo al conceder el permiso **Servicios de ubicación**. Para obtener más información, consulte "Conceder los permisos de sistema necesarios para el Agente de Connect" (p. 58).

Si se aplica un plan de administración remota que tiene **Seguimiento de geolocalización** habilitado a un dispositivo en el que los servicios de ubicación están deshabilitados, se muestra una notificación en el dispositivo. Puede hacer clic en el enlace de la notificación y habilitar los servicios de ubicación.

Puede habilitar los servicios de ubicación de un dispositivo en cualquier otro momento. Para obtener más información sobre los pasos que debe seguir, consulte la documentación del proveedor para el sistema operativo correspondiente.

Visualización de la ubicación de un dispositivo

Puede ver en un mapa la última ubicación en la que se vio un dispositivo. También puede ver las coordenadas y la hora en la que el dispositivo estuvo en esa ubicación.

Requisitos previos

- Los servicios de ubicación están habilitados en la configuración del sistema operativo del dispositivo.
- El agente que está instalado en el dispositivo admite el seguimiento de la ubicación.

Pasos para ver la ubicación de un dispositivo

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en el dispositivo que desea seguir y, a continuación, en el menú **Acciones**, haga clic en **Ver en el mapa**.
   Se abre la página **Rastreo de ubicación**.

© Acronis International GmbH, 2003-2025

3. [Si no se aplica un plan de administración remota a la carga de trabajo] En la página **Rastreo de ubicación**, haga clic en **Aplicar un plan de administración remota** y, a continuación, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
4. [Si el **Seguimiento de geolocalización** está deshabilitado en el plan de administración remota que se aplica a la carga de trabajo] En la página **Rastreo de ubicación**, haga clic en **Ir al plan**, pulse en **Editar**, habilite **Seguimiento de geolocalización**, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
5. En la página **Rastreo de ubicación**, haga clic en el pin que marca la ubicación del dispositivo.

   Se muestra la siguiente información adicional: estado del dispositivo (en línea o offline), coordenadas GPS de la ubicación del dispositivo y hora de la última vez que se vio.

Desde detalles del dispositivo

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en el dispositivo que desea seguir y, a continuación, en el menú **Acciones**, haga clic en **Detalles**.
3. Desplácese hacia abajo en la lista de detalles hasta que vea los datos de ubicación.

   Se muestra la siguiente información adicional: método de geolocalización, coordenadas GPS de la ubicación del dispositivo, país, ciudad y hora de la última vez que se vio.
4. [Opcional] Para ver la ubicación del dispositivo en un mapa, haga clic en **Ir a seguimiento de ubicación**.

   En el mapa, la ubicación del dispositivo está marcada con un pin.

Desde Seguimiento de ubicación

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Rastreo de ubicación**.
2. [Opcional] Para filtrar los dispositivos mostrados, haga clic en **Filtro**, seleccione las condiciones de filtro y, a continuación, haga clic en **Aplicar**.

   Puede filtrar los dispositivos por estado: **Todos**, **En línea** o **Fuera de línea**. Los inquilinos de partners también pueden filtrar por cliente.
3. [Opcional] Para encontrar el dispositivo por su nombre, haga clic en **Buscar** y, a continuación, empiece a escribir el nombre del dispositivo.

   Los resultados cambian dinámicamente con cada carácter que escriba.
4. Haga clic en el recurso informático que quiera seguir.
5. [Si no se aplica un plan de administración remota a la carga de trabajo] En la página **Rastreo de ubicación**, haga clic en **Aplicar un plan de administración remota** y, a continuación, realice

© Acronis International GmbH, 2003-2025

una de las siguientes acciones:

- Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
- Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

  Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).

6. [Si el **Seguimiento de geolocalización** está deshabilitado en el plan de administración remota que se aplica a la carga de trabajo] En la página **Rastreo de ubicación**, haga clic en **Ir al plan**, pulse en **Editar**, habilite **Seguimiento de geolocalización**, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.
7. En la página **Rastreo de ubicación**, haga clic en el pin que marca la ubicación del dispositivo.

   Se muestra la siguiente información adicional: estado del dispositivo (conectado o desconectado), coordenadas GPS de la ubicación del dispositivo y hora de la última vez que se vio.

Chat de asistencia

Nota
La disponibilidad de esta característica depende de la licencia que tenga.

El chat de asistencia es una herramienta de comunicación en tiempo real entre técnicos y usuarios remotos de cargas de trabajo de Windows y macOS gestionados. Al utilizar esta funcionalidad, puede lograr una resolución de problemas más rápida y ofrecer un mejor servicio de atención al cliente.

Puede utilizar la funcionalidad de chat de asistencia para llevar a cabo las siguientes tareas:

- Iniciar una sesión de chat con un usuario remoto de una carga de trabajo gestionada.

  Los chats pueden ser iniciados por el técnico, en la consola de Cyber Protect, o por el usuario remoto, en Cyber Protect Monitor. Tanto el técnico como el usuario remoto reciben notificaciones sobre nuevos mensajes y cambios de mensajes del sistema del estado de sus chats. Los nuevos chats que son iniciados desde usuarios remotos se añaden a una cola en estado **Sin asignar**, desde donde los administradores del inquilino pueden asignarlos. Para obtener más información sobre cómo trabajar con chats en el Monitor, consulte "Chats en el Monitor" (p. 363).

  En los chats, si el nombre y el apellido del administrador están configurados en Portal de administración > **Mi empresa** > **Usuarios**, el sistema los muestra. De lo contrario, el sistema genera y muestra un nombre genérico en el formato Técnico XXXX, donde XXXX son los primeros 4 caracteres del ID del usuario interno.

  Como nombre del usuario remoto que ha iniciado sesión en la carga de trabajo gestionada, el sistema muestra:

© Acronis International GmbH, 2003-2025

  - Para cargas de trabajo en Mac, el nombre completo del usuario o, si no está disponible, el nombre de usuario.
  - Para cargas de trabajo en Windows, el nombre de usuario.

Nota
Si el administrador o técnico al que se le asigna el chat en la consola está desconectado o ausente durante 15 minutos, y el chat no se pone en espera, el sistema cambia automáticamente el estado del chat a **Sin asignar**.

- Gestione una sesión de chat asignando, reasignando, poniendo en espera, finalizando y reabriendo.
- Explorar las sesiones de chat en el inquilino.
- Editar o eliminar mensajes en sesiones de chat activas.
- Buscar sesiones de chat según palabras clave o mensajes específicos.
- Exportar el historial del chat en un archivo `.txt`.

Iniciar un chat con un usuario remoto

Puede iniciar un nuevo chat con un usuario remoto desde las pantallas **Todos los dispositivos** y **Chat**.

Requisitos previos

- El sistema operativo de la carga de trabajo es Windows o macOS.
- La función de chat es compatible con su rol de usuario.

Para iniciar un nuevo chat con un usuario remoto

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo con la que desee iniciar un chat y, a continuación, en el menú **Acciones**, haga clic en **Chat**.
3. [Si no se aplica un plan de administración remota a la carga de trabajo] En la ventana **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
4. [Si el **Chat** está deshabilitado en el plan de administración remota que se aplica a la carga de trabajo] En la ventana **Actualizar plan de administración remota**, haga clic en **Actualizar**,

© Acronis International GmbH, 2003-2025

habilite **Chat**, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.

5. En el cuadro de diálogo **Iniciar chat**, seleccione la carga de trabajo y el usuario conectado con el que desee chatear y, a continuación, haga clic en **Iniciar**.

   Se abre una ventana de chat donde puede escribir su mensaje. El chat se asigna automáticamente a usted y se incluye en la lista **Asignado a mí**.

Nota
Si está desconectado o alejado de la consola durante 15 minutos y el chat no se pone en espera, el sistema cambia automáticamente el estado del chat a **Sin asignar**.

Desde Chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Haga clic en **Iniciar chat**.
3. En el cuadro de diálogo **Iniciar chat**, seleccione la carga de trabajo y el usuario conectado con el que desee chatear y, a continuación, haga clic en **Iniciar**.

   Se abre una ventana de chat donde puede escribir su mensaje. El chat se asigna automáticamente a usted y se incluye en la lista **Asignado a mí**. La ventana de chat está inactiva si no se aplica un plan de administración remota a la carga de trabajo o si la función de chat está deshabilitada.
4. [Si no se aplica un plan de administración remota a la carga de trabajo] En el mensaje de advertencia, haga clic en **Aplicar plan** y luego, en el diálogo **Aplicar plan de administración remota**, realice una de las siguientes acciones:
   - Si desea aplicar un plan de administración remota existente, haga clic en el campo **Planes disponibles**, seleccione el plan y, a continuación, haga clic en **Aplicar**.
   - Si desea crear un nuevo plan de administración remota, haga clic en **Agregar**, ajuste la configuración, pulse en **Crear** y, a continuación, en la ventana de confirmación, haga clic en **Confirmar**.

     Para obtener más información sobre cómo crear y configurar un plan de administración remota, consulte "Creación de un plan de administración remota" (p. 1450).
5. [Si el **Chat** está deshabilitado en el plan de administración remota que se aplica a la carga de trabajo] En la ventana **Actualizar plan de administración remota**, haga clic en **Actualizar**, habilite **Chat**, guarde los cambios y, a continuación, inicie este procedimiento desde el paso 1.

Nota
Si está desconectado o alejado de la consola durante 15 minutos y el chat no se pone en espera, el sistema cambia automáticamente el estado del chat a **Sin asignar**.

Asignar sesiones de chat a uno mismo

Puede asignarse a sí mismo sesiones de chat que estén **Sin asignar** o **Asignadas a otros**.

Para asignarse una sesión de chat a usted mismo

© Acronis International GmbH, 2003-2025

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Localice la sesión de chat que desea reasignar y haga clic en ella.
3. Haga clic en **Asignármelo**.
   La sesión de chat se ha asignado a usted. Ahora puede enviar mensajes en este chat.

Nota
Si está desconectado o alejado de la consola durante 15 minutos y el chat no se pone en espera, el sistema cambia automáticamente el estado del chat a **Sin asignar**.

Reasignar sesiones de chat

Puede reasignar sesiones de chat para asegurarse de que el técnico más adecuado las maneje.

- Cuando se anula la asignación de una sesión de chat.
- Cuando desee cambiar el administrador de una sesión de chat asignada.

Los administradores de partners pueden reasignar una sesión de chat a un administrador del mismo inquilino del partner o a un administrador de un inquilino de cliente directo (si el modo de gestión del cliente es **Gestionado por el proveedor de servicios**).

Los administradores de clientes pueden reasignar una sesión de chat activa a otro administrador del mismo inquilino de cliente o sus unidades.

Los administradores de la unidad pueden reasignar una sesión de chat activa a otro administrador de la misma unidad.

Para reasignar un chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Localice la sesión de chat que desea reasignar y haga clic en ella.
3. Haga clic en el icono de puntos suspensivos (...) y en **Reasignar**.
4. En el cuadro de diálogo **Reasignar chat**, seleccione el administrador al que desea asignar la sesión de chat y haga clic en **Reasignar**.
   La sesión de chat se reasigna y ya no puede enviar mensajes en ella. Se muestra un mensaje del sistema sobre la reasignación tanto a los administradores como al usuario remoto.

Exportar chats

El historial de chats se almacena durante 180 días. Puede descargar chats importantes o partes de chats y guardarlos como archivos `.txt` en su equipo local.

Para exportar un chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Localice el chat que desee exportar y haga clic en él.
3. Haga clic en el icono de puntos suspensivos (...) y, luego, en **Exportar**.

© Acronis International GmbH, 2003-2025

4. En el cuadro de diálogo **Exportar chat**, realice una de las siguientes acciones:
   - Para exportar el historial completo del chat, seleccione **Exportar todo el chat**.
   - Para exportar el historial del chat para un período especificado, haga clic en **Exportar chat para el siguiente período** y luego seleccione un período predefinido (**Último día**, **Última semana**, **Último mes** o **Últimos 6 meses**) o un período personalizado.
5. Haga clic en **Exportar**.
   Se guarda un archivo `.txt` con el historial del chat en su equipo local, en la carpeta de descarga predeterminada.

Filtrar sesiones de chat

Puede filtrar la lista de sesiones de chat que se muestran en la página **Chat** y ver solo las sesiones de chat con usuarios remotos específicos.

Para filtrar sesiones de chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Para filtrar las sesiones de chat en la lista por usuarios remotos, haga clic en **Filtrar**, seleccione los usuarios remotos y, a continuación, haga clic en **Aplicar**.
   En la pantalla solo se enumeran las sesiones de chat con los usuarios que seleccionó.

Buscar mensajes en sesiones de chat

Puede buscar ciertos mensajes o palabras clave en las sesiones de chat o ver el historial de chat de una fecha específica.

Búsqueda en una sola sesión de chat

Para buscar en una única sesión de chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Haga clic en la sesión de chat en la que desee realizar la búsqueda.
3. Haga clic en el icono de bucle.
4. [Opcional] Para ver el historial de chat de una fecha específica, haga clic en el icono del calendario y, a continuación, seleccione la fecha.

   Nota
   Solo las fechas para las que hay un historial de chat disponible están habilitadas para su selección.

   El sistema muestra el historial de chat desde la fecha que seleccionó.
5. En el campo de búsqueda, escriba la palabra clave o el mensaje que desea encontrar.
   El sistema muestra el número de resultados que coinciden con la consulta de búsqueda. Puede utilizar las flechas para ir al siguiente o al anterior resultado.

Búsqueda en múltiples sesiones de chat

© Acronis International GmbH, 2003-2025

Para buscar en varias sesiones de chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. En el campo de búsqueda, escriba la cadena, palabra clave o mensaje que desee encontrar.
   La lista de chats muestra solo las sesiones con mensajes que coinciden con la búsqueda.

Acciones adicionales con las sesiones de chat

Dependiendo del estado de una sesión de chat, puede realizar las siguientes acciones adicionales: poner en espera, reanudar, finalizar, volver a abrir, acciones de carga de trabajo remota.

Poner en espera

Puede pausar temporalmente una sesión de chat activa cuando necesite más tiempo para responder. Por ejemplo, para encontrar la solución al problema del usuario.

Para poner una sesión de chat en espera

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Haga clic en el chat activo que desea poner en espera.
3. Haga clic en el botón de puntos suspensivos (...) y luego en **Poner en espera**.
   La sesión de chat se pone en espera. La etiqueta **En espera** se muestra para este chat en la lista de chats.

Reanudar

Puede reanudar una sesión de chat que se haya puesto en espera y continuar la conversación con el usuario remoto.

Para reanudar una sesión de chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Haga clic en el chat que desea reanudar y, a continuación, en **Reanudar chat**.
   La sesión de chat se reanuda. Puede continuar chateando con el usuario remoto.

Finalizar chat

Puede finalizar una sesión de chat activa con un usuario remoto en cualquier momento. El sistema guardará el historial de chat y notificará al usuario remoto que el chat se cerró.

Para finalizar una sesión de chat

1. En la consola de Cyber Protect, vaya a **Chat**.
2. Haga clic en el chat activo que desea finalizar.
3. Haga clic en **Finalizar chat**.
   La sesión de chat se cierra. El estado del chat cambia a **Cerrado** y en la pantalla de **Chats**, el chat se mueve de la lista de chats **Asignados a mí** a la de **Cerrados**.

Volver a abrir

© Acronis International GmbH, 2003-2025

Puede volver a abrir una sesión de chat cerrada y continuar la conversación con el usuario remoto. Todos los mensajes de las sesiones de chat anteriores se muestran en el hilo.

Para volver a abrir una sesión de chat cerrada

1. En la consola de Cyber Protect, vaya a **Chat**.
2. En la lista de chats **Cerrados**, haga clic en el chat cerrado que desea volver a abrir.
3. Haga clic en **Reabrir chat**.
   La sesión de chat se vuelve a abrir. El estado del chat cambia a **Asignado a mí** y en la pantalla de **Chats**, el chat se mueve de la lista de chats **Cerrados** a la de **Asignados a mí**.

Acciones remotas

Desde **Chats**, puede realizar acciones remotas en sus cargas de trabajo gestionadas o acceder a varias pantallas.

Requisitos previos

Connect Client está instalado en el equipo desde el que ha iniciado sesión en la consola de Cyber Protect.

Para ejecutar una acción remota en una carga de trabajo

1. En la consola de Cyber Protect, vaya a **Chat**.
2. En la lista de chats, haga clic en una sesión de chat con la carga de trabajo en la que desea realizar la acción.
3. Haga clic en el icono de puntos suspensivos (...) después del nombre de la carga de trabajo y haga clic en la opción que corresponda a la acción que desea realizar.

Opción	Descripción
Conectar	Utilice esta opción para conectarse a la carga de trabajo remota.
Transferir archivos	Utilice esta opción para transferir archivos a la carga de trabajo remota.
Reiniciar	Utilice esta opción para reiniciar la carga de trabajo remota.
Parche	Utilice esta opción para aplicar un parche a la carga de trabajo remota.
Ir a carga de trabajo	Al hacer clic en esta acción, se muestran las siguientes opciones: • **Detalles** • **Inventario** • **Supervisión** • **Planes** • **Alertas** • **Actividades**
Detalles	Esta opción se vuelve visible cuando hace clic en **Ir a carga de trabajo**.

© Acronis International GmbH, 2003-2025

Opción	Descripción
	Utilice esta opción para ir a los detalles de la carga de trabajo.
Inventario	Esta opción se vuelve visible cuando hace clic en **Ir a carga de trabajo**. Utilice esta opción para ir a la pestaña **Inventario** > **Hardware** de los detalles de la carga de trabajo.
Supervisión	Esta opción se vuelve visible cuando hace clic en **Ir a carga de trabajo**. Utilice esta opción para ir a la pestaña **Supervisión** de los detalles de la carga de trabajo.
Planes	Esta opción se vuelve visible cuando hace clic en **Ir a carga de trabajo**. Utilice esta opción para ir a la pestaña **Planes** de los detalles de la carga de trabajo.
Alertas	Esta opción se vuelve visible cuando hace clic en **Ir a carga de trabajo**. Utilice esta opción para ir a la pestaña **Alertas** de los detalles de la carga de trabajo.
Actividades	Esta opción se vuelve visible cuando hace clic en **Ir a carga de trabajo**. Utilice esta opción para ir a la pestaña **Actividades** de los detalles de la carga de trabajo.

Acciones adicionales con los mensajes de chat

En las sesiones de chat activas, puede editar o eliminar los mensajes que envió al usuario remoto.

Editar mensaje

Puede editar cualquier mensaje que haya enviado en la sesión de chat.

Para editar un mensaje en la sesión de chat

1. En la ventana del chat, localice el mensaje que desea editar.
2. Pase el ratón sobre el mensaje y haga clic en el icono de lápiz que aparece.
3. Edite el mensaje y presione **Intro**.
   Los cambios se guardan. El mensaje se etiqueta como **Editado**.

Eliminar mensaje

Puede eliminar cualquier mensaje que haya enviado en el chat.

Para eliminar un mensaje en la sesión de chat

1. En la ventana del chat, localice el mensaje que desea eliminar.
2. Pase el ratón sobre el mensaje y haga clic en el icono de la papelera que aparece.
3. Haga clic en **Eliminar** en la ventana de confirmación.

© Acronis International GmbH, 2003-2025

El mensaje se elimina del chat y ya no es visible. El sistema muestra la hora de la eliminación y su nombre.

© Acronis International GmbH, 2003-2025

Supervisión del estado y el rendimiento de las cargas de trabajo

Puede supervisar los parámetros del sistema y el estado de las cargas de trabajo de su organización. Si un parámetro está fuera de la normal, se le notificará inmediatamente y podrá resolver el problema rápidamente. También puede configurar alertas personalizadas y acciones de respuesta automáticas. Estas acciones se ejecutarán de forma automática para resolver anomalías en el comportamiento de las cargas de trabajo.

Nota
La funcionalidad de supervisión requiere la instalación de la versión 15.0.35324 o posterior del agente de Protección en las cargas de trabajo.

Planes de supervisión

Para iniciar la supervisión de los parámetros de rendimiento, hardware, software, sistema y seguridad de sus cargas de trabajo gestionadas, aplique un plan de supervisión en estas. Los planes de supervisión consisten en diferentes monitores que puede habilitar y configurar. Algunos monitores admiten el tipo de supervisión basado en anomalías. Para obtener más información acerca de los planes de supervisión, consulte "Planes de supervisión" (p. 1545). Para obtener más información acerca de los monitores disponibles que puede configurar en los planes de supervisión, consulte "Monitores configurables" (p. 1508).

Si el agente no puede recopilar datos de una carga de trabajo por algún motivo, el sistema generará una alerta.

Tipos de supervisión

Debe configurar el tipo de supervisión para cada monitor que habilite en el plan. El tipo de supervisión determina el algoritmo que el monitor utilizará para estimar el comportamiento normal y las desviación de la carga de trabajo. Hay dos tipos de supervisión: basada en umbrales y basada en anomalías. Algunos monitores admiten solo el tipo de supervisión basado en umbrales.

La supervisión basada en umbrales hace un seguimiento de los valores de los parámetros para ver si están por encima o por debajo del valor del umbral que configura. Con este tipo de supervisión, usted debe definir los valores de umbral correctos para las cargas de trabajo. El sistema determina el comportamiento normal según estos valores de umbral estáticos y sin tener en cuenta otras condiciones específicas que pueden causar el comportamiento. Por este motivo, la supervisión basada en umbrales podría ser menos precisa que la basada en anomalías.

La supervisión basada en anomalías utiliza modelos de aprendizaje automático para crear el patrón de comportamiento normal para una carga de trabajo y detectar comportamientos anormales. Para obtener más información, consulte "Supervisión basada en anomalías" (p. 1508).

© Acronis International GmbH, 2003-2025

Supervisión basada en anomalías

La supervisión basada en anomalías utiliza modelos de aprendizaje automático para crear el patrón de comportamiento normal para una carga de trabajo y detectar anomalías (picos inesperados en los datos de series temporales) en el comportamiento de la carga de trabajo. Cuando se activa este tipo de supervisión, el sistema crea un modelo y empieza a formarse a sí mismo y a ajustar el modelo a la carga de trabajo específica según los datos que recopila de la carga de trabajo. Esto significa que, al principio del periodo de formación, posiblemente los datos no sean completamente precisos. Para crear un modelo de confianza se necesitan al menos tres semanas de formación del modelo. A medida que el sistema recopile más datos y analice los conjuntos de datos históricos, perfeccionará el modelo progresivamente y creará los umbrales dinámicos superior e inferior para cada métrica de la carga de trabajo. Este tipo de supervisión es más flexible en comparación a la basada en umbrales, ya que el sistema supervisa los valores de los parámetros y su contexto. Por ejemplo, puede ser normal que una carga de trabajo específica tenga una carga mayor a determinadas horas del día. Un tipo de supervisión basada en umbrales lo interpretaría erróneamente como un comportamiento anómalo y activaría una alerta.

Puede restablecer los modelos de aprendizaje automático de una carga de trabajo. En este caso, el sistema eliminará todos los datos y modelos de los monitores aplicados a la carga de trabajo. Para obtener más información, consulte "Restablecimiento de los modelos de aprendizaje automático" (p. 1555).

Plataformas compatibles con la supervisión

La función de supervisión es compatible con los siguientes sistemas operativos.

Versiones de Windows compatibles	Versiones de macOS compatibles
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura) • macOS 14.x (Sonoma) • macOS 15.x (Sequoia)

Monitores configurables

La funcionalidad de supervisión es compatible con los siguientes monitores, divididos en seis categorías: hardware, rendimiento, software, sistema, seguridad y personalizado.

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
Hardware					
Espacio de disco	Supervisa el espacio libre en una unidad específica de la carga de trabajo.	Windows macOS	1 minuto	Sí	Protección estándar (modo de licencia basado en servicios) Seguridad y RMM (modo de licencia basado en soluciones)
Temperatura de CPU	Supervisa la temperatura de la CPU.	Windows macOS	30 seg	Sí	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Temperatura de GPU	Supervisa la temperatura de la GPU.	Windows macOS	30 seg	Sí	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Cambios del hardware	Supervisa los cambios de hardware, como añadir,	Windows macOS	24 horas	No	Protección estándar (modo de licencia

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
	eliminar o sustituir hardware en una carga de trabajo				basado en servicios) Seguridad y RMM (modo de licencia basado en soluciones)
Rendimiento					
Uso de la CPU	Supervisa el uso total de la CPU (por todas las CPU de la carga de trabajo).	Windows macOS	30 seg	Sí	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Uso de la memoria	Supervisa el uso de la memoria total (por todas las ranuras de memoria de la carga de trabajo).	Windows macOS	30 seg	Sí	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Velocidad de transferencia del disco	Supervisa la velocidad de lectura y escritura de cada disco físico de la carga de trabajo.	Windows macOS	30 seg	Sí	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
					basado en servicios)
Uso de la red	Supervisa el tráfico de entrada y salida para cada adaptador de red de la carga de trabajo.	Windows macOS	30 seg	Sí	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Uso de la CPU por proceso	Supervisa el uso que hace determinado proceso de la CPU.	Windows macOS	30 seg	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Uso de la memoria por proceso	Supervisa el uso de la memoria del proceso seleccionado.	Windows macOS	30 seg	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Velocidad de transferencia del disco por proceso	Supervisa la velocidad de lectura y escritura del	Windows macOS	30 seg	No	Seguridad y RMM (modo de licencia basado en

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
	proceso seleccionado.				soluciones) Servicio RMM (modo de licencia basado en servicios)
Uso de la red por proceso	Supervisa el tráfico de entrada y salida del proceso seleccionado.	Windows macOS	30 seg	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Software					
Estado del servicio de Windows	Supervisa el estado del servicio de Windows seleccionado (En ejecución o detenido).	Windows	30 seg	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Estado del proceso	Supervisa el estado del proceso seleccionado (En ejecución o detenido).	Windows macOS	30 seg	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
					servicios)
Software instalado	Supervisa la instalación, actualización o eliminación de aplicaciones de software.	Windows macOS	24 horas	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Sistema					
Último reinicio del sistema	Supervisa cuándo se ha reiniciado la carga de trabajo.	Windows macOS	1 hora	No	Protección estándar (modo de licencia basado en servicios) Seguridad y RMM (modo de licencia basado en soluciones)
Registro de eventos de Windows	Supervisa los eventos específicos de datos esenciales para el negocio en los registros de eventos de Windows.	Windows	10 min	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Tamaño de archivos y carpetas	Supervisa el tamaño total de los archivos o	Windows macOS	10 min	No	Protección estándar

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
	carpetas seleccionados.				(modo de licencia basado en servicios) Seguridad y RMM (modo de licencia basado en soluciones)
Seguridad					
Estado de Windows Update	Supervisa el estado de actualización de Windows de la carga de trabajo y si se han instalado las actualizaciones más recientes.	Windows	15 min	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Estado del cortafuegos	Supervisa el estado del cortafuegos integrado o de terceros que está instalado en la carga de trabajo.	Windows macOS	5 min	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Estado de software antimalware	Supervisa el estado del software antimalware integrado o de terceros que	Windows macOS	5 min	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM

© Acronis International GmbH, 2003-2025

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad
	está instalado en la carga de trabajo.				(modo de licencia basado en servicios)
Error al iniciar sesión	Supervisa los intentos de inicio de sesión sin éxito de la carga de trabajo.	Windows	1 hora	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Estado de AutoRun	Supervisa si la función AutoRun está activada en el soporte de almacenamiento extraíble.	Windows	1 hora	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)
Personalizado					
Personalizado	Supervisa los objetos personalizados mediante la ejecución de secuencias de comandos.	Windows macOS	personalizado	No	Seguridad y RMM (modo de licencia basado en soluciones) Servicio RMM (modo de licencia basado en servicios)

© Acronis International GmbH, 2003-2025

Configuración del monitor de espacio en disco

Espacio en disco supervisa el espacio libre en una unidad específica de la carga de trabajo.

Nota
A la hora de calcular el espacio, el monitor utiliza bytes binarios (1024 bytes por KB, 1024 KB por MB y 1024 MB por GB) para las cargas de trabajo de Windows y macOS.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Dispositivo	La unidad que quiere supervisar. Los valores disponibles son los siguientes: • **Unidad del sistema**: Este es el valor predeterminado. Esta es la unidad o partición en un ordenador donde se instala el sistema operativo (SO). En los sistemas Windows, la unidad del sistema es normalmente la unidad C: de forma predeterminada, pero esto puede variar según la configuración. • **Cualquier unidad**
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Menos de**: Este es el valor predeterminado. • **Menor o igual que**
Umbral de espacio libre en disco	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 20.
Incluir unidades extraíbles	Este parámetro está disponible si el valor **Dispositivo** es **Cualquier unidad**. Seleccione este parámetro si desea añadir unidades extraíbles, como unidades flash USB, para la supervisión. De manera predeterminada, se deshabilita la configuración.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	predeterminado es 30.
Supervisión basada en anomalías	
Dispositivo	La unidad que quiere supervisar. Los valores disponibles son los siguientes: • **Unidad del sistema**: Este es el valor predeterminado. Esta es la unidad o partición en un ordenador donde se instala el sistema operativo (SO). En los sistemas Windows, la unidad del sistema es normalmente la unidad C: de forma predeterminada, pero esto puede variar según la configuración. • **Cualquier unidad**
Periodo de entrenamiento del modelo	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. El valor predeterminado es 30 minutos.

Configuración de la supervisión de temperatura de la CPU

La temperatura de la CPU supervisa la temperatura de la CPU de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Se ha excedido la temperatura de la CPU (°C)	El valor máximo del parámetro supervisado. Si se supera el valor, el sistema genera una alerta. Escriba un valor entero (°C). El valor predeterminado es 80.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Periodo de entrenamiento del	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los

© Acronis International GmbH, 2003-2025

Configuración	Descripción
modelo	agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración de la supervisión de temperatura de la GPU

La temperatura de la GPU supervisa la temperatura de la GPU de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Se ha excedido la temperatura de la GPU	El valor máximo del parámetro supervisado. Si se supera el valor, el sistema detecta una anomalía. Escriba un valor entero (°C). El valor predeterminado es 80.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Periodo de entrenamiento del modelo	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración del monitor de cambios de hardware

Cambios del hardware supervisan los cambios de hardware, como añadir, eliminar o sustituir hardware en una carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Componentes del hardware	Seleccione uno o varios componentes de hardware en los que desee supervisar los cambios. Los valores disponibles son los siguientes: • **Todos**: Este es el valor predeterminado.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	• **Placa base** • **CPU** • **RAM** • **Disco** • **GPU** • **Adaptador de red**
Qué supervisar	Especifique los cambios para los que desee supervisar los componentes de hardware seleccionados. Puede seleccionar varios elementos de la lista. Los valores disponibles son los siguientes: • **Cualquier cambio**: Este es el valor predeterminado. • **Componentes recién añadidos** • **Componentes remplazados** • **Componentes eliminados**

Configuración de la supervisión del uso de la CPU

El **Uso de la CPU** supervisa el uso total de la CPU (uso del procesador) de la carga de trabajo. Si la carga de trabajo tiene varias CPU, el uso total de la CPU será la suma del uso de la CPU para cada CPU.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de uso de la CPU	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 90.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Periodo de entrenamiento del modelo	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración de la supervisión del uso de la memoria

Uso de memoria supervisa el uso de la memoria total de todos los módulos de memoria de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de uso de la memoria	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 90.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Supervisión basada en anomalías	
Periodo de entrenamiento del modelo	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes:

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	• **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 30 minutos.

Configuración de la supervisión de la velocidad de transferencia del disco

Velocidad de transferencia de disco supervisa la velocidad de lectura y escritura de cada disco físico de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Qué supervisar	Seleccione la velocidad que quiere supervisar. Los valores disponibles son los siguientes: • **Velocidad de lectura y velocidad de escritura**. Este es el valor predeterminado. • **Velocidad de lectura** • **Velocidad de escritura**
Operador de velocidad de lectura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de lectura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Periodo de tiempo de velocidad de lectura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador de velocidad de escritura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de escritura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de velocidad de escritura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Periodo de entrenamiento del modelo	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Qué supervisar	Seleccione la velocidad que quiere supervisar. Los valores disponibles son los siguientes:

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	• **Velocidad de lectura y velocidad de escritura**. Este es el valor predeterminado. • **Velocidad de lectura** • **Velocidad de escritura**
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía (velocidad de lectura)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Duración de la anomalía (velocidad de escritura)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.

Configuración del monitor de uso de red

El **uso de red** supervisa el tráfico de entrada y salida para cada adaptador de red de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Dirección del tráfico	La dirección del tráfico que quiere supervisar. Los valores disponibles son los siguientes: • **Tráfico entrante y saliente**. Este es el valor predeterminado. • **Tráfico de entrada** • **Tráfico de salida**
Operador de tráfico de entrada	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de entrada	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de entrada	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador del tráfico de salida	El operador es una función condicional que define cómo definir el rendimiento del parámetro.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de salida	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de salida	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Periodo de entrenamiento del modelo	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Dirección del tráfico	• **Tráfico entrante y saliente**. Este es el valor predeterminado. • **Tráfico de entrada** • **Tráfico de salida**
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación:

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía (de entrada)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.
Duración de la anomalía (de salida)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.

Configuración del uso de la CPU por supervisión del proceso

El **uso de la CPU por proceso** supervisa el uso de la CPU del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones.

© Acronis International GmbH, 2003-2025

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	Nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 90.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración del uso de la memoria por supervisión del proceso

El **uso de la memoria por proceso** supervisa el uso de la memoria del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones.

Nota
Los agentes utilizan todo el conjunto de trabajo del proceso (privado y compartido) para calcular el tamaño del uso de memoria por proceso. Por este motivo, el tamaño del uso de memoria que indica el widget puede diferir del que se muestra en el Administrador de tareas de Windows (conjunto de trabajo privado).

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	Nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb). El valor predeterminado es 1.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración de la supervisión de la velocidad de transferencia del disco por proceso

Velocidad de transferencia de disco por proceso supervisa la velocidad de lectura y escritura del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	El nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Qué supervisar	La velocidad que quiere supervisar. Los valores disponibles son los siguientes: • **Velocidad de lectura y velocidad de escritura**. Este es el valor predeterminado. • **Velocidad de lectura** • **Velocidad de escritura**
Operador de velocidad de lectura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que**

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	• **Menos de** • **Menor o igual que**
Umbral de velocidad de lectura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de velocidad de lectura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador de velocidad de escritura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de escritura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de velocidad de escritura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración del uso de la red por supervisión del proceso

Uso de la red por proceso supervisa el tráfico de entrada y salida del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones en todas las instancias.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	Nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Dirección del	La dirección del tráfico que quiere supervisar.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
tráfico	Los valores disponibles son los siguientes: • **Tráfico entrante y saliente**. Este es el valor predeterminado. • **Tráfico de entrada** • **Tráfico de salida**
Operador de tráfico de entrada	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de entrada	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de entrada	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador del tráfico de salida	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de salida	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de salida	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

© Acronis International GmbH, 2003-2025

Configuración de la supervisión del estado del servicio de Windows

Estado del servicio de Windows supervisa si el servicio de evento de Windows seleccionado se está ejecutando o está detenido.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del servicio	El nombre del servicio de Windows que quiere supervisar. Puede seleccionar un nombre de servicio de la lista de servicios de Windows. La lista se rellena con todos los agentes del inquilino después de que se complete correctamente el análisis de inventario de software en las cargas de trabajo. También puede añadir un nombre de servicio que no figure en la lista. Esta es la única opción disponible si no se realiza el análisis de inventario de software en las cargas de trabajo.
Estado del servicio	Si el servicio se encuentra en el estado seleccionado, el sistema generará un evento. Los valores disponibles son los siguientes: • **En ejecución** • **Detenido**: Este es el valor predeterminado.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 1.

Configuración del monitor de estado del proceso

El **estado del proceso** supervisa si el proceso seleccionado se está ejecutando o está detenido. Si hay varias instancias del mismo proceso, el sistema supervisará cada instancia del proceso y generará la alerta cuando se cumplan las condiciones en todas las instancias del proceso.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	El nombre del proceso que quiere supervisar. Especifique el nombre de un archivo ejecutable sin la extensión.
Estado del proceso	Si el proceso está en el estado seleccionado, el sistema generará un evento. Los valores disponibles son los siguientes: • **En ejecución** • **Detenido**: Este es el valor predeterminado.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 1.

Configuración del monitor de Software instalado

El monitor **Software instalado** supervisa la instalación, actualización o eliminación de aplicaciones de software en la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Qué software supervisar	Especifique el software que quiere supervisar. Los valores disponibles son los siguientes: • **Cualquier software**: Este es el valor predeterminado. • **Software específico**
Nombres del software	Este parámetro está disponible si selecciona el valor **Software específico** para **Qué software supervisar**. Escriba el nombre de una o varias aplicaciones de software. Puede seleccionar un nombre de aplicación de software de la lista de servicios de Windows. La lista se rellena con todos los agentes del inquilino después de que se complete correctamente el análisis de inventario de software en las cargas de trabajo. También puede añadir un nombre de aplicación de software que no figure en la lista. Esta es la única opción disponible si no se realiza el análisis de inventario de software en las cargas de trabajo.
Estado de instalación	Especifique si desea supervisar software instalado, no instalado o actualizado. Los valores disponibles son los siguientes: • **Instalado**: Este es el valor predeterminado. Si selecciona este valor, el monitor generará una alerta cuando se instale una nueva aplicación de software en la carga de trabajo. • **Actualizado**: Si selecciona este valor, el monitor generará una alerta cuando se actualice una aplicación de software. • **No instalado**: si selecciona este valor, el monitor generará una alerta cuando se desinstale una aplicación de software o no esté disponible en la carga de trabajo.

© Acronis International GmbH, 2003-2025

Configuración de la supervisión del último reinicio del sistema

Último reinicio del sistema supervisa cuando la carga de trabajo se ha reiniciado por última vez.

Puede configurar el siguiente parámetro para el monitor:

Configuración	Descripción
La carga de trabajo no se ha reiniciado durante	El periodo (número de días) desde el último reinicio de la carga de trabajo. Si la carga de trabajo no se ha reiniciado durante un periodo superior al que ha especificado, el sistema generará una alerta. Escriba un valor entero entre 1 y 180 (días). El valor predeterminado es 30.

Configuración de la supervisión del registro de eventos de Windows

Registro de eventos de Windows supervisa los eventos específicos de datos esenciales para el negocio en los registros de eventos de Windows.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del registro de eventos	Seleccione un registro de eventos específico en una lista de registros de eventos de Windows que estén disponibles en el Visor de eventos de Windows. Los valores disponibles son los siguientes: • **Cualquiera** —Este es el valor predeterminado. • **Aplicación** • **Seguridad** • **Sistema**
Origen del evento	Nombre del origen del evento Puede seleccionar el valor de una lista de orígenes del evento que se recopilan de todos los agentes del inquilino o introducir un nuevo nombre de origen manualmente. Si el análisis de inventario de software está deshabilitado en el inquilino, la lista de orígenes del evento estará vacía.
Modo de coincidencia	En este campo, puede especificar si quiere conectar los ajustes de **ID de los eventos**, **Tipo de evento** y **Descripción del evento** utilizando el operador **Cualquiera** o **Todos**. Los valores disponibles son los siguientes: • **Cualquiera**:Este es el valor predeterminado. Se generará una alerta solo si coincide alguno de los criterios seleccionados. • **Todos**: se generará una alerta si coinciden todos los criterios

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	seleccionados.
ID de los eventos	Escriba uno o varios ID de eventos, separados por una coma Si el sistema encuentra en el registro de eventos alguno de los códigos de evento que ha introducido en este campo, se generará una alerta.
Tipo de evento	Seleccione uno o más tipos de evento que desee supervisar. Los valores disponibles son los siguientes: • **Cualquiera** — Este es el valor predeterminado. • **Error** • **Advertencia** • **Información** • **Auditoría correcta** • **Fallo de auditoría**
Descripción del evento	Frases o palabras clave específicas de la descripción del evento que quiera buscar. Cada frase o palabra clave que escriba debe estar entre comillas y separadas por una coma. Si el sistema encuentra alguna de las frases o palabras clave que ha introducido, se generará una alerta.
Número de ocurrencias	El número mínimo de ocurrencias en el registro que debe tener un evento durante el periodo de tiempo especificado para que el sistema genere una alerta. Escriba un valor entero entre 1 y 1000.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero y seleccione la unidad: minutos o horas. El valor predeterminado es 60 minutos.

Configuración de la supervisión del tamaño de archivos y carpetas

Tamaño de archivos y carpetas supervisa el tamaño total de los archivos o carpetas seleccionados.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Archivos o carpetas para supervisar	Las rutas de los archivos o las carpetas que quiere supervisar. También puede especificar los archivos o las carpetas que quiere excluir de la supervisión. Puede utilizar los siguientes caracteres comodín: • *: para cero o más caracteres en un nombre de archivo o carpeta

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	• ?: para exactamente un carácter en un nombre de archivo o carpeta Para las cargas de trabajo de Windows: • La ruta completa debe empezar por la letra de la unidad seguida del separador :\. • Puede utilizar la barra diagonal o inversa como un carácter separador de ruta. • El nombre del archivo o la carpeta no debe acabar en un espacio o un punto. Para las cargas de trabajo de macOS: • La ruta completa debe empezar por el directorio raíz. • Puede utilizar la barra diagonal como un carácter separador de ruta. • El nombre del archivo o la carpeta no debe acabar en un espacio o un punto.
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Menos de**
Valor del umbral	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (MB).
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 10-60 (min). El valor predeterminado es 10.

Configuración de la supervisión del estado de actualización de Windows

Estado de Windows Update supervisa el estado de actualización de Windows de la carga de trabajo y si se han instalado las actualizaciones más recientes.

Si habilita esta supervisión, el sistema generará una alerta en los siguientes casos.

- La actualización de Windows está deshabilitada en la carga de trabajo.
- La actualización de Windows está habilitada en la carga de trabajo, pero no se han instalado las actualizaciones más recientes.

© Acronis International GmbH, 2003-2025

Configuración de la supervisión del estado del cortafuegos

El estado del cortafuegos supervisa el cortafuegos integrado o de terceros que está instalado en la carga de trabajo.

Si habilita esta supervisión, el sistema generará una alerta en los siguientes casos.

- El cortafuegos integrado en el SO (cortafuegos de Windows Defender o cortafuegos de macOS) está deshabilitado y no se ejecuta ningún cortafuegos de terceros.
- El cortafuegos de Windows Defender está deshabilitado para las redes públicas.
- El cortafuegos de Windows Defender está deshabilitado para las redes privadas.
- El cortafuegos de Windows Defender está deshabilitado para las redes de dominio.

Configuración del monitor de inicios de sesión fallidos

Inicios de sesión fallidos supervisa los intentos de inicio de sesión sin éxito de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Umbral de intentos de inicio de sesión fallidos	El valor del umbral determina los límites del rendimiento normal del parámetro supervisado. Cuando se supera el valor del umbral, el valor está fuera de la norma. Escriba un valor entero. El valor predeterminado es 60.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero entre 1 y 24 y seleccione una unidad: horas o días. El valor predeterminado es 12.

Configuración de la supervisión del estado del software antimalware

El **estado del software antimalware** supervisa el software antimalware integrado o de terceros que está instalado en la carga de trabajo.

Si habilita esta supervisión, el sistema generará una alerta cuando identifique una de las siguientes condiciones.

- El software antimalware no está instalado en la carga de trabajo.
- El software antimalware está instalado, pero no se está ejecutando.
- El software antimalware está instalado y se está ejecutando, pero las definiciones de malware no están actualizadas.

© Acronis International GmbH, 2003-2025

Nota

Esta condición se comprueba para los sistemas operativos de Windows y Windows Server.

Sistema operativo	Software antimalware admitido
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton antivirus • SentinelOne • Endpoint Security de Trend Micro con Apex One • Worry-Free Business de Trend Micro • McAfee Endpoint Security • McAfee Endpoint Protection para SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security

© Acronis International GmbH, 2003-2025

Sistema operativo	Software antimalware admitido
	Nota Puede que el monitor funcione con otras aplicaciones antimalware, pero no se lo podemos asegurar.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus para Mac • Sophos Home • Sophos Endpoint Protection • Avast Security para Mac • AVG AntiVirus para Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus para Mac • Comodo Antivirus para Mac • K7 Antivirus para Mac • Vipre Advanced Security • Total AV para Mac **Nota** Puede que el monitor funcione con otras aplicaciones antimalware, pero no se lo podemos asegurar.

Configuración de la supervisión del estado de la función AutoRun

El **estado de la función AutoRun** supervisa si la función AutoRun está activada para el soporte extraíble.

Por motivos de seguridad, recomendamos deshabilitar la función AutoRun para el dispositivo extraíble en la carga de trabajo. Si la función está habilitada, el sistema generará una alerta.

Configuración del monitor personalizado

Los monitores **personalizados** personalizan los objetos mediante la ejecución de una secuencia de comandos.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Secuencia de comandos que ejecutar	Lista de secuencias de comandos predefinidas desde el repositorio de secuencias de comandos.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
Planificación	La hora a la que se ejecuta la secuencia de comandos y, de forma opcional, otras condiciones que deberían cumplirse para ejecutar la secuencia de comandos. Los valores disponibles son los siguientes: • **Planificar por hora**: la secuencia de comandos se ejecutará a la hora, el día, la semana o el mes que especifique. Este es el valor predeterminado. **Tipo de planificación**: **Cada hora**, **Diaria** o **Mensual** **Ejecutar dentro de un intervalo de fechas**: un intervalo de tiempo en el que ejecutar la secuencia de comandos. • **Cuando el usuario inicia sesión en el sistema**: la secuencia de comandos se ejecutará cuando un usuario inicie sesión en la carga de trabajo. • **Cuando el usuario cierra sesión en el sistema**: la secuencia de comandos se ejecutará cuando un usuario cierre sesión en la carga de trabajo. • **Al iniciarse el sistema**: la secuencia de comandos se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la secuencia de comandos se ejecutará se apague el sistema. • **Cuando el sistema esté en línea**: la secuencia de comandos se ejecutará cuando la carga de trabajo esté disponible en línea. **Condiciones de inicio**: la tarea se ejecutará en un momento o evento específico solo si se cumple la condición. Cuando se seleccionan varias condiciones, deben cumplirse todas simultáneamente para que se inicie la tarea. De forma predeterminada, se selecciona la condición **Evitar el modo de suspensión o hibernación para iniciar una tarea programada**. **Si no se cumplen las condiciones de inicio, ejecute la tarea de todos modos después de**: esta condición está activada de forma predeterminada. El valor predeterminado es 1 hora.
Cuenta para ejecutar la secuencia de comandos	La cuenta en la que se ejecutará la secuencia de comandos. Los valores disponibles son los siguientes: • **Cuenta de sistema**: Este es el valor predeterminado. • **Cuenta con sesión iniciada actualmente**
Duración máxima	El periodo máximo durante el cual se puede ejecutar la secuencia de comandos en la carga de trabajo. Si la secuencia de comandos no se completa durante este periodo, la operación fallará.

© Acronis International GmbH, 2003-2025

Configuración	Descripción
	Escriba un valor entero entre 1 y 1440 (minutos). El valor predeterminado es 3 minutos.
Directiva de ejecución de PowerShell	La directiva de ejecución de PowerShell. Los valores disponibles son los siguientes: • **Undefined** • **AllSigned** • **Bypass**: Este es el valor predeterminado. • **RemoteSigned** • **Restricted** • **Unrestricted** Para obtener más información sobre estos valores, consulte la documentación de Microsoft.

Planes de supervisión

Los planes de supervisión son planes que aplica en sus cargas de trabajo gestionadas para habilitar y configurar la funcionalidad de supervisión.

Si no se aplica ningún plan de supervisión a una carga de trabajo, las características de supervisión no estarán disponibles para la carga de trabajo.

Nota
La disponibilidad de esta función y los ajustes que puede configurar en el plan de supervisión dependen de la licencia que tenga.

Crear un plan de supervisión

Puede crear un plan de supervisión y asignarle cargas de trabajo para configurar la funcionalidad de supervisión en las cargas de trabajo gestionadas.

Requisitos previos

La versión del agente que está instalada en la carga de trabajo es compatible con la funcionalidad de supervisión.

Pasos para crear un plan de supervisión

Desde Planes de supervisión

1. En la consola de Protección, vaya a **Gestión** > **Planes de supervisión**.
2. Cree un plan de supervisión mediante una de estas dos opciones:
   - Si no hay planes de supervisión en la lista, haga clic en **Crear**.
   - Si no hay planes de supervisión en la lista, haga clic en **Crear plan**.

© Acronis International GmbH, 2003-2025

3. En la ventana **Crear plan de supervisión**, dependiendo de la licencia de su inquilino, haga lo siguiente:
   - Si su inquilino utiliza la protección estándar (modo de licencia basado en servicios), los siguientes cuatro monitores se añadirán automáticamente al plan de supervisión: Espacio del disco, cambios de hardware, último reinicio del sistema y tamaño de archivos y carpetas.
   - Si el paquete RMM está habilitado para su inquilino (modo de licencia basado en servicios) o si está utilizando Seguridad y RMM (modo de licencia basado en soluciones), seleccione una de las opciones de la plantilla y, a continuación, haga clic en **Siguiente**.

Opción	Descripción
Recomendada	Seleccione esta opción para crear un plan de supervisión con la configuración de supervisión predeterminada.
Personalizado	Utilice esta opción para crear un plan de supervisión desde cero.

4. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Aceptar**.
5. [Opcional] Para añadir un monitor al plan, haga clic en **Añadir monitor**, en el monitor de la lista y en **Agregar**.

   Nota
   La configuración del monitor se completará automáticamente con los valores predeterminados. Puede añadir hasta 30 monitores a un plan de supervisión.

6. [Opcional] En la pantalla de parámetros de supervisión, cambie la configuración predeterminada del monitor y las alertas y haga clic en **Listo**.

   Nota
   Puede configurar diferentes parámetros para cada monitor. Para obtener más información, consulte "Monitores configurables" (p. 1508) y "Configuración de alertas de supervisión" (p. 1555).

7. [Opcional] Para eliminar un monitor, haga clic en el icono de la papelera y en **Eliminar**.
8. [Opcional] Pasos para añadir cargas de trabajo al plan:
   a. Haga clic en **Añadir cargas de trabajo**.
   b. Seleccione las cargas de trabajo y haga clic en **Agregar**.
   c. Si hay problemas de compatibilidad que desea resolver, siga el procedimiento descrito en "Resolver problemas de compatibilidad" (p. 258).
9. Haga clic en **Crear**.

Desde Todos los dispositivos

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que desee aplicar un plan de supervisión.

© Acronis International GmbH, 2003-2025

3. Haga clic en **Proteger**.
4. Según si el plan de supervisión se aplica a la carga de trabajo, haga lo siguiente:
   - Si un plan de supervisión ya se aplica a la carga de trabajo, haga clic en **Crear plan** y seleccione **Supervisión**.
   - Si no se aplica ningún plan de supervisión a la carga de trabajo, haga clic en **Agregar plan** y luego en **Crear plan** y seleccione **Supervisión**.
5. En la ventana **Crear plan de supervisión**, seleccione una de las opciones de plantilla y haga clic en **Siguiente**.

Opción	Descripción
Recomendada	Seleccione esta opción para crear un plan de supervisión con la configuración de supervisión predeterminada.
Personalizado	Utilice esta opción para crear un plan de supervisión desde cero.

6. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Aceptar**.
7. [Opcional] Si desea cambiar la configuración predeterminada del monitor y las alertas, configure los nuevos valores y haga clic en **Listo**.

   Nota
   Puede añadir hasta 30 monitores a un plan de supervisión.

8. [Opcional] En la pantalla de parámetros de supervisión, cambie la configuración predeterminada del monitor y las alertas y haga clic en **Listo**.

   Nota
   Puede configurar diferentes parámetros para cada monitor. Para obtener más información, consulte "Monitores configurables" (p. 1508) y "Configuración de alertas de supervisión" (p. 1555).

9. [Opcional] Para eliminar un monitor, haga clic en el icono de la papelera y en **Eliminar**.
10. Haga clic en **Crear**.

Añadir cargas de trabajo a los planes de supervisión

Según sus necesidades, puede añadir cargas de trabajo a un plan de supervisión después de crearlo.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- La versión del agente que está instalada en la carga de trabajo es compatible con la funcionalidad de supervisión.
- Al menos un plan de supervisión está disponible.

© Acronis International GmbH, 2003-2025

Pasos para añadir una carga de trabajo a un plan de supervisión

Desde Planes de supervisión

1. En la consola de Protección, vaya a **Gestión** > **Planes de supervisión**.
2. Haga clic en el plan de supervisión.
3. Según si el plan ya se ha aplicado a una carga de trabajo, haga lo siguiente:
   - Haga clic en **Añadir cargas de trabajo**, si el plan todavía no se ha aplicado a ninguna carga de trabajo.
   - Haga clic en **Gestionar cargas de trabajo**, si el plan se ha aplicado a alguna carga de trabajo.
4. Seleccione una carga de trabajo de la lista y haga clic en **Agregar**.
5. Haga clic en **Guardar**.
6. Si es necesario, haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Desde Todos los dispositivos

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que desee aplicar un plan de supervisión.
3. Haga clic en **Proteger**.
4. Busque el plan de supervisión al que desee añadir la carga de trabajo y haga clic en **Aplicar**.
5. Si es necesario, haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Revocación de planes de supervisión

Puede revocar un plan de supervisión desde una carga de trabajo donde se aplique el plan.

Requisitos previos

Al menos un plan de supervisión se aplica a la carga de trabajo.

Pasos para revocar el plan de supervisión

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo y en **Proteger**.
3. Haga clic en el icono **Más acciones** del plan de supervisión que desea revocar y, a continuación, en **Revocar**.

Configuración de las acciones de respuesta automática

Las medidas de respuesta automática en los eventos de alertas son medidas o acciones predefinidas que se activan automáticamente en respuesta a los incidentes o eventos detectados. El propósito de estas acciones es mitigar las posibles amenazas y reducir el daño.

© Acronis International GmbH, 2003-2025

Puede configurar una o varias medidas de respuesta automática en los eventos de alertas. El número máximo de medidas de respuesta automática por monitor son 20.

Pasos para configurar medidas de respuesta automática

1. En la consola de Protección, vaya a **Gestión** > **Planes de supervisión**.
2. Seleccione el plan de supervisión en el que quiere configurar las medidas de respuesta automática.
3. Seleccione el monitor en el que quiere configurar las medidas de respuesta automática, o, si aún no ha añadido ningún monitor, haga clic en **Añadir monitor**, haga clic en el monitor de la lista, haga clic en **Agregar** y, por último, seleccione el monitor.
4. Haga clic en el enlace junto a **Acciones de respuesta automática**.
5. En la ventana **Acciones de respuesta automática**, añada una o varias acciones de respuesta que se ejecutarán automáticamente cuando se active una alerta.
6. Configure cada una de las medidas de respuesta. Por ejemplo, si ha añadido la medida de respuesta **Iniciar un servicio de Windows**, haga lo siguiente:
   a. Junto a **Servicio de Windows**, haga clic en **Especificar**.
   b. En el campo **Servicio**, seleccione un servicio para iniciar una medida de respuesta.
   c. Haga clic en **Listo**.
7. En la lista con todas las medidas de respuesta añadidas, utilice las flechas hacia arriba y abajo o arrastre y suelte para establecer la secuencia de las medidas de respuesta.
8. Configure cómo gestionar las medidas de respuesta siguientes si falla la anterior. Seleccione una de las siguientes opciones:
   a. **Continuar con la medida de respuesta siguiente**.
   b. **No continuar con la medida de respuesta siguiente**.
9. Haga clic en **Listo**.

   Verá el número de medidas configuradas junto a la opción de **Acciones de respuesta automática** en el plan de supervisión. Puede modificar o eliminar estas medidas, así como añadir nuevas en cualquier momento.

La siguiente tabla enumera y describe todas las acciones de respuesta automática disponibles en la configuración del monitor.

Acción de respuesta automática	Descripción	SO compatibles
Ejecutar una secuencia de comandos	Si añade esta medida, puede: 1. Seleccionar una determinada secuencia de comandos para ejecutar en la carga de trabajo. 2. Especifique la cuenta con la que quiere ejecutar la secuencia de comandos. 3. Especifique la duración máxima de la	Windows y macOS

© Acronis International GmbH, 2003-2025

Acción de respuesta automática	Descripción	SO compatibles
	operación. 4. Especifique la directiva de ejecución de PowerShell. 5. Ejecutar una secuencia de comandos. **Nota** Para realizar esta acción, necesita la licencia RMM (modo de licencia basado en servicios) o Seguridad y RMM (modo de licencia basado en soluciones) para la carga de trabajo, si aún no se ha asignado. El sistema ejecutará la secuencia de comandos remota seleccionada con los parámetros especificados cuando se cumplan las condiciones.	
Reiniciar la carga de trabajo	Si añade esta medida el sistema reiniciará la carga de trabajo de forma remota cuando se cumplan las condiciones.	Windows y macOS
Detener el proceso	Si añade esta medida, puede especificar que se detenga el proceso cuando se introduzca manualmente el nombre del proceso. El sistema detendrá el proceso cuando se cumplan las condiciones.	Windows y macOS
Iniciar el servicio de Windows	Si añade esta medida, puede seleccionar qué servicio de Windows se debe iniciar en la lista dinámica de servicios que rellenan los agentes. El sistema iniciará el servicio cuando se cumplan las condiciones.	Windows
Detener el servicio de Windows	Si añade esta medida, puede seleccionar qué servicio de Windows se debe detener en la lista dinámica de servicios que rellenan los agentes. El sistema detendrá el servicio cuando se cumplan las condiciones.	Windows
Habilitar la actualización de Windows	Si añade esta medida, el sistema habilitará la actualización de Windows cuando se cumplan las condiciones. Esta acción solo está disponible en la	Windows

© Acronis International GmbH, 2003-2025

Acción de respuesta automática	Descripción	SO compatibles
	supervisión del estado de la actualización de Windows.	
Deshabilitar AutoRun en las unidades extraíbles	Si añade esta medida, el sistema deshabilitará la función AutoRun en los soportes de almacenamiento extraíbles para la carga de trabajo cuando se cumplan las condiciones. Esta acción solo está disponible en la supervisión del estado de la función Autorun.	Windows

Acciones adicionales con planes de supervisión

Desde la pantalla **Planes de supervisión**, puede realizar las siguientes acciones adicionales con los planes de supervisión: ver detalles, editar, ver las actividades, ver las alertas, renombrar, habilitar, deshabilitar, clonar, exportar, establecer como favorito, establecer como predeterminado y eliminar.

Ver detalles

Pasos para consultar los detalles de un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Ver detalles**.
3. [Opcional] Si desea consultar los detalles de un monitor habilitado en el plan, haga clic en el nombre del monitor.

Editar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para editar un plan

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Editar**.
3. [Opcional] Para eliminar un monitor del plan, haga clic en el icono de papelera de reciclaje situado a la derecha del nombre del monitor.
4. [Opcional] Para habilitar o deshabilitar un monitor del plan, utilice el conmutador que se encuentra junto al nombre del monitor.
5. [Opcional] Para editar los parámetros del monitor, siga los pasos siguientes:

© Acronis International GmbH, 2003-2025

a. Haga clic en el nombre del monitor.

b. Haga clic en la información general de los parámetros del monitor.

c. En la pantalla **Parámetros del monitor**, configure los parámetros y haga clic en **Listo**.

> **Nota**
> Puede configurar diferentes parámetros para cada monitor. Para obtener más información, consulte "Monitores configurables" (p. 1508) y "Configuración de alertas de supervisión" (p. 1555).

d. Cierre la pantalla y confirme los cambios.

6. [Opcional] Para añadir un monitor, haga clic en **Añadir monitor** y, a continuación, si es necesario, edite los parámetros según se indica en el paso anterior.
7. Haga clic en **Guardar**.

Actividades

Pasos para ver las actividades relacionadas con un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Actividades**.
3. Haga clic en una actividad para ver más información sobre ella.

Alertas

Pasos para ver las alertas

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Alertas**.

Cambiar nombre

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para cambiar el nombre de un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Cambiar nombre**.
3. Escriba el nuevo nombre del plan y haga clic en **Aceptar**.

Habilitar

Requisitos previos

© Acronis International GmbH, 2003-2025

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- El plan de supervisión se aplica al menos a una carga de trabajo.

Pasos para habilitar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Habilitar**.

Deshabilitar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para deshabilitar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Deshabilitar**.

Clonar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para clonar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Clonar**.
3. Haga clic en **Crear**.

Exportar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para exportar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Exportar**.
   La configuración del plan se exporta en formato JSON al equipo local.

Importar

Requisitos previos

© Acronis International GmbH, 2003-2025

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- Un archivo JSON con la configuración del plan está disponible en el equipo desde el que ha iniciado sesión en la consola.

Para importar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en **Importar plan**.
2. En la ventana que se abre, busque el archivo JSON.
3. Haga clic en el archivo y luego en **Abrir**.
   El plan de supervisión aparece en la pantalla. Ahora puede aplicarlo a las cargas de trabajo.

Eliminar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

Establecer como predeterminado

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para establecer un plan de supervisión como predeterminado

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Establecer como predeterminado**.
3. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla de **Planes de supervisión**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Agregar a favoritos

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para marcar un plan de supervisión como favorito

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Agregar a favoritos**.
   En la pantalla de **Planes de supervisión**, aparece un icono de estrella junto al nombre del plan.

© Acronis International GmbH, 2003-2025

Restablecimiento de los modelos de aprendizaje automático

Puede restablecer los modelos de una carga de trabajo cuando se vuelven obsoletos o dejan de ser válidos por algún motivo. Esta acción eliminará los modelos creados y los datos de la carga de trabajo que hayan recopilado los monitores con el tipo de supervisión basada en anomalías y, a continuación, iniciará la formación de los modelos de aprendizaje automático para la carga de trabajo desde cero.

Para restablecer los modelos de aprendizaje automático para una carga de trabajo

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en una carga de trabajo de la lista y, a continuación, en la pestaña **Detalles**.
3. En la sección **Restablecer los modelos de aprendizaje automático**, haga clic en **Restablecer**.
4. Vuelva a hacer clic en **Restablecer** en la ventana de confirmación.

Supervisión de alertas

Las alertas de supervisión se muestran en la consola de Protección y se envían por correo electrónico cuando el comportamiento supervisado de las cargas de trabajo está fuera de lo normal. Las alertas aseguran que se informe a los interesados lo antes posible cuando haya algún problema en el entorno de TI de la organización.

Nota
Para habilitar las alertas de supervisión a través del correo electrónico, debe configurar al menos una directiva de notificaciones por correo electrónico para el tipo de alerta correspondiente. Para obtener más información, consulte "Configurar directivas de notificaciones por correo electrónico" (p. 1563).

Configuración de alertas de supervisión

Puede configurar los parámetros de la alerta del monitor al añadir un monitor a un plan de supervisión o al editar un monitor que ya esté disponible en un plan de supervisión.

Pasos para configurar alertas de supervisión

1. En la ventana **Parámetros del monitor**, vaya a la sección **Generar alertas**.
2. En **Gravedad de la alerta**, seleccione la gravedad que corresponde a la prioridad de la alerta.

Opción	Descripción
Crítico	Estas alertas tienen la máxima prioridad y están relacionadas con problemas que son críticos para el funcionamiento de la carga de trabajo. Resuelva estos problemas lo antes posible.
Error	Una alerta de error es menos grave e indica que algo va mal o no se

© Acronis International GmbH, 2003-2025

Opción	Descripción
	comporta de forma normal. Resuelva los problemas a tiempo para evitar que den lugar a problemas más graves.
Advertencia	Una alerta de advertencia indica que existe una situación de la que debe ser consciente, pero es posible que aún no esté causando ningún problema. Resuelva estos problemas después de resolver los que están causando alertas críticas y de error. Este es el valor predeterminado.
Informativo	Estas alertas son las de menor prioridad. La gravedad informativa no indica un problema. Dichas alertas ofrecen información sobre las acciones relacionadas con un objeto supervisado.

3. En **Frecuencia de alertas**, seleccione con qué frecuencia el sistema debería generar una alerta cuando se cumpla la condición.

Opción	Descripción
Una vez hasta pasar la comprobación	El sistema generará una alerta una vez hasta que la comprobación se complete correctamente. Este es el valor predeterminado.
Después de X fallos consecutivos	El sistema generará una alerta después de X comprobaciones consecutivas fallidas, donde X es un valor entero.

4. En **Mensaje de alerta**, haga clic en el icono de lápiz para editar el mensaje de alerta predeterminado que se utilizará cuando el sistema genere una alerta. Puede especificar un mensaje de alerta personalizado que incluya variables. Para obtener más información acerca de las variables que puede utilizar, consulte "Variables de alertas de supervisión" (p. 1556).

   Nota
   Puede configurar más de un mensaje de alerta para algunos de los monitores.

5. Habilite la **Resolución automática de alertas** si desea que el sistema resuelva automáticamente la alerta cuando el parámetro supervisado vuelva al estado normal y el comportamiento vuelva a ser normal. De manera predeterminada, se habilita la configuración.

Variables de alertas de supervisión

Puede configurar diferentes variables de alertas para diferentes monitores. Para utilizar una variable, debe estar adjunta en {{}}.

La siguiente tabla proporciona más información sobre las variables disponibles.

© Acronis International GmbH, 2003-2025

Variable	Descripción	Disponible para supervisión
plan_name	El nombre de la directiva	Todos los monitores
monitor_name	El nombre de la subdirectiva del plan de supervisión	Todos los monitores
workload_name	El nombre de la carga de trabajo	Todos los monitores
threshold_value	Condiciones de supervisión específicas o umbrales para generar una alerta	Todos los monitores que admiten la supervisión basada en umbrales.
threshold_unit	La unidad que está asociada al valor del umbral. Por ejemplo, %, MB o mb/s.	Todos los monitores que admiten la supervisión basada en umbrales.
time_period	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado.	Todos los monitores que admiten la supervisión basada en umbrales.
time_unit	La unidad que estará asociada al periodo de tiempo (seg./min./horas/día).	Todos los monitores que admiten la supervisión basada en umbrales.
anomaly_value	El valor de la anomalía	Todos los monitores que admiten la supervisión basada en anomalías.
anomaly_unit	La unidad que estará asociada al valor de anomalía	Todos los monitores que admiten la supervisión basada en anomalías.
deviation_value	El valor de desviación	Todos los monitores que admiten la supervisión basada en anomalías.
deviation_unit	La unidad que estará asociada al valor de desviación	Todos los monitores que admiten la supervisión basada en anomalías.

© Acronis International GmbH, 2003-2025

Variable	Descripción	Disponible para supervisión
drive_name	La unidad de Windows o la partición de macOS	Espacio de disco,
CPU_model	El modelo de la CPU supervisada	Temperatura de CPU
GPU_model	El modelo de la GPU supervisada	Temperatura de GPU
hardware_model	El modelo del componente supervisado	Cambios del hardware
hardware_component	El tipo de hardware supervisado	Cambios del hardware
hardware_model_old	El modelo del componente supervisado que se ha reemplazado	Cambios del hardware
hardware_model_new	El modelo del nuevo componente supervisado que se ha añadido	Cambios del hardware
disk_model	El modelo del disco	Velocidad de transferencia del disco
network_adapter_model	El modelo del adaptador de red	Uso de la red
process_name	El nombre del proceso	Uso de la CPU por proceso Uso de la memoria por proceso Velocidad de transferencia del disco por proceso Uso de la red por proceso Estado del proceso
service_name	El nombre del servicio	Estado del servicio de Windows
software_name	El de la aplicación de software	Software instalado
software_version	La versión de la aplicación de software	Software instalado
software_version_old	La versión de la aplicación de software antes de la actualización	Software instalado

© Acronis International GmbH, 2003-2025

Variable	Descripción	Disponible para supervisión
software_version_new	La versión de la nueva aplicación de software actualizada	Software instalado
number_of_occurrences	El número de veces que aparece un evento en el registro	Registro de eventos de Windows
event_types	El tipo de evento	Registro de eventos de Windows
event_source	El origen del evento	Registro de eventos de Windows
event_log_name	El nombre del evento	Registro de eventos de Windows
firewall_software_name	El nombre del software de cortafuegos	Estado del cortafuegos
antimalware_software_name	El nombre del software antimalware	Estado de software antimalware
user_name	El nombre del usuario	Estado de la función AutoRun
script_name	El nombre de la secuencia de comandos	Personalizado

Medidas de respuesta manuales

Cuando vea una alerta, puede seleccionar una medida de respuesta que desee ejecutar sobre los eventos con alertas.

Pasos para ejecutar una medida de respuesta manual

1. En la consola de Protección, vaya a **Alertas**.
2. Abra la alerta que quiera ver.
3. Haga clic en **Medida de respuesta** y seleccione una medida de respuesta de la lista desplegable:

La lista de medidas de respuesta disponible para una alerta específica depende del tipo de alerta, de la disponibilidad de las funciones para un inquilino concreto y del sistema operativo de la carga de trabajo.

La siguiente tabla enumera y describe todas las medias de respuesta manuales para que pueda consultarlas.

Medida de respuesta manual	Descripción	SO compatibles
Examinar la tendencia de	Abre una ventana con el gráfico **Uso del**	Windows y

© Acronis International GmbH, 2003-2025

Medida de respuesta manual	Descripción	SO compatibles
uso del espacio de disco	**espacio de disco**, en la que puede: • Examinar cómo ha cambiado el uso del espacio de disco con el tiempo (para el último día, los últimos siete días o el último mes). • Examinar el delta para el uso del espacio de disco en el valor relativo (%) para el periodo seleccionado.	macOS
Examinar la tendencia de crecimiento del tamaño de los archivos	Abre una ventana con el gráfico **Crecimiento del tamaño de los archivos**, en la que puede: • Examinar cómo ha cambiado el tamaño total de los archivos y carpetas supervisados con el tiempo (para el último día, los últimos siete días o el último mes). • Examinar el delta para el tamaño total de los archivos en el valor relativo (%) para el periodo seleccionado.	Windows y macOS
Ejecutar una secuencia de comandos	Abre una ventana en la que puede: 1. Seleccionar una determinada secuencia de comandos para ejecutar en la carga de trabajo. 2. Especifique la cuenta con la que quiere ejecutar la secuencia de comandos. 3. Especifique la duración máxima de la operación. 4. Especifique la directiva de ejecución de PowerShell. 5. Ejecutar una secuencia de comandos. Para realizar esta acción, se debe asignar una licencia de RMM (modo de licencia basado en servicios) o de Seguridad y RMM (modo de licencia basado en soluciones) a la carga de trabajo.	Windows y macOS
Conectar a través de NEAR	Acronis Cliente de Connect establece una conexión remota.	Windows y macOS
Conectar a través de RDP	Acronis Cliente de Connect establece una conexión remota.	Windows

© Acronis International GmbH, 2003-2025

Medida de respuesta manual	Descripción	SO compatibles
Ejecutar línea de comandos	Inicia la línea de comandos (símbolo del sistema o PowerShell) de la carga de trabajo.	Windows
Ejecutar Terminal	Inicia la app Terminal (BASH o ZSH) de la carga de trabajo.	macOS
Abrir inventario de hardware	Se le redirigirá a la pestaña **Inventario de hardware** para la carga de trabajo actual.	Windows, macOS
Examinar los 10 principales procesos que han cargado la CPU	Abre una ventana con los 10 principales procesos que han cargado la CPU y pueden haber causado que se sobrecaliente (La instantánea del sistema en el momento de la generación de la alerta).	Windows, macOS
Examinar los 10 principales procesos que han cargado la GPU	Abre una ventana con los 10 principales procesos que han cargado la GPU y pueden haber causado que se sobrecaliente (La instantánea del sistema en el momento de la generación de la alerta).	Windows, macOS
Examinar los 10 principales procesos que han cargado la memoria	Abre una ventana con los 10 principales procesos que han cargado la memoria (La instantánea del sistema en el momento de la generación de la alerta).	Windows, macOS
Examinar los 10 principales procesos que han cargado el disco	Abre una ventana con los 10 principales procesos que han cargado el disco (La instantánea del sistema en el momento de la generación de la alerta).	Windows, macOS
Examinar los 10 principales procesos que han cargado la red	Abre una ventana con los 10 principales procesos que han cargado el adaptador de interfaz de red (La instantánea del sistema en el momento de la generación de la alerta).	Windows, macOS
Examinar el uso de recursos por proceso	Abre una ventana con información detallada acerca del uso de recursos de hardware por proceso relacionado: Uso de la CPU, uso de la memoria, disco E/S, uso de red.	Windows, macOS
Reiniciar carga de trabajo	Abre una ventana de confirmación. Reinicia la carga de trabajo después de la confirmación.	Windows, macOS

© Acronis International GmbH, 2003-2025

Medida de respuesta manual	Descripción	SO compatibles
Iniciar el servicio de Windows	Abre una ventana de confirmación. Inicia el servicio de Windows después de la confirmación.	Windows
Detener el servicio de Windows	Abre una ventana de confirmación. Detiene el servicio de Windows después de la confirmación.	Windows
Detener proceso	Abre una ventana de confirmación. Detiene el proceso al cual se refiere la alerta después de la confirmación.	Windows, macOS
Habilitar la actualización de Windows	Abre una ventana de confirmación. Habilita la actualización de Windows después de la confirmación.	Windows
Deshabilitar la función AutoRun en las unidades extraíbles	Abre una ventana de confirmación. Deshabilita la función AutoRun a nivel del sistema de la carga de trabajo después de la confirmación.	Windows

Importante
Por motivos de seguridad, se requiere la Autenticación de doble factor para ejecutar las siguientes medidas de respuesta manuales:

- Ejecutar una secuencia de comandos
- Conectar a través de NEAR
- Conectar a través de RDP
- Reiniciar carga de trabajo
- Iniciar el servicio de Windows
- Detener el servicio de Windows
- Detener proceso
- Habilitar la actualización de Windows
- Deshabilitar la función AutoRun en las unidades extraíbles

Consultar las alertas de supervisión para una carga de trabajo

En la pestaña de **Alertas**, puede ver las alertas de supervisión de una carga de trabajo específica y realizar diferentes acciones de alerta.

Para ver las alertas de supervisión para una carga de trabajo

© Acronis International GmbH, 2003-2025

1. En la consola de Protección, vaya a **Todos los dispositivos**.
2. Haga clic en una carga de trabajo, y luego seleccione la pestaña **Alertas**.
3. [Opcional] En el panel de alerta de supervisión, realice una de las siguientes acciones:
   - Para borrar la alerta, haga clic en **Borrar**.
   - Para tomar una acción de respuesta, haga clic en **Medida de respuesta** y luego en la acción.
   - Para contactar con el equipo de Soporte, haga clic en **Obtener soporte**.
4. [Opcional] Para borrar todas las alertas de supervisión para la carga de trabajo, haga clic en **Borrar todo**.

Visualización del registro de alertas de supervisión

Puede ver todos los eventos relacionados con una alerta de supervisión en orden cronológico: las acciones de respuesta (tanto automáticas como manuales) que se ejecutaron y las notificaciones por correo electrónico que se enviaron.

Pasos para ver el registro de alertas de una alerta de supervisión

1. En la consola de Protección, vaya a **Alertas**.
2. Abra la **Vista de tabla**.
3. En la lista de alertas, haga clic en la alerta de supervisión que desea ver.
4. Haga clic en **Detalles** y, a continuación, en **Registro de alertas**.

Configurar directivas de notificaciones por correo electrónico

Las directivas de notificaciones por correo electrónico especifican qué usuarios recibirán notificaciones por correo electrónico de diferentes monitores.

Desde la pantalla **Notificaciones por correo electrónico**, puede realizar las acciones siguientes con las directivas de notificaciones por correo electrónico: añadir, editar, habilitar, deshabilitar y eliminar.

Añadir

Pasos para añadir una nueva directiva de notificación por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. Haga clic en **Añadir directiva**.
3. Haga clic en **Seleccionar destinatarios**.
4. En la pantalla **Seleccionar destinatarios**, seleccione los usuarios que desea que reciban alertas por correo electrónico y haga clic en **Seleccionar**.
5. En **Tipos de alerta**, seleccione los monitores para los que desea que el sistema envíe alertas por

© Acronis International GmbH, 2003-2025

correo electrónico.

6. Haga clic en **Agregar**.

Editar

Para editar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. Haga clic en el icono de puntos suspensivos de la directiva de notificaciones y, luego, en **Editar**.
3. [Opcional] Para cambiar los destinatarios, haga clic en **Editar destinatarios**, añada o elimine usuarios de la lista y haga clic en **Seleccionar**.
4. [Opcional] En **Tipos de alerta**, seleccione los tipos de alerta de supervisión que desea que se envíen a los destinatarios seleccionados.
5. Haga clic en **Guardar**.

Habilitar

Para habilitar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. En la pantalla **Notificaciones por correo electrónico**, haga clic en el icono de **...** de la directiva de notificaciones por correo electrónico.
3. Haga clic en **Habilitar**.

Deshabilitar

Para deshabilitar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. En la pantalla **Notificaciones por correo electrónico**, haga clic en el icono de **...** de la directiva de notificaciones por correo electrónico.
3. Haga clic en **Deshabilitar**.

Eliminar

Para eliminar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. En la pantalla **Notificaciones por correo electrónico**, haga clic en el icono de **...** de la directiva de notificaciones por correo electrónico.
3. Haga clic en **Eliminar** y, luego, en **Confirmar**.

Ver datos de supervisión

Para cada carga de trabajo, puede ver la lista de monitores aplicados, el estado actual de los monitores y los detalles históricos del rendimiento en una vista gráfica. Puede usar esta

© Acronis International GmbH, 2003-2025

información para analizar el estado del recurso informático y cómo ha cambiado el estado con el tiempo.

Requisitos previos

- El plan de supervisión se aplica a la carga de trabajo.
- La carga de trabajo está en línea y tiene datos para el monitor correspondiente.
- La versión del agente que está instalada en la carga de trabajo es compatible con los planes de supervisión.

Pasos para ver los monitores aplicados a una carga de trabajo y los datos del monitor

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en una carga de trabajo y luego en la pestaña **Supervisión**.
   La pestaña **Supervisión** muestra un widget para cada monitor que está habilitado para la carga de trabajo. Cada widget muestra la siguiente información:

Información mostrada	Descripción
Nombre del monitor	El nombre del monitor
Último resultado	El valor más reciente del parámetro supervisado o el estado más reciente del evento
Última comprobación	La fecha y la hora en las que el monitor recopiló los últimos datos
Alertas	El número de alertas que ha generado el monitor y aún no se han resuelto. Si hay al menos una alerta sin resolver generada por este monitor, al hacer clic en el número se abrirá la pestaña **Alertas**. Las alertas se filtrarán y solo se mostrarán las de este monitor.

   Nota
   Los widgets se verán en la pestaña 15 minutos (o la frecuencia de supervisión mínima establecida para el monitor) después de aplicar un plan de supervisión a la carga de trabajo.

3. [Opcional] Para ver más información sobre el monitor, y si aplica, los datos históricos recopilados para el parámetro supervisado, en el widget del monitor, haga clic en el icono de puntos suspensivos y, a continuación, en **Detalles**.
   Para obtener más información acerca de los detalles de monitor que puede ver en los widgets, consulte "Widgets de supervisión" (p. 1565).

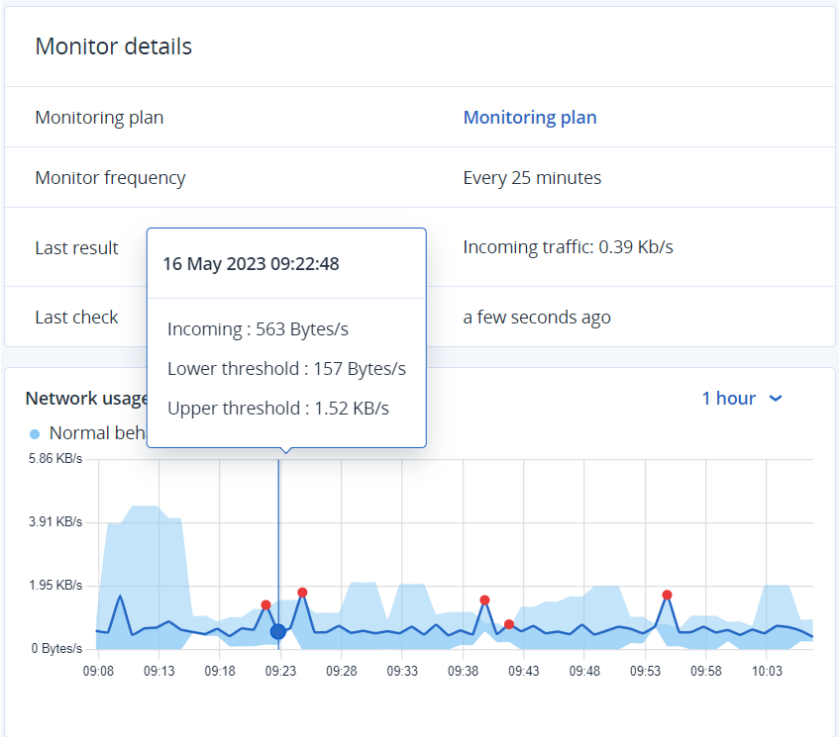
Widgets de supervisión

En el widget de supervisión, puede ver la siguiente información acerca de la supervisión.

© Acronis International GmbH, 2003-2025

Detalle	Descripción
Plan de supervisión	El nombre del plan de supervisión que incluye la supervisión. El nombre del plan de supervisión es un enlace que abre el plan de supervisión en el modo de vista.
Frecuencia del monitor	El intervalo de tiempo durante el cual el monitor recopila datos de la carga de trabajo
Último resultado	El valor más reciente del parámetro supervisado o el estado más reciente del evento
Última comprobación	La fecha y la hora en las que el monitor recopiló los últimos datos
Última alerta	La fecha y la hora en las que se generó la última alerta. El campo se muestra solo si se ha generado al menos una alerta para el monitor.
Gráfico histórico	Para los monitores que recogen datos de series temporales, el widget muestra datos históricos para un período seleccionado (1 hora, 6 horas, 12 horas, 1 día, 1 semana o 1 mes) en una vista gráfica. El gráfico muestra los valores reales de los parámetros durante el período que seleccione. Si por alguna razón el agente no ha enviado los datos recopilados a la nube, los valores faltantes se muestran como una línea punteada que conecta los puntos de datos con valores reales que preceden y siguen al valor faltante. Para los monitores que utilizan la supervisión **Basada en anomalías**, el gráfico muestra el área de líneas base, una línea que muestra los valores reales de la métrica y las anomalías. Las anomalías son los picos o los valores que están fuera de las líneas de base y se muestran como puntos rojos en el gráfico. Si pasa el ratón por encima de la gráfica, podrá ver el valor real y los valores del umbral para un momento específico.

© Acronis International GmbH, 2003-2025

Detalle	Descripción
	 **Nota** Los datos de los gráficos se muestran en la zona horario del sistema local. Se trata de la zona horaria del navegador de la carga de trabajo por la que accede a la consola de Protección.

© Acronis International GmbH, 2003-2025

Herramientas de Cyber Protection adicionales

Modo de cumplimiento

El modo de cumplimiento está diseñado para clientes con mayores demandas de seguridad. Este modo requiere cifrado obligatorio para todas las copias de seguridad y solo permite contraseñas de cifrado establecidas localmente.

Con el modo de Cumplimiento, todas las copias de seguridad creadas en un inquilino de cliente y sus unidades se cifrarán automáticamente con el algoritmo AES y una clave de 256 bits. Los usuarios solo podrán establecer las contraseñas de cifrado en los dispositivos protegidos y no podrán configurarlas en los planes de protección.

Importante
El modo de cumplimiento no puede desactivarse.

Limitaciones

- El modo de cumplimiento solo es compatible con agentes de la versión 15.0.26390 o superior.
- El modo de cumplimiento no está disponible para dispositivos que ejecuten Red Hat Enterprise Linux 4.x o 5.x y sus derivados.
- Los servicios en la nube no pueden acceder a las contraseñas de cifrado. Debido a esta limitación, algunas funciones no están disponibles para los inquilinos en el modo de cumplimiento.

Características no compatibles

Las siguientes funciones no están disponibles para los inquilinos en el modo de cumplimiento:

- Recuperación mediante la consola de Cyber Protect
- Examen de copias de seguridad a nivel de archivo mediante la consola de Cyber Protect
- Acceso a la consola de Web Restore
- Copia de seguridad de la nube a la nube
- Copia de seguridad de sitios web
- Copia de seguridad de aplicación
- Copia de seguridad de dispositivos móviles
- Análisis antimalware de copias de seguridad
- Recuperación segura
- Creación automática de listas blancas corporativas
- Mapa de protección de datos

© Acronis International GmbH, 2003-2025

- Recuperación ante desastres
- Informes y paneles de control relacionados con las características no disponibles

Definición de la contraseña de cifrado

Debe establecer la contraseña de cifrado de forma local en el dispositivo protegido. No podrá establecer la contraseña de cifrado en el plan de protección. Sin una contraseña, las copias de seguridad fallarán.

Advertencia.
No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.

Puede establecer la contraseña de cifrado de las siguientes formas:

1. Durante la instalación de un agente de protección (para Windows, macOS y Linux).
2. Mediante el uso de la línea de comandos (para Windows y Linux).
   Esta es la única forma de establecer una contraseña cifrada en un dispositivo virtual.
   Para obtener más información sobre cómo establecer una contraseña de cifrado con la herramienta **Acropsh**, consulte "Cifrado" (p. 583).
3. En Cyber Protect Monitor (para Windows y macOS).

Para establecer la contraseña de cifrado en Cyber Protect Monitor

1. Inicie sesión como administrador en el dispositivo protegido.
2. Haga clic en el icono de Cyber Protect Monitor en el área de notificaciones (en Windows) o en la barra del menú (en macOS).
3. Haga clic en el icono de engranaje.
4. Haga clic en **Cifrado**.
5. Defina la contraseña de cifrado.
6. Haga clic en **Aceptar**.

Cambio de contraseña de cifrado

Puede cambiar la contraseña de cifrado antes de que un plan de protección cree copias de seguridad.

Le recomendamos que no cambie la contraseña de cifrado después de crear copias de seguridad porque las copias de seguridad posteriores fallarán. Para seguir protegiendo el mismo equipo, cree un nuevo plan de protección. Si cambia la contraseña de cifrado y el plan de protección, se crearán nuevas copias de seguridad encriptadas con la contraseña cambiada. Esto no afectará a las copias de seguridad que se crearon antes de estos cambios.

De forma alternativa, puede mantener el plan de protección aplicado y cambiar solo el nombre del archivo de la copia de seguridad. Así también se crearán nuevas copias de seguridad encriptadas

© Acronis International GmbH, 2003-2025

con la contraseña cambiada. Para obtener más información acerca del nombre del archivo de la copia de seguridad, consulte "Nombre del archivo de copia de seguridad." (p. 596).

Puede cambiar la contraseña de cifrado de las siguientes formas:

1. En Cyber Protect Monitor (para Windows y macOS).
2. Mediante el uso de la línea de comandos (para Windows y Linux).
   Para obtener más información sobre cómo establecer la contraseña de cifrado con la herramienta **Acropsh**, consulte "Cifrado" (p. 583).

Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento

Con el modo de cumplimiento, no puede recuperar copias de seguridad en la consola de Cyber Protect.

Las siguientes opciones están disponibles:

- Recuperación de todo el equipo, sus discos y archivos mediante un dispositivo de arranque.
- Extracción de archivos desde copias de seguridad locales de equipos Windows con el agente instalado mediante el explorador de archivos de Windows.

Almacenamiento inmutable

El almacenamiento inmutable es un tipo de almacenamiento de datos que impide que las copias de seguridad se alteren, modifiquen o eliminen durante un período definido. Garantiza que los datos permanezcan seguros e inalterables, para lo que proporciona una capa adicional de protección contra modificaciones no autorizadas o no intencionadas o ataques de ransomware. El almacenamiento inmutable está disponible para todas las copias de seguridad en la nube almacenadas en una instancia de almacenamiento en la nube compatible. Consulte "Almacenamientos y agentes admitidos" (p. 1571).

Con el almacenamiento inmutable, puede acceder a copias de seguridad eliminadas durante el período de retención especificado. Puede recuperar el contenido de esas copias de seguridad, pero no puede cambiarlo, moverlo o eliminarlo. Cuando finaliza el período de retención, las copias de seguridad eliminadas desaparecen de forma permanente.

El almacenamiento inmutable contiene las siguientes copias de seguridad:

- Copias de seguridad eliminadas manualmente.
- Las copias de seguridad eliminadas automáticamente, según la configuración de la sección **Cuánto tiempo se conservarán** de un plan de protección o la sección **Normas de retención** de un plan de limpieza.

Las copias de seguridad eliminadas en el almacenamiento inmutable siguen usando espacio de almacenamiento y se cobran en consonancia.

© Acronis International GmbH, 2003-2025

A los inquilinos eliminados no se les cobra por ningún almacenamiento, incluido el almacenamiento inmutable.

Modos de almacenamiento inmutables

El almacenamiento inmutable está disponible en los siguientes modos:

- **Modo de gobierno**
  Puede deshabilitar y volver a habilitar el almacenamiento inmutable. Puede cambiar el período de retención o cambiar al modo de cumplimiento.
- **Modo de cumplimiento normativo**

  Advertencia.
  Seleccionar el modo de cumplimiento es irreversible.

  No puede desactivar el almacenamiento inmutable. No puede cambiar el período de retención y tampoco puede volver al modo de administración.

Almacenamientos y agentes admitidos

- El almacenamiento inmutable solo es compatible con el almacenamiento en la nube.
  - El almacenamiento inmutable está disponible para los almacenamientos en la nube alojados por Acronis y por los partners que utilicen la versión 4.7.1 o posterior de Acronis Cyber Infrastructure.
  - Todos los almacenamientos que se pueden utilizar con Acronis Cyber Infrastructure Backup Gateway son compatibles. Por ejemplo, el almacenamiento Acronis Cyber Infrastructure, los almacenamientos Amazon S3 y EC2, y el almacenamiento Microsoft Azure.
  - El almacenamiento inmutable requiere que el puerto TCP 40440 esté abierto para el servicio Backup Gateway en Acronis Cyber Infrastructure. En la versión 4.7.1 y posteriores, el puerto TCP 40440 se abre automáticamente con el tipo de tráfico **Copia de seguridad (ABGW) pública**. Para obtener más información sobre los tipos de tráfico, consulte la documentación de Acronis Cyber Infrastructure.
- Para el almacenamiento inmutable es necesario un agente de protección versión 21.12 (compilación 15.0.28532) o posteriores.
- Solo se admiten copias de seguridad TIBX (versión 12).

Habilitación del almacenamiento inmutable

Puede configurar los ajustes de almacenamiento inmutable en la consola de Cyber Protect o en el portal de administración. Ambos proporcionan acceso a los mismos ajustes. El procedimiento siguiente utiliza la consola de Cyber Protect. Para obtener información sobre cómo configurar los ajustes de almacenamiento inmutable en el portal de administración, consulte Configuración del almacenamiento inmutable en la guía del administrador.

Pasos para habilitar el almacenamiento inmutable

© Acronis International GmbH, 2003-2025

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. Vaya a **Configuración** > **Configuración del sistema**.
3. Desplácese por la lista de opciones de copia de seguridad predeterminadas y después haga clic en **Almacenamiento inmutable**.
4. Habilite el control deslizante **Almacenamiento inmutable**.
5. Especifique un período de retención entre 14 y 3650 días.

   El período de retención predeterminado es de 14 días. Si establece un período de retención mayor, aumentará el uso del almacenamiento.
6. Seleccione el modo de almacenamiento inmutable y, si se le solicita, confirme su elección.
   - **Modo de gobierno**

     Este modo garantiza que el ransomware o los actores malintencionados no puedan manipular ni borrar los datos de copia de seguridad, ya que todas las copias de seguridad eliminadas se mantienen en el almacenamiento inmutable durante el período de retención que haya especificado. También garantiza la integridad de los datos de copia de seguridad, lo cual es fundamental para la recuperación ante desastres.

     En este modo, puede deshabilitar y volver a habilitar el almacenamiento inmutable, cambiar el período de retención o cambiar al modo de cumplimiento.
   - **Modo de cumplimiento normativo**

     Además de los beneficios del modo de gobierno, el modo de cumplimiento ayuda a las organizaciones a cumplir con los requisitos reglamentarios para la retención y la seguridad de los datos al evitar la manipulación de los mismos.

     Advertencia.
     La selección del modo de cumplimiento es irreversible. Después de seleccionar este modo, no puede deshabilitar el almacenamiento inmutable, cambiar el período de retención o volver al modo de gobierno.
7. Haga clic en **Guardar**.
8. Para agregar un archivo comprimido existente al almacenamiento inmutable, cree una nueva copia de seguridad en ese archivo comprimido al ejecutar el plan de protección correspondiente de forma manual o según un horario.

   Advertencia.
   Si elimina una copia de seguridad antes de establecer el soporte de archivo comprimido como el almacenamiento inmutable, la copia de seguridad se eliminará de forma permanente.

Inhabilitación del almacenamiento inmutable

Nota
Solo puede desactivar el almacenamiento inmutable en el Modo de gobierno.

Pasos para deshabilitar el almacenamiento inmutable

© Acronis International GmbH, 2003-2025

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. En el menú de navegación, haga clic en **Configuración** > **Configuración del sistema**.
3. Desplácese por la lista de opciones de copia de seguridad predeterminadas y después haga clic en **Almacenamiento inmutable**.
4. Deshabilite el control deslizante **Almacenamiento inmutable**.
5. Haga clic en **Deshabilitar** para confirmar su elección.

Advertencia.
Deshabilitar el almacenamiento inmutable no entra en vigor de inmediato. Durante un periodo de gracia de 14 días (336 horas), puede acceder a las copias de seguridad eliminadas según su periodo de retención original.

Cuando finaliza el periodo de gracia, todas las copias de seguridad en el almacenamiento inmutable se eliminan de forma permanente. Por ejemplo, si desactiva el almacenamiento inmutable el 1 de octubre a las 10:00, todas las copias de seguridad que sigan en el almacenamiento inmutable el 15 de octubre a las 10:00 se eliminarán de forma permanente.

Acceder a copias de seguridad eliminadas en el almacenamiento inmutable

Durante el periodo de retención, puede acceder a copias de seguridad eliminadas y recuperar datos de ellas.

Una copia de seguridad eliminada puede ser parte de un archivo comprimido eliminado o de un archivo comprimido no eliminado.

Nota
Para permitir el acceso a las copias de seguridad eliminadas, el puerto 40440 en el almacenamiento de copia de seguridad debe estar habilitado para conexiones entrantes.

Pasos para acceder a una copia de seguridad eliminada

En un archivo comprimido eliminado

1. En la pestaña **Almacenamiento de la copia de seguridad**, seleccione el almacenamiento en la nube que contenga la copia de seguridad eliminada.
2. Para ver los archivos comprimidos eliminados, haga clic en **Mostrar eliminados**.
3. Seleccione el archivo que contiene la copia de seguridad que desea recuperar.
4. Haga clic en **Mostrar copias de seguridad**.
5. Seleccione la copia de seguridad que desea recuperar.
6. Continúe con la operación de recuperación como se describe en "Recuperación" (p. 653).

En un archivo comprimido no eliminado

© Acronis International GmbH, 2003-2025

1. En la pestaña **Almacenamiento de la copia de seguridad**, seleccione el almacenamiento en la nube que contenga la copia de seguridad eliminada.
2. Seleccione el archivo que contiene la copia de seguridad que desea recuperar.
3. Haga clic en **Mostrar copias de seguridad** y en **Mostrar elementos eliminados**.
4. Seleccione la copia de seguridad que desea recuperar.
5. Continúe con la operación de recuperación como se describe en "Recuperación" (p. 653).

Visualización del uso del almacenamiento inmutable

Puede ver cuánto espacio utiliza el almacenamiento inmutable en la consola de Cyber Protect.

Limitaciones

- El valor notificado incluye el tamaño total de todas las copias de seguridad eliminadas y los metadatos de los archivos de copia de seguridad en el almacenamiento. Los metadatos pueden ser hasta el 10 % del valor notificado.
- El valor muestra los datos de uso de hasta 24 horas antes.
- Si el uso real es inferior a 0,01 GB, se muestra como 0,0 GB.

Pasos para ver el uso del almacenamiento inmutable

En la consola de Cyber Protect

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Almacenamiento de la copia de seguridad** > **Copias de seguridad** y luego seleccione una ubicación de almacenamiento en la nube que admita almacenamiento inmutable.
3. Compruebe la columna **Almacenamiento inmutable y metadatos**.

Almacenamiento redundante geográficamente

Con el almacenamiento con redundancia geográfica, los datos respaldados se copian de forma asíncrona a una ubicación de replicación que está geográficamente alejada de la ubicación de respaldo primaria. Por lo tanto, los datos se siguen conservando y son accesibles incluso si la ubicación primaria no está disponible.

Los datos replicados utilizan la misma cantidad espacio de almacenamiento que los datos originales.

Limitaciones

- El almacenamiento con redundancia geográfica puede no estar disponible en todos los centros de datos.
- La redundancia geográfica solo es compatible con el almacenamiento en la nube. No es compatible con almacenamientos de terceros, como los almacenamientos alojados por partners o los almacenamientos en la nube pública.

© Acronis International GmbH, 2003-2025

- La ubicación de los datos de la replicación depende de su centro de datos. Para obtener más información, consulte este artículo de la base de conocimientos.
- Se aplican limitaciones adicionales cuando utiliza el almacenamiento con redundancia geográfica junto con Disaster Recovery.

  Para obtener más información, consulte "Limitaciones al usar el almacenamiento en la nube con redundancia geográfica" (p. 1015).

Habilitar el almacenamiento con redundancia geográfica

Requisitos previos

- Se asigna un almacenamiento que proporciona soporte con redundancia geográfica al inquilino de cliente.
- Se proporciona almacenamiento con redundancia geográfica para el inquilino de cliente en el portal de administración.

  No se puede realizar el aprovisionamiento del almacenamiento con redundancia geográfica si se asigna un almacenamiento no compatible. Por ejemplo, un almacenamiento alojado por un partner.

Puede habilitar el almacenamiento con redundancia geográfica en la pantalla principal de la consola de Cyber Protect o en la pestaña **Configuración**. El resultado de ambos procedimientos es el mismo.

Pasos para habilitar el almacenamiento con redundancia geográfica

En la ventana principal

1. Inicie sesión en la consola de Cyber Protect como administrador.

   Aparece un mensaje de advertencia en la parte superior de la consola de Cyber Protect.
2. En el mensaje de advertencia, haga clic en **Activar almacenamiento en la nube con redundancia geográfica**.
3. Seleccione la casilla de verificación para confirmar que ha comprendido las ubicaciones de replicación y las tarifas.
4. Para confirmar su elección, haga clic en **Habilitar**.

Como resultado, se habilita el almacenamiento con redundancia geográfica y los datos de la copia de seguridad se copiarán en la ubicación de replicación.

En la pestaña Configuración

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Configuración** > **Configuración del sistema**.
3. Contraiga la lista de opciones de copia de seguridad predeterminadas y haga clic en **Almacenamiento en la nube con redundancia geográfica**.
4. Habilite el conmutador **Almacenamiento en la nube con redundancia geográfica**.
5. Haga clic en **Guardar**.

© Acronis International GmbH, 2003-2025

6. Seleccione la casilla de verificación para confirmar que ha comprendido las ubicaciones de replicación y las tarifas.
7. Para confirmar su elección, haga clic en **Habilitar**.

Como resultado, se habilita el almacenamiento con redundancia geográfica y los datos de la copia de seguridad se copiarán en la ubicación de replicación.

Deshabilitar el almacenamiento con redundancia geográfica

Puede deshabilitar el almacenamiento con redundancia geográfica en la consola de Cyber Protect.

Pasos para deshabilitar el almacenamiento con redundancia geográfica

1. Inicie sesión en la consola de Cyber Protect como administrador.
2. Vaya a **Configuración** > **Configuración del sistema**.
3. Contraiga la lista de opciones de copia de seguridad predeterminadas y haga clic en **Almacenamiento en la nube con redundancia geográfica**.
4. Deshabilite el conmutador **Almacenamiento en la nube con redundancia geográfica**.
5. Haga clic en **Guardar**.
6. Para confirmar su elección, escriba **Deshabilitar** y, a continuación, haga clic en **Deshabilitar**.

Como resultado, el almacenamiento con redundancia geográfica está deshabilitado. Los datos replicados se eliminarán en un plazo de un día.

Visualización del estado de georreplicación

El estado de georreplicación muestra si los datos de la ubicación primaria de la copia de seguridad se copian en la ubicación de replicación.

Se pueden dar los siguientes estados:

- **Sincronizados**: los datos se han copiado en la ubicación de replicación.
- **Sincronizando**: los datos se están copiando en la ubicación de replicación. La duración esta operación dependerá del tamaño de los datos.
- **En espera**: se ha suspendido la replicación de los datos temporalmente.
- **Deshabilitada**: se ha deshabilitado la replicación de los datos.

Pasos para comprobar el estado de la replicación

1. Inicie sesión en la consola de Cyber Protect.
2. En la pestaña **Almacenamiento de la copia de seguridad**, seleccione la ubicación y luego seleccione el archivo de copia de seguridad.
3. Haga clic en **Detalles** y compruebe el estado en la sección **Estado de georreplicación**.

© Acronis International GmbH, 2003-2025

Panel de control de concienciación

Este panel de control está disponible si el proveedor de servicios habilita el servicio de Formación en concienciación sobre seguridad.

El panel de control es accesible en el nivel de cliente para los usuarios con los siguientes roles: administrador de partner, administrador de cliente, administrador de protección o ciberadministrador.

El panel de control proporciona una visión general del progreso de la formación en concienciación sobre seguridad en la organización y sirve como puerta de enlace para navegar hasta la consola de administración de la formación en concienciación sobre seguridad en Wizer.

Funcionamiento del servicio de Formación en concienciación sobre seguridad

Para gestionar los usuarios y el contenido de formación disponibles para su organización, haga clic en **Consola de administración** en la parte superior izquierda del panel de control de concienciación. Se abrirá la consola de administración de Wizer.

Consulte la documentación de Wizer para obtener instrucciones detalladas.

© Acronis International GmbH, 2003-2025

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

OpenVPN de sitio a sitio: información adicional

Cuando cree un servidor de recuperación, configure su **dirección IP en la red de producción** y su **dirección IP de prueba**.

Después de una conmutación por error (ejecutar la máquina virtual en la nube) y de iniciar sesión en la máquina virtual para comprobar la dirección IP del servidor, verá la **dirección IP en la red de producción**.

Cuando realice la conmutación por error de prueba, solo puede llegar al servidor de prueba usando la **dirección IP de prueba**, que solo es visible en la configuración del servidor de recuperación.

Para acceder a un servidor de prueba desde su sitio local, tiene que usar la **Dirección IP de prueba**.

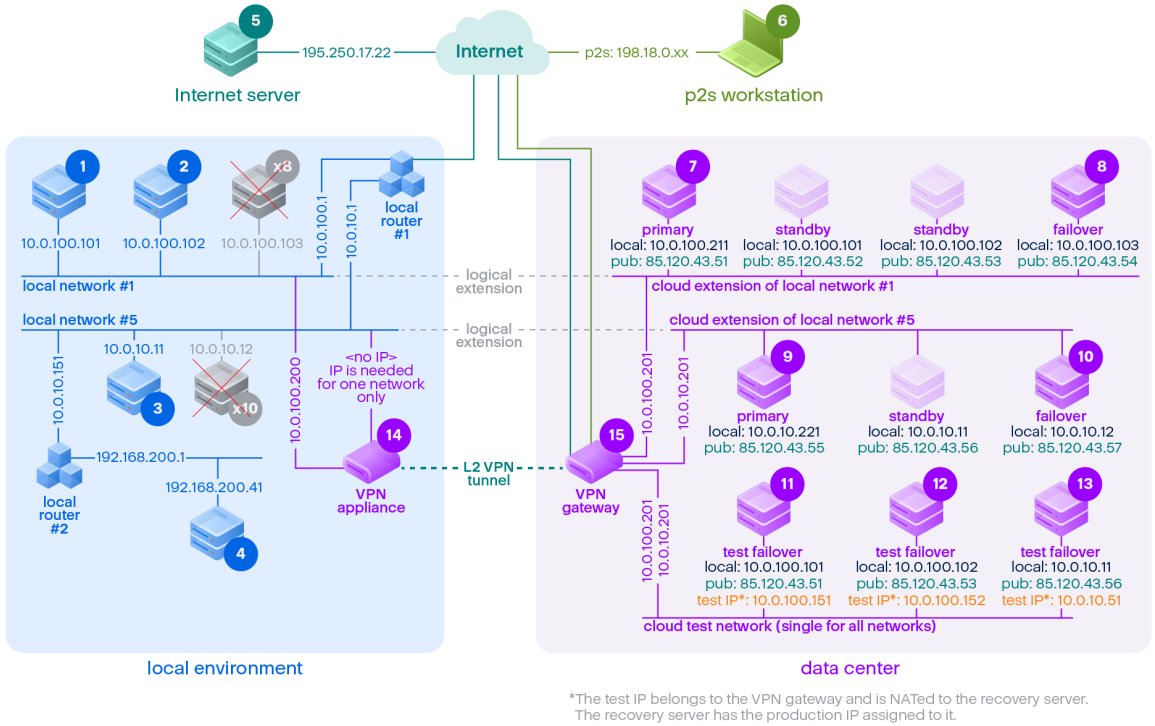
Nota
La configuración de red del servidor siempre muestra la **dirección IP en la red de producción** (ya que el servidor de prueba refleja cómo se vería el servidor de producción). Esto ocurre porque la dirección IP de prueba no pertenece al servidor de prueba, sino a la puerta de enlace VPN, y se traduce a la dirección IP de producción utilizando NAT.

El siguiente diagrama presenta un ejemplo de la configuración de la conexión OpenVPN de sitio a sitio. Algunos de los servidores del entorno local se recuperan en la nube mediante la conmutación por error (mientras la infraestructura de la red funcione).

1. El cliente habilitó Disaster Recovery:
   a. mediante la configuración del dispositivo VPN (14) y su conexión al servidor VPN exclusivo de la nube (15)
   b. al proteger algunos de los servidores locales con Disaster Recovery (1, 2, 3, x8 y x10)
      Algunos servidores del sitio local (como el 4) están conectados a redes que no están conectadas al dispositivo VPN. Dichos servidores no están protegidos por Disaster Recovery.
2. Parte de los servidores (conectados a diferentes redes) funcionan en el sitio local: (1, 2, 3 y 4)
3. Los servidores protegidos (1, 2 y 3) se están probando con la conmutación por error de prueba (11, 12 y 13)
4. Algunos servidores del sitio local no están disponibles (x8 y x10). Después de ejecutar una conmutación por error, estarán disponibles en la nube (8 y 10)

© Acronis International GmbH, 2003-2025

5. Algunos servidores principales (7 y 9), conectados a diferentes redes, están disponibles en el entorno de la nube
6. (5) es un servidor en Internet con una dirección IP pública
7. (6) es una estación de trabajo conectada a la nube mediante una conexión VPN de punto a sitio (p2s)



En este ejemplo, está disponible la siguiente configuración de conexión (por ejemplo, "ping") desde un servidor en la fila **Desde:** a uno en la columna **Hasta:**.

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
De:		local	local	local	local	Internet	p2s	principal	conmutación por error	principal	conmutación por error	conmutación por error de prueba	conmutación por error de prueba	conmutación por error de prueba	dispositivo VPN	servidor VPN
1	local		directo	a través del enrutador local 1	a través del enrutador local 2	a través del enrutador local 1 y de Internet	no	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del enrutador local 1 y del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	directo	no
2	local	directo		a través del enrutador local 1	a través del enrutador local 2	a través del enrutador local 1 y de Internet	no	a través del túnel: local a	a través del túnel: local a través del	a través del túnel: local a	a través del túnel: local a través del	a través del túnel: NAT (servidor VPN) a través	a través del túnel: NAT (servidor VPN) a través	a través del enrutador local 1 y del túnel: NAT (servidor	directo	no

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								través del enrutador local 1 y de Internet: pub	enrutador local 1 y de Internet: pub	través del enrutador local 1 y de Internet: pub	enrutador local 1 y de Internet: pub	del enrutador local 1 y de Internet: pub	del enrutador local 1 y de Internet: pub	VPN) a través del enrutador local 1 y de Internet: pub		
3	local	a través del enrutador local 1	a través del enrutador local 1		a través del enrutador local 2	a través del enrutador local 1 y de Internet	no	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: local a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del enrutador local 1 y del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	a través del enrutador local	no
4	local	a través	a través	a través		a través del	no	a través	a través del	a través	a través del	a través del túnel:	a través del túnel:	a través del túnel:	a través	no

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		del enrutador 2 y del enrutador 1 locales	del enrutador 2 y del enrutador 1 locales	del enrutador local 2		enrutador 2 y del enrutador 1 locales y de Internet		del enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	del enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	enrutador local 2 y del túnel: local a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	NAT (servidor VPN) a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	NAT (servidor VPN) a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	NAT (servidor VPN) a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	del enrutador local 2	
5	Internet	no	no	no	no		n/d	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	a través de Internet: pub	no	no

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6	p2s	no	no	no	no	a través de Internet		a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s (servidor VPN): local a través de Internet: pub	a través de VPN p2s: NAT (servidor VPN) a través de Internet: pub	a través de VPN p2s: NAT (servidor VPN) a través de Internet: pub	a través de VPN p2s: NAT (servidor VPN) a través de Internet: pub	no	no
7	principal	a través del túnel	a través del túnel	a través del túnel y del enrutador local 1	a través del túnel y del enrutador local 1 y 2	a través de Internet (mediante un servidor VPN)	no		directo de la nube: local	a través del túnel y del enrutador local 1: local	a través del túnel y del enrutador local 1: local	a través de un servidor VPN: NAT	a través de un servidor VPN: NAT	a través del túnel y del enrutador local 1: NAT	no	Solo protocolos DHCP y DNS
8	conmutación	a través	a través	a través	a través	a través de	no	directo de la		a través	a través del túnel	a través de un	a través de un	a través del túnel	no	Solo protoc

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	por error	del túnel	del túnel	del túnel y del enrutador local 1	del túnel y del enrutador local 1 y 2	Internet (mediante un servidor VPN)		nube: local		del túnel y del enrutador local 1: local	y del enrutador local 1: local	servidor VPN: NAT	servidor VPN: NAT	y del enrutador local 1: NAT		olos DHCP y DNS
9	principal	a través del túnel y del enrutador local 1	a través del túnel y del enrutador local 1	a través del túnel	a través del túnel	a través de Internet (mediante un servidor VPN)	no	a través del túnel y del enrutador local 1: local	a través del túnel y del enrutador local 1: local		directo de la nube: local	a través del túnel y del enrutador local 1: NAT	a través del túnel y del enrutador local 1: NAT	a través de un servidor VPN: NAT	no	Solo protocolos DHCP y DNS
10	conmutación por error	a través del túnel y del enrutador local 1	a través del túnel y del enrutador local 1	a través del túnel	a través del túnel	a través de Internet (mediante un servidor VPN)	no	a través del túnel y del enrutador local 1: local	a través del túnel y del enrutador local 1: local	directo de la nube: local		a través del túnel y del enrutador local 1: NAT	a través del túnel y del enrutador local 1: NAT	a través de un servidor VPN: NAT	no	Solo protocolos DHCP y DNS
11	conmut	no	no	no	no	a través	no	no	no	no	no		directo de	a través	no	Solo

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	ación por error de prueba					de Internet (mediante un servidor VPN)							la nube: local	de un servidor VPN: local (enrutamiento)		protocolos DHCP y DNS
12	conmutación por error de prueba	no	no	no	no	a través de Internet (mediante un servidor VPN)	no	no	no	no	no	directo de la nube: local		a través de un servidor VPN: local (enrutamiento)	no	Solo protocolos DHCP y DNS
13	conmutación por error de prueba	no	no	no	no	a través de Internet (mediante un servidor VPN)	no	no	no	no	no	a través de un servidor VPN: local (enrutamiento)	a través de un servidor VPN: local (enrutamiento)		no	Solo protocolos DHCP y DNS
14	dispositivo VPN	directo	directo	a través del enrutador local 1	a través del enrutador local 2	a través de Internet (enrutador local 1)	no	no	no	no	no	no	no	no		no

© Acronis International GmbH, 2003-2025

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
15	servidor VPN	no	no	no	no	no	no	no	no	no	no	no	no	no	no	

© Acronis International GmbH, 2003-2025

Glosario

A

Agente de protección

El agente de protección es aquel que se instala en los equipos para proteger los datos.

Agente para la prevención de pérdida de datos

Un componente de cliente del sistema de prevención de pérdida de datos que protege al equipo servidor del acceso no autorizado, la transmisión y el almacenamiento de datos confidenciales, protegidos o sensibles al aplicar una combinación de técnicas de análisis de contenido y contexto y políticas de prevención de pérdida de datos administradas de forma centralizada. Cyber Protection proporciona un agente para la prevención de pérdida de datos con todas las funciones. Sin embargo, la funcionalidad del agente en un equipo protegido se limita al conjunto de funciones de prevención de pérdida de datos disponibles para las licencias de Cyber Protection y depende del plan de protección que se aplique al equipo.

B

Base de datos de dispositivos USB

[Control de dispositivos] El módulo de control de dispositivos mantiene una base de datos de dispositivos USB desde la que se puede agregar a la lista de exclusiones desde el control de acceso de dispositivos. La base de datos registra los dispositivos USB por ID del dispositivo, que puede introducirse a mano o seleccionarse de entre los dispositivos conocidos de la consola de Cyber Protect.

C

Conexión de punto a sitio (P2S)

[Disaster Recovery] Una conexión VPN segura desde el exterior hacia los sitios locales y la nube mediante sus dispositivos de endpoint (como un ordenador de sobremesa o un portátil).

Conexión de sitio a sitio (S2S)

[Disaster Recovery] Conexión que amplía la red local a la nube mediante un túnel de VPN seguro.

Conjunto de copias de seguridad

Es un grupo de copias de seguridad al que se le puede aplicar una regla de retención individual. Para el esquema personalizado de copia de seguridad, los conjuntos de copias de seguridad se corresponden con los métodos de copia de seguridad (completa, diferencial e incremental). En los demás casos, los conjuntos de copias de seguridad son mensual, diaria, semanal o cada hora. Una copia de seguridad mensual es la primera copia de seguridad creada una vez comenzado un mes. Una copia de seguridad semanal es la primera copia de seguridad que se crea el día de la semana seleccionado en la opción Copia de seguridad semanal (haga clic en el icono de engranaje y, a continuación, en Opciones de copia de seguridad > Copia de seguridad semanal). Si una copia de seguridad semanal es también la primera copia de seguridad que se crea en un nuevo mes, se considerará mensual. En ese caso, se creará una copia de seguridad semanal el día de la semana siguiente seleccionado. Una copia de seguridad diaria es la primera copia de seguridad que se crea en un día, excepto si

© Acronis International GmbH, 2003-2025

puede considerarse mensual o semanal. Una copia de seguridad de cada hora es la primera copia de seguridad que se crea en una hora, excepto si puede considerarse mensual, semanal o diaria.

Conmutación por recuperación

Traslado de una carga de trabajo de un servidor adicional (como la réplica de un equipo virtual o un servidor de recuperación que se ejecuta en el cloud) al servidor de producción.

Copia de seguridad completa

Es una copia de seguridad autosuficiente que contiene todos los datos seleccionados para la copia de seguridad. No necesita acceso a otra copia de seguridad para recuperar los datos de una copia de seguridad completa.

Copia de seguridad diferencial

Una copia de seguridad diferencial almacena todos los cambios desde la última copia de seguridad completa. Necesita tener acceso a la copia de seguridad completa correspondiente para recuperar los datos de una copia de seguridad diferencial.

Copia de seguridad huérfana

Una copia de seguridad huérfana es una copia de seguridad que ya no está asociada a un plan de protección.

Copia de seguridad incremental

Es una copia de seguridad que almacena los cambios de los datos a partir de la última copia de seguridad. Necesita tener acceso a otras copias de seguridad para recuperar los datos de una copia de seguridad incremental.

D

Dirección IP de prueba

[Disaster Recovery] Una dirección IP necesaria en caso de una prueba de conmutación por error que evita que se duplique la dirección IP de producción.

Dirección IP pública

[Disaster Recovery] Una dirección IP necesaria para que los servidores en la nube estén disponibles desde Internet.

Dispositivo VPN

[Disaster Recovery] Un equipo virtual especial que permite la conexión entre la red local y el sitio en la nube mediante un túnel de VPN seguro. El dispositivo VPN se implementa en el sitio local.

E

Equipo físico

Un equipo que tiene una copia de seguridad realizada por un agente instalado en el sistema operativo.

Equipo virtual

Un equipo virtual que tiene una copia de seguridad a nivel de hipervisor realizada por un agente externo como Agente para VMware o Agente para Hyper-V. Un equipo virtual con un agente dentro se considera un equipo físico desde la perspectiva de la copia de seguridad.

F

Finalización

La operación que convierte un equipo virtual temporal que se ejecuta a partir de una copia

© Acronis International GmbH, 2003-2025

de seguridad en un equipo virtual permanente. Físicamente, esto implica recuperar todos los discos del equipo virtual y los cambios sucedidos mientras se ejecutaba dicho equipo al almacén de datos donde se guardan dichos cambios.

Formato de copia de seguridad de archivo único

Es un formato de copia de seguridad en el que las copias de seguridad iniciales completas e incrementales subsiguientes se guardan en un único archivo .tibx. Este formato aprovecha la velocidad del método de copia de seguridad incremental, al mismo tiempo que se evita la desventaja principal: la eliminación compleja de copias de seguridad desactualizadas. El software marca los bloques que usan las copias de seguridad desactualizadas como "libres" y escribe nuevas copias de seguridad en esos bloques. Con este formato, la limpieza es extremadamente rápida, y el consumo de recursos es mínimo. El formato de copia de seguridad de archivo único no está disponible cuando se realiza la copia en ubicaciones que no son compatibles con los accesos de lectura y escritura aleatorios.

M

Módulo

Un módulo es una parte del plan de protección que proporciona una funcionalidad de protección de datos concreta, por ejemplo, el módulo de copia de seguridad, el módulo de protección antivirus y antimalware, etc.

Módulo de control de dispositivos

Como parte de un plan de protección, el módulo de control de dispositivos aprovecha un subconjunto funcional del agente de prevención de pérdida de datos de cada equipo protegido para detectar y evitar el acceso no autorizado y la transmisión de datos en los canales del equipo local. Esto incluye el acceso de usuario a dispositivos y puertos periféricos, la impresión de documentos, las operaciones de copiar y pegar del portapapeles, el formato de medios y las operaciones de extracción, así como la sincronización con dispositivos móviles conectados de manera local. El módulo del control de dispositivos proporciona control granular y contextual sobre los tipos de dispositivos y los puertos a los que los usuarios tienen acceso en el equipo protegido y las acciones que los usuarios pueden llevar a cabo sobre los dispositivos.

O

Objetivo del punto de recuperación (RPO)

[Disaster Recovery] Cantidad de datos perdidos debido a una interrupción que se miden en la cantidad de tiempo transcurrido desde una interrupción planificada o un desastre. El umbral de RPO define el intervalo temporal máximo permitido entre el último punto de recuperación viable para una conmutación por error y el momento presente.

P

Plan de protección

Un plan de protección es aquel que combina módulos de protección de datos como los siguientes: copia de seguridad, protección antivirus y antimalware, filtrado de URL, antivirus Windows Defender, Microsoft Security Essentials, evaluación de vulnerabilidades, gestión de parches, mapa de protección de datos y control de dispositivos.

© Acronis International GmbH, 2003-2025

Prevención de pérdida de datos (antes, prevención de fuga de datos)

Un sistema de tecnologías integradas y medidas organizativas destinado a detectar y evitar la divulgación o el acceso accidental o intencional a datos confidenciales, protegidos o sensibles por parte de entidades no autorizadas de fuera o dentro de la organización, o la transferencia de tales datos a entornos que no son de confianza.

Puerta de enlace de VPN (anteriormente, servidor VPN o puerta de enlace de conectividad)

[Disaster Recovery] Un equipo virtual especial que proporciona una conexión entre las redes del sitio local y el sitio en la nube mediante un túnel de VPN seguro. La puerta de enlace de VPN se implementa en el sitio en el cloud.

R

Recuperación de fallos

Traslado de una carga de trabajo de un servidor de producción a un servidor adicional (como la réplica de un equipo virtual o un servidor de recuperación que se ejecuta en el cloud).

Red de prueba

[Disaster Recovery] Red virtual aislada que se usa para probar el proceso de conmutación por error.

Red productiva

[Disaster Recovery] La red interna ampliada por túneles VPN que cubre sitios locales y en la nube. Los servidores locales y en el cloud pueden comunicarse en la red de producción.

Runbook

[Disaster Recovery] Situación planificada que consiste en pasos configurables que automatizan las acciones de recuperación ante desastres.

S

Servidor de recuperación

[Disaster Recovery] Una réplica en equipo virtual del equipo original basada en las copias de seguridad del servidor protegido almacenadas en la nube. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.

Servidor en la nube

[Disaster Recovery] Referencia general a un servidor principal o de recuperación.

Servidor principal

[Disaster Recovery] Un equipo virtual que no tiene un equipo enlazado en el sitio local (como un servidor de recuperación). Los servidores principales se utilizan para proteger una aplicación o para ejecutar varios servicios auxiliares (como un servidor web).

Sitio en el cloud (o sitio de recuperación ante desastres)

[Disaster Recovery] Sitio remoto alojado en la nube, usado para la ejecución de infraestructuras de recuperación en caso de desastres.

Sitio local

[Disaster Recovery] La infraestructura local implementada en las instalaciones de su

© Acronis International GmbH, 2003-2025

empresa.

V

Validación

Una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad. La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad a un destino ficticio. La validación de la copia de seguridad de un disco calcula la suma de comprobación por cada bloque de datos guardado en la copia de seguridad. Ambos procedimientos utilizan muchos recursos. Si bien la validación correcta implica una alta probabilidad de tener una recuperación exitosa, no verifica todos los factores que influyen en el proceso de recuperación.

© Acronis International GmbH, 2003-2025

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

Índice

#

#CyberFit Score para equipos 468

#CyberFit Score por equipo 335

¿

¿32 bits o 64 bits? 986

¿Cómo funciona? 1245

¿Cómo llegan los archivos a la carpeta de cuarentena? 1209

¿Cuánto tiempo se conservarán las copias de seguridad? 537

¿Cuántos agentes necesito? 137, 142, 147, 160

¿Cuántos agentes se necesitan para la copia de seguridad y recuperación compatible con el clúster? 802

¿Cuántos agentes se necesitan para la copia de seguridad y recuperación de los datos del clúster? 800

¿Cuántos dispositivos virtuales necesito? 171

¿Dispositivos de arranque basados en Linux o en WinPE/WinRE? 984

¿Dónde se ven los nombres del archivo de copia de seguridad? 597

¿Los paquetes requeridos ya están instalados? 50

¿Por qué hay copias de seguridad mensuales con un esquema horario? 578

¿Por qué necesita Extended Detection and Response (XDR)? 1339

¿Por qué se debe usar Bootable Media Builder? 986

¿Por qué se debe usar Secure Zone? 549

¿Qué activa una regla de directiva? 1222

¿Qué Agente necesito? 42

¿Qué almacena una copia de seguridad de un disco o volumen? 540

¿Qué elementos de datos pueden recuperarse? 852, 869, 875, 879, 904, 916, 920, 925

¿Qué elementos no se pueden recuperar? 875

¿Qué elementos se pueden incluir en copias de seguridad? 852, 869, 874, 879, 904, 915, 920, 925, 947

¿Qué es un archivo de copia de seguridad? 596

¿Qué es un atasco? 729

¿Qué implica la protección de Google Workspace? 907

¿Qué información se incluye en una fase de ataque? 1291

¿Qué necesito para realizar una copia de seguridad de un sitio web? 947

¿Qué necesito para usar la copia de seguridad compatible con la aplicación? 804

¿Qué son exactamente los incidentes? 1259

¿Qué tipo de copia de seguridad necesito? 41

¿Se muestran los atascos en las cargas de trabajo, los agentes y las ubicaciones de copia de seguridad? 733

¿Un dispositivo de arranque personalizado o uno disponible? 983

A

Acceder a copias de seguridad eliminadas en el almacenamiento inmutable 1573

Acceder a un dispositivo virtual a través de un cliente SSH 186

© Acronis International GmbH, 2003-2025

Acceso a los servicios de Cyber Protection 25

Acceso a sitio web malicioso 1195

Acceso a vulnerabilidades y gestión de parches 1379

Acceso de VPN remoto de punto a sitio 1046

Acceso mediante VPN al sitio local 1049

Acción sobre la detección 1184

Acciones 1224

Acciones adicionales con chats en Cyber Protect Monitor 363

Acciones adicionales con la consola de línea de comandos remota 1480

Acciones adicionales con las sesiones de chat 1503

Acciones adicionales con los mensajes de chat 1505

Acciones adicionales con planes de administración remota 1461

Acciones adicionales con planes de despliegue de software 1437

Acciones adicionales con planes de supervisión 1551

Acciones con planes de protección 251

Acciones de respuesta para los nodos individuales de la cyber kill chain 1307

Acciones predeterminadas 1205

Acerca de Acronis Disaster Recovery 1010

Acerca de la planificación de copia de seguridad 908

Acerca de Secure Zone 549

Acerca del servicio de envío de datos físicos 637

Activación de Extended Detection and Response (XDR) 1340

Activación de la cuenta 22

Activación de Startup Recovery Manager 1008

Activar o desactivar las notificaciones de chat en Cyber Protect Monitor 365

Activar una regla de retención 782

Activar una regla de retención legal 786

Active Protection 30, 1163, 1166

Active Protection en la edición Cyber Backup Standard 1183

Actualización de agentes de protección 121

Actualización de agentes de protección automática 130

Actualización de agentes de protección en cargas de trabajo cifradas con BitLocker 133

Actualización de las definiciones de Cyber Protection bajo demanda 218

Actualización de las definiciones de Cyber Protection mediante la planificación 217

Actualización manual de agentes de protección 128

Actualizaciones automáticas de los componentes 215

Actualizaciones que faltan por categoría 344

Actualizar Agente para Synology 183

Actualizar, reconstruir o eliminar índices 933

Adición de cargas de trabajo a la consola de Cyber Protect 385

Adición de un recurso informático a un plan de despliegue de software 1436

Adición de una carga de trabajo a un plan de administración remota 1460

Adjuntar bases de datos de SQL Server 817

Administración de cargas de trabajo de destino para un plan 494

© Acronis International GmbH, 2003-2025

Administración de organizaciones de Microsoft 365 añadidas en diferentes niveles 843

Advanced Data Loss Prevention 1217

Agent para Scale Computing HC3 508

roles obligatorios 146

Agente instalado de forma local para Office 365 902

Agente para Azure 509

Agente para Exchange (para la copia de seguridad de buzones de correo) 503

Agente para File Sync & Share 502

Agente para Hyper-V 507

Agente para la prevención de la pérdida de datos 502

Agente para la Virtuozzo Hybrid Infrastructure 508

Agente para Linux 504

Agente para Mac 506

Agente para Microsoft 365 503

Agente para MySQL/MariaDB 504

Agente para Nutanix 509

Agente para Oracle 504

Agente para oVirt 508

roles y puertos necesarios 165

Agente para SQL, Agente para Active Directory y Agente para Exchange (para copia de seguridad de bases de datos y copias de seguridad compatibles con la aplicación) 501

Agente para Synology 509

Agente para Virtuozzo 508

Agente para VMware

copia de seguridad sin LAN 961

Agente para VMware (dispositivo virtual) 507

Agente para VMware (Windows) 507

Agente para Windows 499

Agente para Windows (heredado) 500

Agregar credenciales 1464

Agregar o eliminar dispositivos USB de la base de datos 442

Agregar una red de recuperación de producción desde Microsoft Azure 1120

Agregar una red de recuperación de prueba desde Microsoft Azure 1120

Ahorrar batería 570

Ajuste de la configuración de RDP 1467

Ajuste de la configuración del servidor proxy 53

Ajuste de los permisos en las reglas de la directiva de flujo de datos 1222

Ajustes del filtrado de URL 1195

Ajustes del mapa de protección de datos 356

Al ocurrir un evento en el registro de eventos de Windows 565

Alertas 592

Alertas de conexión a nubes públicas 322

Alertas de control de dispositivos 319, 458

Alertas de copia de seguridad 296

Alertas de despliegue del software 326

Alertas de EDR 318

Alertas de filtrado 293

Alertas de filtrado de URL 315

Alertas de licencias 316

Alertas de protección antimalware 310

Alertas de recuperación ante desastres 300

© Acronis International GmbH, 2003-2025

Alertas del servidor en la nube 1158

Alertas del sistema 320

Alertas sobre el estado del disco 340

Algoritmo de distribución 966

Almacenamiento de copias de seguridad 720

Almacenamiento en caché 218

Almacenamiento inmutable 1570

Almacenamiento inmutable para el archivado de correos electrónicos 791

Almacenamiento redundante geográficamente 1574

Almacenamientos y agentes admitidos 1571

Almacenar los eventos de seguridad durante 180 días 1253

Alta disponibilidad de un equipo recuperado 979

Analice la información sobre el incidente 1263

Análisis antimalware de buzones de correo 857

Análisis antimalware de copias de seguridad 1212

Análisis planificado 1165

Antes de empezar 38, 137, 141, 147, 159, 166, 171, 176

Antimalware avanzado 1167

Antivirus Microsoft Defender 1203

Antivirus Microsoft Defender y Microsoft Security Essentials 1203

Anular la asignación de credenciales de una carga de trabajo 1466

Añade o elimina un proceso, archivo o red en la lista de bloqueados o permitidos del plan de protección 1328

Añadir acceso a una conexión de nube pública 758

Añadir archivos en cuarentena a la lista blanca 1211

Añadir cargas de trabajo a los planes de supervisión 1547

Añadir cargas de trabajo a un grupo estático 411

Añadir el acceso a una suscripción de Microsoft Azure 754

Añadir la variable AR_RETENTION_LOCK_SUPPORT 524

Añadir un servidor de correo 763

Añadir VLAN 1001

Apagar máquinas virtuales de destino al iniciar la recuperación 719

Aplicación de medidas de respuesta 1345

Aplicación de un plan de archivado 768

Aplicación de un plan de copia de seguridad 895

Aplicación de un plan de protección a una carga de trabajo 252

Aplicación potencialmente no deseada 1183

Aplicaciones de Cloud 346

Aplicar parche a una carga de trabajo 1314

Aplicar un plan a un grupo 433

Aprobación automática de parches 1401

Aprobar parches manualmente 1406

Aprovisionamiento del disco 960

Archivado de correos electrónicos 762

Archivo comprimido de correo electrónico en inquilinos deshabilitados o eliminados 765

Archivos de registro de VPN de IPsec de varios sitios 1046

© Acronis International GmbH, 2003-2025

Archivos de un script 991

Argumentos del comando 1418

Asignación de clientes 1350

Asignación de credenciales a una carga de trabajo 1465

Asignar sesiones de chat a uno mismo 1500

Atributos de búsqueda para cargas de trabajo de la nube a la nube 416

Atributos de búsqueda para cargas de trabajo que no son de nube a nube 417

Autenticación de doble factor 22

Autoprotección 1169, 1185

Avanzado 1206

Azure Bastion 1117

Azure ExpressRoute 1117

Azure Firewall 1116

B

Basado en Linux 984

Basados en WinPE/WinRE 984

Base de datos de dispositivos USB 453

Biblioteca 1410

Bloqueo de retención 524

Bootable Media Builder 985

Borrado de datos de una carga de trabajo gestionada 462

Borrado de planes predeterminados 238

Buscar 327

Buscar indicadores de compromiso (IoC) y actividades sospechosas 1265

Buscar mensajes en sesiones de chat 1502

Busque indicadores de compromiso (IOC) de ataques conocidos públicamente en sus cargas de trabajo 1298

Búsqueda automática de controladores 708

Búsqueda de correos electrónicos 772

Búsqueda de eventos 1265

Búsqueda en copias de seguridad de nube a nube 931

Búsqueda en el inventario de hardware 1369

Búsqueda en el inventario de software 1376

Búsqueda en los repositorios de software 1412

Búsqueda en Mi bandeja de entrada 27

Búsqueda en todo el texto 932

C

calculate hash 624

Cambiar el formato de copia de seguridad a la versión 12 (TIBX) 601

Cambiar la cuota de servicio de cargas de trabajo 214

Cambio de contraseña de cifrado 1569

Cambio de la cuenta de usuario para agente para VMware 978

Cambio de las credenciales de acceso de Microsoft 365 904

Cambio de las credenciales de acceso de SQL Server o Exchange Server 828

Cambio de los puertos utilizados por el agente de protección 41

Cambio de registro de una carga de trabajo 120

Cambio de VPN de sitio a sitio OpenVPN a VPN IPsec de varios sitios 1033

Cambio de VPN IPsec de varios sitios a OpenVPN de sitio a sitio 1042

© Acronis International GmbH, 2003-2025

Cambio del adaptador gráfico de un dispositivo virtual 165

Cambio del entorno de recuperación 706

Cambio del estado de la secuencia de comandos 486

Cambio del tiempo de espera para el Latido del equipo virtual y la validación de la captura de pantalla 267

Cambios en el identificador de seguridad (SID) 718

Campos de eventos 1276

Capacidades SIEM de Acronis 280

Capturar paquetes de red 1060

Características de la protección antimalware 1164

Características no compatibles 1568

Cargando paquetes de software 1415

Cargas de trabajo 383

Cargas de trabajo agregadas 464

Cargas de trabajo de CyberApp 464

Carpeta personalizada de autoservicio bajo demanda 1210

Caso de uso de aprobación automática de parches sin prueba 1405

Caso de uso de prueba y aprobación automática de parches 1402

Categorías de confidencialidad personalizadas 1241

Categorías que se pueden filtrar 1195

Certificación de copias de seguridad con datos forenses 619

Chat de asistencia 1498

Chats en el Monitor 363

Cifrado 583

Citrix Hypervisor/XenServer 519

Clases de almacenamiento admitidas 749

Claves de acceso 750, 752

Clonación de una secuencia de comandos 484

Códec adaptable 1446

Comando de Post-copia de seguridad 641

Comando de precopia de seguridad 639

Comandos antes de la captura de datos 642

Comandos antes de la recuperación 717

Comandos de desinstalación 1418

Comandos de instalación 1418

Comandos Post de la captura de datos 644

Comandos posteriores a la recuperación 718

Comandos previos o posteriores a la captura de datos 642

Comandos previos/posteriores 639, 716, 960

Comandos y argumentos de instalación y desinstalación 1418

Combinación de las reglas de la directiva de flujo de datos 1224

Cómo agregar o quitar columnas en la vista de diseño de tabla 1268

Cómo agregar paquetes de software desde la biblioteca 1414

Cómo analizar el gráfico XDR 1342

Cómo analizar qué incidentes de seguridad necesitan atención inmediata 1260

Cómo añadir una organización de Microsoft 365 841, 902

Cómo asignar derechos de usuario 68

Cómo cambiar la cuenta de inicio de sesión en equipos Windows 67

Cómo comprender el nivel de protección

© Acronis International GmbH, 2003-2025

actual 288

Cómo comprobar los detalles de una amenaza detectada 859

Cómo crear Secure Zone 550

Cómo deshabilitar el servicio de gestión de Microsoft 365 1352

Cómo eliminar Secure Zone 551

Cómo eliminar una organización de Microsoft 365 845

Cómo empezar a realizar copias de seguridad de los datos 830

Cómo empezar a usar Cyber Protection 22

Cómo funciona 336, 352, 355, 468, 552, 588, 619, 930, 1184, 1193

Cómo funciona el enrutamiento 1021, 1025, 1036

Cómo funciona la conversión periódica a una máquina virtual 276

Cómo ir a las fases del ataque 1291

Cómo la creación de Secure Zone transforma el disco 550

Cómo probar si Endpoint Detection and Response (EDR) funciona correctamente 1337

Cómo quitar el agente para dispositivo virtual de Azure 170

Cómo quitar recursos informáticos de los planes de despliegue de software 1437

Cómo realizar copias de seguridad de máquinas virtuales de Nutanix 176

Cómo realizar una conmutación por error de servidores mediante DNS local 1085

Cómo recuperar canales de equipo o archivos de canales de equipo 882

Cómo recuperar los datos en un dispositivo móvil 831

Cómo reducir los atascos 731

Cómo revisar los datos a través de la consola de Cyber Protect 831

Cómo se realiza una conmutación por error de un servidor DHCP 1085

Cómo se utiliza Endpoint Detection and Response (EDR) 1257

Cómo trabajar con consultas guardadas 1269

Cómo trabajar con el módulo de control de dispositivos 434

Cómo utilizar la notarización 588, 930

Cómo utilizar Secure Zone 531

Comodines 608

Comparación de soluciones de copia de seguridad para datos de Microsoft 365 833

Comparación de versiones de secuencias de comandos 487

Comparación entre la finalización y una recuperación estándar 954

Compartir contenido del portapapeles entre cargas de trabajo 1473

Compatibilidad con almacenamientos Dell EMC Data Domain 524

Compatibilidad con discos duros de formato avanzado (sector de 4 K) 532

Compatibilidad con software de cifrado 531

Compatibilidad de Disaster Recovery con el software de cifrado 1158

Componentes del agente 193

Componentes para una instalación desatendida (EXE) 83

Componentes para una instalación desatendida (MSI) 92

© Acronis International GmbH, 2003-2025

Comprender y personalizar la vista de la cyber kill chain 1289

Compresión de los planes 221

Comprobación de las actividades del cortafuegos de la nube 1076

Comprobación de sus notificaciones 27

Comprobación del estado 1156

Comprobación del estado de validación 269

Comprobar dirección IP del dispositivo 573

Comprobar el tamaño de un índice de búsqueda 933

Comprobar si hay ataques de dominio público en sus cargas de trabajo utilizando las fuentes de información sobre amenazas 1253

Compruebe el acceso a los controladores en el entorno de inicio 708

Conceder los permisos de sistema necesarios para el Agente de Connect 58

Concesión de permiso de acceso a la cuenta de usuario 977

Condiciones de inicio 493, 566

Condiciones de inicio de la tarea 647

Conectar a cargas de trabajo gestionadas mediante una dirección IP 1486

Conectar a cargas de trabajo no administradas a través de Acronis Asistencia rápida 1485

Conectar a una carga de trabajo gestionada a través del cliente web 1471

Conectividad y redes 1020

Conectividad y redes en Microsoft Azure 1115

Conexión a cargas de trabajo administradas para asistencia o escritorio remotos 1468

Conexión a cargas de trabajo para asistencia o escritorio remotos 1441

Conexión a línea de comandos remota 1478

Conexión a un equipo que se inició desde un dispositivo de arranque 1001

Conexión a una cuenta de Microsoft 1349

Conexión local 1001

Conexión OpenVPN de sitio a sitio 1023

Conexión remota a dispositivos descubiertos 210

Conexión remota a una carga de trabajo 1319

Conexión VPN de IPsec de varios sitios 1035

Conexiones a cargas de trabajo remotas para asistencia o escritorio remotos 1448

Conexiones activas de punto a sitio 1050

Conexiones SSH a un dispositivo virtual 185

Configuración de acceso de VPN remoto de punto a sitio 1048

Configuración de Active Protection en Cyber Backup Standard 1184

Configuración de alertas de supervisión 1555

Configuración de conexiones de Microsoft 365 1348

Configuración de cuarentena 1172

Configuración de detección pasiva de dispositivos 196

Configuración de enrutación local 1057

Configuración de filtros de archivo 609

Configuración de gestión de parches en el plan de protección 1391

Configuración de la aprobación automática de parches 1401

Configuración de la autenticación de doble factor para su cuenta 23

© Acronis International GmbH, 2003-2025

Configuración de la conmutación por error de prueba automatizada 1081

Configuración de la conmutación por error de prueba automatizada en Microsoft Azure 1132

Configuración de la copia de seguridad con información de aplicaciones de máquinas virtuales que ejecutan Windows Server 2022 y versiones posteriores 805

Configuración de la evaluación de vulnerabilidades 1382

Configuración de la frecuencia de las copias de seguridad de Google Workspace 914

Configuración de la frecuencia de las copias de seguridad de Microsoft 365 847

Configuración de la lista blanca 1212

Configuración de la protección 215

Configuración de la protección antivirus y antimalware 1160

Configuración de la recopilación de datos forenses 617

Configuración de la red de recuperación de prueba 1120

Configuración de la supervisión de la velocidad de transferencia del disco 1526

Configuración de la supervisión de la velocidad de transferencia del disco por proceso 1533

Configuración de la supervisión de temperatura de la CPU 1518

Configuración de la supervisión de temperatura de la GPU 1520

Configuración de la supervisión del estado de actualización de Windows 1540

Configuración de la supervisión del estado de la función AutoRun 1543

Configuración de la supervisión del estado del cortafuegos 1541

Configuración de la supervisión del estado del servicio de Windows 1536

Configuración de la supervisión del estado del software antimalware 1541

Configuración de la supervisión del registro de eventos de Windows 1538

Configuración de la supervisión del tamaño de archivos y carpetas 1539

Configuración de la supervisión del último reinicio del sistema 1538

Configuración de la supervisión del uso de la CPU 1522

Configuración de la supervisión del uso de la memoria 1524

Configuración de las acciones de respuesta automática 1548

Configuración de los ajustes de Cliente de Connect 1492

Configuración de los ajustes de la protección antivirus y antimalware 1166

Configuración de los ajustes de VPN de IPsec de varios sitios 1037

Configuración de OpenVPN de sitio a sitio 1026

Configuración de privacidad 25

Configuración de red de la puerta de enlace de VPN 1025

Configuración de reglas de cortafuegos para servidores en la nube 1073

Configuración de reglas de retención 580

Configuración de seguridad de IPsec o IKE 1040

Configuración de servidores de recuperación 1061

© Acronis International GmbH, 2003-2025

Configuración de servidores DNS personalizados 1056

Configuración de servidores principales 1066

Configuración de un flujo de trabajo automatizado de Endpoint Detection and Response (EDR) 1333

Configuración de una conexión OpenVPN de sitio a sitio 1027

Configuración de una copia de seguridad de CDP 555

Configuración de Universal Restore 708

Configuración de VPN de IPsec de varios sitios 1036

Configuración del acceso 445

Configuración del archivado de correos electrónicos 763

Configuración del bucket 750, 753

Configuración del dispositivo virtual 138, 143, 156, 162

Configuración del dispositivo virtual de Nutanix 173

Configuración del método predeterminado para actualizar agentes 122

Configuración del modo de visualización 1002

Configuración del modo solo en la nube 1022

Configuración del monitor de cambios de hardware 1521

Configuración del monitor de espacio en disco 1516

Configuración del monitor de estado del proceso 1536

Configuración del monitor de inicios de sesión fallidos 1541

Configuración del monitor de Software instalado 1537

Configuración del monitor de uso de red 1529

Configuración del monitor personalizado 1543

Configuración del número de reintentos en caso de error 268

Configuración del servidor proxy en Cyber Protect Monitor 362

Configuración del uso de la CPU por supervisión del proceso 1531

Configuración del uso de la memoria por supervisión del proceso 1532

Configuración del uso de la red por supervisión del proceso 1534

Configuración personalizada 1182

Configuraciones avanzadas 1230

Configuraciones de clúster compatibles 800-801

Configuraciones de red 1000

Configurar cuentas de usuario en la Virtuozzo Hybrid Infrastructure 148

Configurar directivas de notificaciones por correo electrónico 1563

Configurar el cifrado como una propiedad del equipo 584

Configurar el cifrado en el plan de protección 584

Configurar el objeto de directiva de grupo 135

Configurar el plan de protección Instalación de parches en entornos de producción 1404

Configurar el plan de protección Instalación de parches en entornos de prueba 1403

Configurar el tiempo de los parches en la lista 1400

Configurar los ajustes de red 1001

© Acronis International GmbH, 2003-2025

Configurar redes en la Virtuozzo Hybrid Infrastructure 148

Configurar una copia de seguridad con información de aplicaciones 938

Conmutación por error de Disaster Recovery 1321

Conmutación por error de producción 1082, 1126

Conmutación por error de prueba 1078, 1127

Conmutación por error de prueba automatizada 1080, 1127, 1156

Conmutación por error de prueba automatizada en Microsoft Azure 1131

Conmutación por error de prueba en Microsoft Azure 1128

Conmutación por error en Microsoft Azure 1126

Conmutación por error en una réplica 958

Conmutación por recuperación 959, 1086

Conmutación tras recuperación basada en agente mediante dispositivo de arranque 1087

Conmutación tras recuperación basada en agente mediante dispositivos de arranque de Microsoft Azure 1136

Conmutación tras recuperación desde Cyber Protect Cloud a una máquina virtual de Azure 1099

Conmutación tras recuperación desde Microsoft Azure a una máquina virtual de Azure 1148

Conmutación tras recuperación en Microsoft Azure 1135

Conmutación tras recuperación manual 1097

Conmutación tras recuperación manual desde Microsoft Azure 1146

Conmutación tras recuperación sin agente a través de un agente de hipervisor 1091

Conmutación tras recuperación sin agente mediante un agente de hipervisor desde Microsoft Azure 1140

Consejos importantes 576

Consejos útiles 910

Consola de Cyber Protect 372

Consolidación de la copia de seguridad 595

Consultar las alertas de supervisión para una carga de trabajo 1562

Consultas de búsqueda 771

Consultas de muestra 1273

Contenedor de Proxmox 662

Contenedor de Virtuozzo Hybrid Server 658

Control de errores 605, 714, 960

Controladores de dominio de Active Directory para conectividad OpenVPN L2 1051

Controladores de dominio de Active Directory para conectividad VPN de IPsec L3 1051

Conversión a equipo virtual 273

Conversión periódica a máquina virtual frente a ejecución de una máquina virtual desde una copia de seguridad 276

Copia de bibliotecas de Microsoft Exchange Server 827

Copia de seguridad 529, 533

Copia de seguridad anterior a la actualización 1397

Copia de seguridad basada en agente de máquinas virtuales de Microsoft Azure y Amazon EC2 982

Copia de seguridad basada en agente y sin agente 41

© Acronis International GmbH, 2003-2025

Copia de seguridad compatible con el clúster 801

Copia de seguridad compatible con la aplicación 803

Copia de seguridad de cargas de trabajo de Proxmox 946

Copia de seguridad de casillas de correo 807

Copia de seguridad de equipos Hyper-V en clúster 979

Copia de seguridad de la base de datos 797

Copia de seguridad de los datos del clúster de Exchange 802

Copia de seguridad de un sitio web 947

Copia de seguridad directa en el almacenamiento de copia de seguridad de Microsoft 365 891

Copia de seguridad en almacenamiento compatible con S3 (incluye Wasabi, IONOS Cloud e Impossible Cloud) 751

Copia de seguridad en Amazon S3 749

Copia de seguridad en Microsoft Azure 749

Copia de seguridad sector por sector 646

Copia de seguridad semanal 652

Copias de seguridad de bases de datos incluidas en AAG 800

Copias de seguridad de equipos de Microsoft Azure y Amazon EC2 982

Copias de seguridad de servidores de nube 1072

Copias de seguridad incrementales/diferenciales rápidas 607

Corrección de línea base de inquilinos de forma manual 1359

Corrección de riesgos de usuario 1362

Creación de copias de seguridad en un archivo de copias de seguridad existente 599

Creación de dispositivos de arranque basados en WinPE o WinRE 996

Creación de la directiva de flujo de datos y reglas de la directiva 1218

Creación de servidores de recuperación en Microsoft Azure 1122

Creación de soportes de arranque para recuperar sistemas operativos 983

Creación de un dispositivo de arranque físico 984

Creación de un grupo dinámico 411

Creación de un grupo estático 409

Creación de un plan de administración remota 1450

Creación de un plan de archivado 767

Creación de un plan de programación 490

Creación de un plan de protección 250

Creación de un plan de protección de recuperación ante desastres 1016

Creación de un plan de protección de recuperación ante desastres con Microsoft Azure 1111

Creación de un plan de reenvío SIEM genérico para múltiples clientes 281

Creación de un plan de réplica de copia de seguridad 261

Creación de un plan de replicación 956

Creación de un plan de validación 270

Creación de un plan global de exclusiones de antivirus y antimalware 381

Creación de un plan SIEM para un cliente individual 283

Creación de un runbook 1100

© Acronis International GmbH, 2003-2025

Creación de un runbook en Microsoft Azure 1149

Creación de un servidor de recuperación 1062

Creación de un servidor principal 1067

Creación de un sitio de recuperación ante desastres en Microsoft Azure 1113

Creación de un ticket del centro de asistencia a partir de una alerta 295

Creación de una consulta de búsqueda guardada 774

Creación de una regla de retención 780

Creación de una regla de retención legal 784

Creación de una secuencia de comandos 479

Creación de una secuencia de comandos con IA 481

Creación del archivo de transformación y extracción de los paquetes de instalación 135

Creación y aplicación de un nuevo plan de copias de seguridad 892

Crear grupos de dispositivos estáticos en el nivel de partner 377

Crear un grupo dinámico de dispositivos en el nivel de partner 377

Crear un plan de despliegue de software 1427

Crear un plan de supervisión 1545

Credenciales de la carga de trabajo 1464

Cree un proyecto personal de Google Cloud 910

Cuarentena 1208

Cuotas 950

Cyber Protect Monitor 360, 509

Cyber Protection 329

D

Dar de baja a usuarios 1365

Dar de baja cargas de trabajo 119

Datos considerados información de identificación personal (PII) 1234

Datos considerados Información de Salud Protegida 1233

Datos considerados PCI DSS 1236

Datos forenses 616

Datos informados según el tipo de widget 369

De qué puede realizar una copia de seguridad 829

Deduplicación de datos 529

Deduplicación en archivos comprimidos 602

Defina la configuración de la fuente de información sobre amenazas 1299

Defina las acciones de respuesta para un archivo sospechoso 1326

Defina las acciones de respuesta para un proceso sospechoso 1322

Defina las acciones de respuesta para una carga de trabajo afectada 1309

Defina las acciones de respuesta para una entrada de registro sospechosa 1327

Definición de la contraseña de cifrado 1569

Definición de una ubicación de copia de seguridad en Amazon S3 737

Definición de una ubicación de copia de seguridad en un almacenamiento compatible con Wasabi, IONOS Cloud, Impossible Cloud o S3 742

Definición del modo del producto 1351

Definiciones de datos confidenciales 1232

© Acronis International GmbH, 2003-2025

Definir una ubicación de copia de seguridad en Microsoft Azure 734

Dependencia de Internet 1134

Depósito de secuencia de comandos 488

Derechos de usuario necesarios 808, 839, 907

Derechos de usuario necesarios para copias de seguridad con información de aplicaciones 805

Desactivación de Startup Recovery Manager 1009

Descarga de agentes de protección 49

Descarga de archivos adjuntos 790

Descarga de archivos de registro de VPN de IPsec 1045

Descarga de archivos en la consola de Web Restore 697

Descarga de direcciones MAC 1058

Descarga de registros de la puerta de enlace VPN 1059

Descarga de registros del dispositivo VPN 1059

Descarga de un informe de licencias para el archivado de correos 765

Descarga del programa de instalación 178

Descargar configuración para OpenVPN 1049

Descargar datos de cargas de trabajo afectadas recientemente 346

Descargar el resultado de una operación de programación 488

Descripción de la detección de atascos 729

Descripción de la opción 624

Descripción de soluciones de alta disponibilidad de SQL Server 799

Deshabilitación de la conexión de sitio a sitio 1034

Deshabilitación de la conmutación por error de prueba automatizada 1081, 1133

Deshabilitación de la Recuperación con un clic 631

Deshabilitar el almacenamiento con redundancia geográfica 1576

Deshabilitar el DRS automático para el agente 137

Deshabilitar la asignación automática para un agente 967

Deshabilitar la búsqueda de texto completo para las copias de seguridad de Gmail 935

Deshabilitar una regla de retención 782

Deshabilitar una regla de retención legal 786

Deshacer la eliminación de correos electrónicos en almacenamiento inmutable 791

Desinstalación de agentes 73

Desinstalación de software 1423

Despliegue de Agente para Nutanix AHV 171

Despliegue de agentes de protección a través de la directiva de grupo 134

Despliegue de dispositivos virtuales 137

Despliegue del agente para Azure 166

Despliegue del agente para el dispositivo virtual de Azure 167

Destinos compatibles 555

Detalles del análisis de copias de seguridad 345

Detección activa de dispositivos mediante Device Sense ™ 197

Detección automatizada de destino 1231

Detección de Cryptomining 1188

Detección de dispositivos 186

© Acronis International GmbH, 2003-2025

Detección de dispositivos mediante Device Sense ™ 194

Detección de varios dispositivos 187

Detección del proceso de criptominería 1171

Detección pasiva de dispositivos mediante Device Sense ™ 196

Detección pasiva de la solución de problemas 211

Detección por tácticas 334

Detectores de contenido personalizados 1242

Detención de la ejecución de un runbook 1104

Detención de una conmutación por error 958

Detener una conmutación por error 1086

Diferencias entre la replicación y la copia de seguridad 955

Diferentes opciones de inicio de sesión 1447

Direcciones IP de prueba y públicas 1051

Direcciones IP públicas 1117

Disaster Recovery para Cyber Protect Cloud 1010

Disaster Recovery para Microsoft Azure 1106

Disponibilidad de las opciones de copia de seguridad 589

Disponibilidad de las opciones de recuperación 710

Dispositivo VPN 1026

Dispositivos de arranque basados en Linux 986

Dispositivos de arranque basados en Windows 995

Dispositivos detectados 330

Dispositivos elegibles para la recuperación ante desastres 1155

Dispositivos móviles compatibles 829

Distribución de los principales incidentes por carga de trabajo 331

División 646

Dónde obtener la aplicación Acronis Cyber Protect 830

E

Edición de la configuración del servidor de recuperación 1126

Edición de la configuración predeterminada de un servidor de recuperación 1018

Edición de paquetes de software 1419

Edición de un grupo dinámico 431

Edición de un plan de archivado 768

Edición de un plan de copia de seguridad 894

Edición de un plan de protección 253

Edición de una consulta de búsqueda guardada 777

Edición de una regla de retención 782

Edición de una regla de retención legal 786

Edición o eliminación de una secuencia de comandos 485

Ejecución de comandos anteriores y posteriores a la instantánea automáticamente 968

Ejecución de copias de seguridad de nube a nube de forma manual 278

Ejecución de un análisis #CyberFit Score 472

Ejecución de un análisis de detección activa de dispositivos mediante Device Sense ™ 198

Ejecución de un equipo virtual desde una copia de seguridad (Instant Restore) 951

Ejecución de un runbook 1104

© Acronis International GmbH, 2003-2025

Ejecución de una conmutación por error permanente 959

Ejecución de una prueba de conmutación por error 1078

Ejecución del equipo 952

Ejecución rápida de la secuencia de comandos 496

Ejecutar autodetección de equipos en el nivel de partner 377

Ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros 1405

Ejecutar la línea de comando remota 1320

Ejecutar una consulta de búsqueda guardada 777

Ejecutar una copia de seguridad en una planificación 559

Ejecutar una copia de seguridad forense bajo demanda en una carga de trabajo 1318

Ejecutar una copia de seguridad manualmente 574

Ejemplo 77, 87, 101, 568-573, 579

- Copia de seguridad de emergencia en case de bloques dañados en el disco duro 566
- Instalación manual de los paquetes en Fedora 14 53

Ejemplos 76, 78, 86-87, 99, 150, 154

Ejemplos de filtros 609

Ejemplos de uso 581, 952, 955, 968

El flujo de trabajo de gestión de parches 1390

El servidor de la ubicación de copia de seguridad está disponible 568

El usuario está inactivo 568

Elementos afectados recientemente 345

Eliminación automática de entornos de clientes que no se usan en el sitio en la nube 1015

Eliminación de cargas de trabajo de la consola de Cyber Protect 390

Eliminación de cargas de trabajo de un plan de administración remota 1460

Eliminación de copias de seguridad 727

Eliminación de copias de seguridad fuera de la consola de Cyber Protect 728

Eliminación de paquetes de software 1419

Eliminación de planes de favoritos 241

Eliminación de servidores DNS personalizados 1057

Eliminación de todas las alertas 355

Eliminación de un plan de archivado 769

Eliminación de un plan de copias de seguridad 900

Eliminación de un plan de protección 256

Eliminación de un plan SIEM 286

Eliminación de un servidor de recuperación 1126

Eliminación de una conexión a la nube pública 761

Eliminación de una consulta de búsqueda guardada 778

Eliminación de una regla de retención 783

Eliminación de una regla de retención legal 787

Eliminación del equipo 953

Eliminación reversible de inquilinos que tienen un sitio de recuperación en Microsoft Azure 1154

Eliminar credenciales 1466

© Acronis International GmbH, 2003-2025

Eliminar el acceso a una suscripción de Microsoft Azure 756

Eliminar el sitio de DR de Microsoft Azure 1115

Eliminar el sitio de recuperación ante desastres 1105

Eliminar un grupo 432

Eliminar un servidor de correo 765

En Cyber Protect Cloud 840

En Cyber Protection 907

En Google Workspace 907

En Microsoft 365 840

Encienda el equipo virtual de destino cuando haya finalizado la recuperación. 719

Endpoint Detection and Response (EDR) 1250

Enlace de equipos virtuales 966

Enlace manual 967

Enrutamiento de subredes (rutas definidas por el usuario) 1117

Entender el ámbito y el impacto de los incidentes 1262

Entienda las acciones emprendidas para mitigar un incidente 1295

Entornos de recuperación 705

Envío de datos físicos 637

Equipo físico 656

Equipo virtual de Virtuozzo Hybrid Infrastructure 659

Equipo virtual Nutanix 661

Equipos vulnerables 342

Escenarios de usos 723

Espacio libre en disco que se requiere para la actualización 121

Esperar hasta que se cumplan las condiciones de la planificación 648

Esquemas de copia de seguridad 557

Establecer el orden de los planes favoritos 242

Establecer la contraseña root en un dispositivo virtual 186

Establecimiento de planes como favoritos 240

Establecimiento de planes como predeterminados 237

Estado de instalación del parche 343

Estado de la actividad de validación 269

Estado de la amenaza 332

Estado de la protección 330

Estado de la red de las cargas de trabajo 334

Estado de validación 268

Estado del plan 248

Estándar de Seguridad de los Datos para la Industria de Tarjetas de Pago (PCI DSS) 1236

Estructura de autostart.json 992

Estructura de la directiva de flujo de datos 1220

Estructura de la regla 1220

Evaluación de vulnerabilidades 1379

Evaluación de vulnerabilidades para dispositivos macOS 1386

Evaluación de vulnerabilidades para equipos Linux 1386

Evaluación de vulnerabilidades para equipos Windows 1385

Eventos para la prevención de pérdida de datos 1238

Evitar copias de seguridad duplicadas de grupos de Microsoft 365 851

© Acronis International GmbH, 2003-2025

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

Evitar la desinstalación o modificación de agentes no autorizadas 212

Excluir dispositivos USB individuales del control de acceso 442

Excluir subclases de dispositivo del control de acceso 441

Exclusión de dispositivos de la detección 209

Exclusión de procesos del control de acceso 456

Exclusiones 1189, 1207

Exclusiones de archivos 715

Exclusiones de protección 1179

Exclusiones de URL 1202

Exportación de copias de seguridad 725

Exportar chats 1501

Exportar un plan de protección 254

Expresión lógica para el idioma japonés 1236

Expresión lógica para todos los idiomas admitidos menos el japonés 1235

Expresión lógica utilizada para la detección de contenido 1233, 1235, 1237

Extended Detection and Response (XDR) 1339

Extensiones y reglas de excepción 358

Extracción de archivos MSI, MST y CAB 84

Extraer archivos de copias de seguridad locales 701

F

Fecha y hora de los archivos 713

Filtrado de URL 1192

Filtrar sesiones de chat 1502

Filtros de archivo (inclusiones y exclusiones) 607

Finalización de equipos en ejecución a partir de copias de seguridad en la nube 954

Finalización del equipo 953

Firma de un archivo con ASign 699

Flashback 715

Flujo de trabajo de la configuración del filtrado de URL 1195

Flujos de trabajo de Endpoint Detection and Response (EDR) 1330

Formato de la copia de seguridad 600

Formato y archivos de copia de seguridad 601

Fuente de amenazas 352

Fuentes de datos compatibles 554

Funcionamiento del servicio de Formación en concienciación sobre seguridad 1577

Funciones 1251

Funciones compatibles por plataforma 1161

Funciones de asistencia y escritorio remotos 1442

Funciones de protección compatibles con el sistema operativo 28

G

Generalidades de clústeres de Exchange Server 801

Generar un token de registro 112

Gestión 326

Gestión de cargas de trabajo en la consola de Cyber Protect 372

Gestión de energía de VM 718, 960

Gestión de la configuración de la conexión de punto a sitio 1049

Gestión de la configuración del dispositivo VPN 1028

© Acronis International GmbH, 2003-2025

Gestión de la copia de seguridad y recuperación de cargas de trabajo y archivos 499

Gestión de licencias para servidores de gestión locales 220

Gestión de los archivos detectados que no tienen protección 356

Gestión de los archivos que están en cuarentena 1209

Gestión de parches 1390

Gestión de redes 1051

Gestión de redes en el modo Solo en la nube 1022

Gestión de redes en Microsoft Azure 1118

Gestión de redes para OpenVPN de sitio a sitio 1029

Gestión de software 1374

Gestión de tokens de registro 114

Gestión de usuarios de Microsoft 365 1361

Gestión de vulnerabilidades encontradas 1387

Gestión del acceso a otros servicios de almacenamiento en la nube pública 757

Gestión del cortafuegos 1207

Gestión del inventario de hardware 1367

Gestión del inventario de software 1374

Gestión del sitio de recuperación ante desastres en Microsoft Azure 1112

Gestión y supervisión del entorno de Microsoft 365 1348

Gestionar el acceso a la cuenta de la nube pública 748

Gestionar el acceso a las suscripciones de Microsoft Azure 753

Gestionar el acceso a su suscripción de Microsoft Azure 1110

Gestionar los incidentes en la página Incidentes 1252

Gestione el aislamiento de red de una carga de trabajo 1310

get content 623

Grabar y reproducir sesiones remotas 1491

Gráfico de quemado de incidentes de seguridad 333

Grupos de los dispositivos 406

Grupos de nube a nube y grupos que no son de nube a nube 408

Grupos de palabras clave 1238

Grupos de seguridad de red (NSG) 1116

Grupos dinámicos 408

Grupos dinámicos y estáticos 407

Grupos estáticos 408

Grupos integrados 407

Grupos integrados y grupos personalizados 407

Grupos personalizados 407

Guardar información del sistema si falla una acción de recuperación con reinicio 714

Guardar un archivo de registro del agente 219

H

H.264 1446

Habilitación de la conectividad de sitio a sitio 1026

Habilitación de la funcionalidad Endpoint Detection and Response (EDR) 1254

Habilitación de la recuperación con un clic 629

Habilitación de los servicios de ubicación en el sistema operativo 1496

© Acronis International GmbH, 2003-2025

Habilitación del almacenamiento inmutable 1571

Habilitación del modo compatible con FIPS para un dispositivo virtual 65

Habilitación del uso del módulo de control de dispositivos en macOS 438

Habilitación o deshabilitación de la corrección automática de las desviaciones de línea base 1360

Habilitar Advanced Data Loss Prevention en los planes de protección 1228

Habilitar el almacenamiento con redundancia geográfica 1575

Habilitar el modo de supervisión para Endpoint Detection and Response (EDR) 1335

Habilitar la búsqueda mejorada en copias de seguridad cifradas 934

Habilitar o deshabilitar el análisis de inventario de hardware 1367

Habilitar o deshabilitar el análisis del inventario de software 1374

Habilitar o deshabilitar el control de dispositivos 437

Habilitar o deshabilitar las notificaciones del sistema operativo y alertas del servicio 441

Habilitar o deshabilitar un plan de protección 255

Habilitar y deshabilitar la gestión del cortafuegos 1208

Hacer copias de seguridad de cargas de trabajo en nubes públicas 734

Herramienta "tibxread" para obtener datos incluidos en una copia de seguridad 621

Herramientas de Cyber Protection adicionales 1568

Historial de actividad del incidente 332

Historial de instalación de parches 344

Hoja de referencia de la copia de seguridad 535

I

Iconos del gráfico XDR 1346

Idiomas admitidos 1232-1233, 1236-1237

Ignorar errores 714

Ignorar escritores de VSS fallidos 649

Ignorar los sectores defectuosos 606

Imágenes basadas en WinPE 996

Imágenes basadas en WinRE 996

Implementación de Agent para Scale Computing HC3 (dispositivo virtual) 141

Implementación de Agente para VMware (dispositivo virtual) 137

Implementación de la plantilla de OVA 160

Implementación de la plantilla de QCOW2 142, 155, 172

Implementación de la plantilla OVF 138

Implementación de la recuperación ante desastres 1010

Implementación del Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual) 147

Implementando Agent para oVirt (dispositivo virtual) 159

Implementar Agente para Synology 176

Importación de planes de programación 496

Importando correos electrónicos desde archivos PST 769

Importar un plan de protección 254

© Acronis International GmbH, 2003-2025

Inclusión automática de aplicaciones en la lista blanca 1211

Inclusión manual de aplicaciones en la lista blanca 1211

Incorporación de una organización de Google Workspace 909

Incorporación de usuarios 1361

Incorporación de varios dispositivos 189

Índices de búsqueda 932

Información de identificación personal (PII) 1233

Información de salud protegida (PHI) 1232

Información general 27

Información general a simple vista en el panel de control 1253

Información general acerca del proceso de envío de datos físicos 638

Información para administradores de partners 390

Informe de licencia de usuarios de Microsoft 365 846

Informes 365

Infraestructura de red en la nube predeterminada 1019

Inhabilitación del almacenamiento inmutable 1572

Iniciar Secure Shell 185

Iniciar un chat con un usuario remoto 1499

Iniciar un chat en Cyber Protect Monitor 363

Inicio manual de un análisis de inventario de hardware 1368

Inicio manual de un análisis de inventario de software 1375

Inquilinos en el modo de cumplimiento 702

Instalación de Agente para Proxmox 945

Instalación de Agente para Synology 178

Instalación de agentes de protección en Linux 70

Instalación de agentes de protección en macOS 72

Instalación de agentes de protección en Windows 65

Instalación de agentes de protección utilizando la interfaz gráfica de usuario 65

Instalación de agentes y componentes (combinación de MSI y MST) 85

Instalación de los paquetes del repositorio 51

Instalación de software 1420

Instalación del agente de máquina virtual de Microsoft Azure con acceso a Internet 1134

Instalación del Agente de máquina virtual de Microsoft Azure sin acceso a Internet 1134

Instalación del Agente para Linux en el modo compatible con FIPS 64

Instalación del Agente para Windows en modo compatible con FIPS 61

Instalación desatendida y desinstalación con un archivo EXE 75

Instalación desatendida y desinstalación con un archivo MSI 84

Instalación dinámica de componentes 57

Instalación e implementación de los agentes de Cyber Protection 38

Instalación manual de los paquetes 52

Instalación remota de agentes 201, 205

Instalación y desinstalación de agentes de protección en Linux 93

© Acronis International GmbH, 2003-2025

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

Instalación y desinstalación de agentes de protección en macOS 100

Instalación y desinstalación de agentes de protección en Windows 75

Instalación y desinstalación de agentes de protección utilizando la interfaz de línea de comandos 75

Instalación y desinstalación de agentes y componentes (EXE) 76

Instalación y desinstalación de agentes y componentes (MSI y selección directa) 85

Instalar de todos maneras los controladores de los dispositivos de almacenamiento masivo 709

Instalar parches bajo demanda 1406

Instantánea de la copia de seguridad a nivel de archivo 615

Instantánea multivolumen 627

Instantáneas intermedias 277

Integraciones para DirectAdmin, cPanel y Plesk 951

Interacción con otras opciones de copia de seguridad 642

Investigación de incidentes 1284

Investigación de nodos individuales 1343

Investigar nodos individuales en la cyber kill chain 1293

Investigue las fases del ataque de un incidente 1290

L

La compatibilidad del formato de copia de seguridad en las diferentes versiones del producto 602

La funcionalidad clave 1010

La pestaña Actividades 359

Lenguaje de consulta XDR de Acronis (XQL) 1270

Licencia de Disaster Recovery para Microsoft Azure 1109

Limitaciones 61, 148, 160, 172, 178, 275, 336, 475, 513, 516, 518, 520, 522-523, 538-539, 543, 546, 549, 663, 678, 697, 706, 713, 720, 763, 770, 839, 858, 869, 874, 879, 908, 916, 920-921, 925-926, 937, 947, 956, 963, 1008, 1013, 1108, 1134, 1214, 1568, 1574

Limitaciones al usar el almacenamiento en la nube con redundancia geográfica 1015

Limitaciones de los nombres de archivos de copia de seguridad 597

Limitaciones para cargas de trabajo de Proxmox 944

Limitaciones para recuperar archivos en la consola de Cyber Protect 702

Limitaciones y problemas conocidos 890

Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo 980

Limpieza 272

Líneas base de inquilinos 1356

Linux 541

list backups 622

list content 622

Lista de dispositivos USB en un equipo 456

Lista de dispositivos USB permitidos 452

Lista de permitidos corporativa 1210

Lista de tipos de dispositivo permitidos 450

Listas de planes de reenvío SIEM 280

© Acronis International GmbH, 2003-2025

Llevar a cabo acciones de control en cargas de trabajo gestionadas 1475

Lo que necesita saber sobre conversión 274

Lo que necesita saber sobre la finalización 954

Lo que se puede hacer con una réplica 956

Los notificadores del escritorio remoto 1493

Los usuarios cerraron la sesión 569

M

Mac 541

Manejo de conflictos de direcciones IP en la conmutación por error 1127

Manejo de fallos de la tarea 647

Mapa de la organización 1245

Mapa de protección de datos 340, 355

Máquina virtual Broadcom (VMware) ESXi 656

Máquina virtual de Microsoft Azure 657

Máquina virtual de Proxmox 661

Máquina virtual de Red Hat Virtualization/oVirt 660

Máquina virtual de Scale Computing HyperCore 660

Máquina virtual de Virtuozzo Hybrid Server 658

Máquina virtual Microsoft Hyper-V 657

Marcado como confidencial 1237

McAfee Endpoint Encryption y PGP Whole Disk Encryption 532

Mecanismo de puntuación de #CyberFit Score 468

Medidas de respuesta manuales 1559

Mejores prácticas para la configuración de red de Disaster Recovery 1118

Método de seguimiento de geolocalización compatible por sistema operativo 1495

Métodos de planes de reenvío SIEM 286

Métodos de validación 265

Mi bandeja de entrada 27

Microsoft 515

Microsoft 365 Business (copia de seguridad) 848

Microsoft BitLocker Drive Encryption 531

Microsoft Exchange Server 604

Microsoft Security Essentials 1204

Microsoft SQL Server 603

Mis paquetes 1411

Modificación de un plan de reenvío SIEM 285

Modo compatible con FIPS 60

Modo de arranque 712

Modo de copia de seguridad de clústeres 603

Modo de cumplimiento 1568

Modo solo en la nube 1021

Modos de almacenamiento inmutables 1571

Monitores configurables 1508

Montaje de bases de datos de Exchange Server 820

Montaje de volúmenes desde una copia de seguridad 723

Motivos para usar la copia de seguridad compatible con la aplicación 803

Motor de comportamiento 1172

N

Navegadores web compatibles 26

NEAR 1446

© Acronis International GmbH, 2003-2025

Niveles de administración en la consola de Cyber Protect 373

No iniciar con conexiones a las siguientes redes Wi-Fi 572

No iniciar con conexiones de uso medido 571

No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso) 606, 714

No se realizan copias de seguridad correctamente durante un número especificado de días 592

Nombre de archivo de copia de seguridad predeterminado 597

Nombre del archivo de copia de seguridad. 596

Nombres sin variables 598

Normas de retención 575, 779

Nota para los usuarios de Mac 655

Notarización 587, 929

Notificaciones del sistema operativo y alertas del servicio 449

Novedades de la consola de Cyber Protect 373

Nubes públicas 515

Nutanix 522

O

Objeto de nivel superior 992

Objeto de variable 992

Observar varias cargas de trabajo gestionadas de manera simultánea 1483

Obtener el certificado de copias de seguridad con datos forenses 620

Obtener el ID y el secreto de la aplicación 902

Omitir la ejecución de tarea 648

Opción de almacenamiento avanzada 548

Opciones de copia de seguridad 589

Opciones de copia de seguridad predeterminadas 588

Opciones de planificación adicionales 573

Opciones de recuperación 710

Opciones de recuperación tras error 960

Opciones de reinicio 1396

Opciones de replicación 959

OpenVPN de sitio a sitio

información adicional 1578

Operaciones admitidas con volúmenes lógicos 529

Operaciones con copias de seguridad 720

Operaciones con máquinas virtuales de Microsoft Azure 1014

Operaciones con runbooks 1104

Operaciones con runbooks en Microsoft Azure 1152

Operaciones con servidores de recuperación 1065

Operaciones con servidores principales 1069

Operaciones especiales con equipos virtuales 951

Operaciones locales con dispositivos de arranque 1002

Operaciones remotas con soportes de arranque 1003

Operadores de búsqueda 414

Oracle 521

Ordenación de alertas 294

Organización (runbooks) 1099

Otras opciones 561

© Acronis International GmbH, 2003-2025

Otros requisitos para copias de seguridad compatibles con la aplicación 795

Otros requisitos para equipos virtuales 806

oVirt/Red Hat Virtualization 4.2 y 4.3/Oracle Virtualization Manager 4.3 165

oVirt/Red Hat Virtualization 4.4 y 4.5 165

P

Página de administración de la base de datos de dispositivos USB 454

Panel de control Actividades 289

Panel de control de Alertas 290

Panel de control de concienciación 1577

Panel de control de Información general 288

Panel de control de recuperación ante desastres 1155

Paquetes de Linux necesarios para la instalación de agentes en Linux 50

Paquetes de software 1410

Parallels 521

Parámetros 987

Parámetros adicionales 98

Parámetros básicos 96

Parámetros de desinstalación 99

Parámetros de información 98

Parámetros de instalación 96

Parámetros de instalación o desinstalación sin supervisión 95

Parámetros de kernel 987

Parámetros de registro 97

Parámetros de runbook 1102

Parámetros de runbook en Microsoft Azure 1151

Parámetros del evento 565

Parámetros para funciones heredadas 99

Parámetros para una instalación desatendida (EXE) 78

Parámetros para una instalación desatendida (MSI) 88

Paso 1 38

Paso 2 38

Paso 3 38

Paso 4 39

Paso 5 39

Paso 6 41

Pasos para investigar incidentes en la cyber kill chain 1285

Permisos 1224

Permisos de directiva 749, 751

Permisos obligatorios para la instalación sin supervisión en macOS 102

Permitir copia de seguridad completa de VSS 650

Permitir tráfico DHCP a través de VPN L2 1033

Personalización del panel de control Alertas 291

Planes compatibles con grupos de dispositivos 409

Planes de administración remota 1450

Planes de administración remota integrados 235

Planes de análisis de copia de seguridad 277

Planes de archivos comprimidos 766

Planes de copias de seguridad aplicados y programados para cargas de trabajo de Microsoft 365 848

© Acronis International GmbH, 2003-2025

Planes de copias de seguridad para aplicaciones en la nube 278

Planes de implementación de software 1427

Planes de programación 489

Planes de protección de datos fuera del host 260

Planes de protección individual para integraciones del panel de control de alojamiento 257

Planes de protección integrados 224

Planes de protección y módulos 249

Planes de reenvío de SIEM 279

Planes de supervisión 1507, 1545

Planes de supervisión integrados 233

Planes en diferentes niveles de administración 246

Planes favoritos 240

Planes integrados 224

Planes predeterminados 237

Planes preseleccionados 244

Planificación 356, 492, 645, 1383, 1394

Planificación por eventos 562

Planificación y condiciones de inicio 492

Planificar análisis 1175, 1204

Planificar por hora 560

Plataformas compatibles 475

Plataformas compatibles con la supervisión 1508

Plataformas de virtualización compatibles 511, 1012, 1107

Por qué necesita Endpoint Detection and Response (EDR) 1250

Preconfiguración de múltiples conexiones de red 1000

Preparación 38, 708

WinPE 2.x y 3.x 998

WinPE 4.0 y posterior 998

Preparación de equipos para la instalación remota mediante el uso de un GPO 203

Preparación de los equipos para la instalación remota manual 202

Preparar los controladores 708

Prevención de vulnerabilidades 1173

Priorice qué incidentes necesitan atención inmediata 1259

Prioridad de la CPU 635

Privilegios necesarios para el agente para VMware 971

Privilegios necesarios para la cuenta de inicio de sesión 68

Problemas conocidos 938

Problemas conocidos y limitaciones 1248

Problemas de compatibilidad con los planes 257

Problemas de configuración entre suscripciones en Microsoft Azure 1111

Procedimientos de recuperación específicos del software 531

Proceso de copia de seguridad forense 617

Proceso de la conmutación por error de prueba 1129

Proceso de Universal Restore 709

Producto de prueba de Disaster Recovery 1014

Productos de Apple compatibles 1381

Productos de Apple y de terceros compatibles con la evaluación de vulnerabilidades 1381

© Acronis International GmbH, 2003-2025

Productos de Linux compatibles para la evaluación de vulnerabilidades 1382

Productos de Microsoft 1392

Productos de Microsoft compatibles 1380

Productos de Microsoft y de terceros compatibles con la evaluación de vulnerabilidades 1380

Productos de terceros a Windows 1393

Productos de terceros compatibles con Windows 1381

Productos de terceros compatibles para macOS 1382

Programación de copia de seguridad 556

Protección antivirus y antimalware 1164

Protección continua de datos (CDP) 552

Protección contra malware y antivirus 31, 1161

Protección de aplicaciones de colaboración y comunicación 279

Protección de aplicaciones de Microsoft 792

Protección de archivos de Google Drive 920

Protección de archivos de OneDrive 869

Protección de archivos de unidades compartidas 925

Protección de base de datos de Oracle 936

Protección de carpetas de red 1167, 1187

Protección de cuadernos de OneNote 889

Protección de datos de MySQL y MariaDB 936

Protección de dispositivos móviles 828

Protección de entornos de virtualización 970

Protección de licencias de la app de colaboración de Microsoft 365 890

Protección de los buzones de correo de Exchange Online 904

Protección de los datos de Exchange Online 852

Protección de los datos de Gmail 915

Protección de los datos de Google Workspace 907

Protección de los datos de Microsoft 365 833

Protección de los equipos virtuales y contenedores Proxmox 943

Protección de los grupos de disponibilidad Always On (AAG) 799

Protección de los grupos de disponibilidad de bases de datos (DAG) 801

Protección de los sitios web 946

Protección de Microsoft 365 Teams 879

Protección de Microsoft SharePoint 793

Protección de Microsoft SQL Server y Microsoft Exchange Server 792

Protección de SAP HANA 936

Protección de servidores de alojamiento web 950

Protección de sitios de SharePoint Online 874

Protección de sitios web y servidores de alojamiento 946

Protección de un controlador de dominio 793

Protección del servidor 1168, 1187

Protección en tiempo real 1165, 1174, 1205

Protección inteligente 352

Protocolos de conexión remota 1446

Proxmox VE 519

Puerta de enlace de VPN 1025, 1036

Puertos 1027

Puertos necesarios 166

Puertos necesarios para el componente de

© Acronis International GmbH, 2003-2025

descarga 40

Puertos utilizados por Device Sense ™ 198

Puntos de cálculo 1076

Puntos de montaje 626, 716

Puntos de restauración de Azure 593

Gestión de discos no compatibles 594

Nivel de coherencia 593

Retención 593

Q

Qué analizar 1382

Qué hacer a continuación 1018

Qué necesita saber 829

Qué replicar 262

R

RDP 1447

Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque 1089

Realización de conmutación tras recuperación basada en agente mediante dispositivo de arranque desde Microsoft Azure 1137

Realización de conmutación tras recuperación sin agente a través de un agente de hipervisor 1093

Realización de conmutación tras recuperación sin agente a través de un agente hipervisor desde Microsoft Azure 1142

Realización de pruebas en una réplica 957

Realización de una conmutación por error 1083

Realización de una conmutación por error de producción en Microsoft Azure 1128

Realización de una conmutación tras recuperación manual 1097

Realización de una conmutación tras recuperación manual desde Microsoft Azure 1146

Realización de una prueba de conmutación por error en Microsoft Azure 1130

Reasignación de direcciones IP 1055

Reasignar sesiones de chat 1501

Recibir notificaciones de alerta cuando ocurra una infracción 1252

Recomendaciones 713, 1135

Recomendaciones generales para sitios locales 1039

Recomendaciones para la disponibilidad de AD DS en el sitio de DR en Azure 1119

Recomendaciones para la disponibilidad de servicios de dominio de Active Directory 1050, 1119

Recomendaciones y medidas de corrección 1253

Recopilación automática de datos de rendimiento 217

Recopilación de una réplica inicial 960

Recuperación 530, 653

Recuperación a contenedores o máquinas virtuales Virtuozzo 702

Recuperación a partir de la copia de seguridad 1320

Recuperación con reinicio 704

Recuperación con soporte de arranque in situ 1003

Recuperación con un clic 628

Recuperación de aplicaciones 793

Recuperación de apuntes 653

© Acronis International GmbH, 2003-2025

Recuperación de archivos 695

Recuperación de archivos de Google Drive 923

Recuperación de archivos de OneDrive 872

Recuperación de archivos de unidades compartidas 928

Recuperación de archivos en la consola de Cyber Protect 695

Recuperación de archivos usando dispositivos de arranque 700

Recuperación de bases de datos 940

Recuperación de bases de datos de Exchange 817

Recuperación de bases de datos de SQL como archivos 814

Recuperación de bases de datos del sistema 816

Recuperación de bases de datos incluidas en un AAG 800

Recuperación de bases de datos SQL 809

Recuperación de blocs de notas de OneNote de los que se han hecho copia de seguridad 889

Recuperación de buzones de correo 822, 860, 905, 917

Recuperación de buzones de correo y elementos de los buzones 860, 905, 917

Recuperación de cargas de trabajo de Proxmox 946

Recuperación de carpetas públicas y elementos de carpeta 867

Recuperación de contenedores 691

Recuperación de copias de seguridad en inquilinos en el modo de cumplimiento 1570

Recuperación de correos electrónicos, carpetas y buzones de correo 788

Recuperación de datos a partir de una copia de seguridad con información de aplicaciones 939

Recuperación de datos de SharePoint Online 877

Recuperación de datos de un archivo comprimido de correos electrónicos 787

Recuperación de datos forenses 618

Recuperación de elementos de buzón de correo 824, 861, 906, 918

Recuperación de elementos de buzón de correo y de buzones de correo de Exchange 821

Recuperación de elementos de una copia de seguridad 897

Recuperación de elementos del buzón de correo del equipo en archivos PST 885

Recuperación de elementos del buzón de correo en archivos PST 865

Recuperación de equipos físicos 663

Recuperación de Google Drive y archivos de Google Drive 922

Recuperación de instancias 940

Recuperación de la base de datos maestra 816

Recuperación de la configuración de ESXi 703

Recuperación de las bases de datos de SQL en un equipo original 809

Recuperación de las bases de datos de SQL en un equipo que no sea original 811

Recuperación de los datos del clúster de Exchange 803

Recuperación de OneDrive y archivos de OneDrive 871

Recuperación de ruta completa 715

© Acronis International GmbH, 2003-2025

Recuperación de rutinas almacenadas 943

Recuperación de tablas 942

Recuperación de todo el servidor 940

Recuperación de un equipo completo 881

Recuperación de un equipo físico como un equipo físico 664

Recuperación de un equipo físico en una máquina virtual 665

Recuperación de un Google Drive completo 922

Recuperación de un OneDrive completo 871

Recuperación de un sitio de equipo o de elementos específicos de un sitio 888

Recuperación de un sitio web 949

Recuperación de una máquina virtual como máquina virtual 680

Recuperación de una máquina virtual como un equipo físico 679

Recuperación de una unidad compartida completa 927

Recuperación de unidades compartidas y archivos de unidades compartidas 927

Recuperación del buzón de correo de un equipo 885

Recuperación del equipos virtuales 678

Recuperación del estado del sistema 703

Recuperación del servidor de recuperación en conmutación por error a un momento dado anterior 1127

Recuperación desde el almacenamiento en la nube 990

Recuperación desde un recurso compartido de red 990

Recuperación Máquinas equipos de Microsoft Azure y Amazon EC2 983

Recuperación multiplataforma 654-655

Recuperación multiplataforma mediante dispositivos de arranque 662

Recuperación segura 719

Recuperar discos usando dispositivos de arranque 693

Recuperar mensajes de correo electrónico y reuniones 887

Recuperar todos los buzones de correo en archivos de datos PST 863

Recuperar un equipo con Recuperación con un clic 631

Red de recuperación de producción 1118

Red de recuperación de prueba 1118

Red Hat y Linux 520

Redireccionamiento de sonido remoto 1447

Redireccionamiento del sonido desde una carga de trabajo remota de Linux 1448

Redireccionamiento del sonido desde una carga de trabajo remota de macOS 1448

Redireccionamiento del sonido desde una carga de trabajo remota de Windows 1447

Redistribución 966

Reenvío de correos electrónicos archivados 790

Registro de cargas de trabajo 109

Registro de cargas de trabajo utilizando credenciales de usuario 111, 115

Registro de cargas de trabajo utilizando la consola de Cyber Protect 110

Registro de cargas de trabajo utilizando la interfaz gráfica de usuario 110

Registro de cargas de trabajo utilizando un token de registro 112, 117

© Acronis International GmbH, 2003-2025

Registro de eventos de Windows 653, 719

Registro del dispositivo de arranque 999

Registro y anulación de registro de cargas de trabajo utilizando la interfaz de línea de comandos 115

Regla común de copia de seguridad 531

Regla común de instalación 531

Reglas de cortafuegos para servidores en la nube 1072

Reglas de directiva para discos y volúmenes 541

Reglas de directiva para los archivos y las carpetas 544

Reglas de retención legales 783

Reglas de retención según el esquema de copias de seguridad 577

Reiniciar una carga de trabajo 1317

Reinstalación de la puerta de enlace de VPN 1056

Reintentar si se produce un error 605, 714

Reintentar si se produce un error durante la creación de instantáneas de VM 606

Rendimiento 716, 960

Renombrar un plan de reenvío SIEM 285

Renovación de la directiva de flujo de datos 1225

Renovación de la directiva de una empresa o unidad 1225

Renovación de la directiva de uno o más usuarios de la empresa o unidad 1226

Renovación del acceso a una conexión de nube pública 760

Renovar el acceso a una suscripción de Microsoft Azure 755

Réplica de copia de seguridad 261

Replicación 581

Replicación de equipos virtuales 955

Repositorios de software 1410

Requisitos 701, 723, 1134

Requisitos adicionales para equipos con Windows 806

Requisitos de acceso necesarios para hacer una copia de seguridad en el almacenamiento en la nube pública 748

Requisitos de contraseña 22

Requisitos de equipos virtuales Hyper-V 796

Requisitos de espacio en disco 705, 1007

Requisitos de red para el agente para la Virtuozzo Hybrid Infrastructure (dispositivo virtual) 148

Requisitos de software para Disaster Recovery en Microsoft Azure 1107

Requisitos de software para Disaster Recovery para Cyber Protect Cloud 1011

Requisitos de software para Endpoint Detection and Response 1254

Requisitos del control de cuentas de usuario (UAC) 192

Requisitos del dispositivo VPN 1026

Requisitos del sistema 1026

Requisitos del sistema para agentes 47

Requisitos del sistema para el agente 137, 141, 147, 159, 166

Requisitos del sistema para el dispositivo virtual 171

Requisitos habituales 794

Requisitos para copias de seguridad con información de aplicaciones 794

Requisitos para equipos virtuales ESXi 795

© Acronis International GmbH, 2003-2025

Requisitos para la detección de dispositivos 188

Requisitos para las cuentas de usuario 822

Requisitos previos 128, 134, 183, 185-186, 378, 465-466, 474, 546, 631, 701, 938, 952, 968, 1023, 1046, 1048, 1406, 1565

Requisitos y limitaciones para la conmutación por error de máquinas virtuales Linux a Microsoft Azure 1134

Resolver problemas de compatibilidad 258

Restablecimiento de contraseñas de usuario 1365

Restablecimiento de los modelos de aprendizaje automático 1555

Resumen de la instalación del parche 344

Reversión al disco RAM inicial original 710

Revisar incidentes 1258

Revise y analice los IOC descubiertos 1301

Revise y mitigue los IOC mitigados en las cargas de trabajo afectadas 1300

Revisión de la posición de seguridad 1352

Revisión del panel de control de riesgos 1353

Revisión y gestión de directivas 1225

Revocación de los derechos de acceso de la aplicación de servicio de copia de seguridad 846

Revocación de planes de supervisión 1548

Revocación de un plan de protección 255

Revocación de un plan desde un grupo 434

Revocar un plan de archivado 769

Revocar un plan de copias de seguridad para Copia de seguridad directa en Microsoft 365 899

Revocar un plan de copias de seguridad para Microsoft 365 Business – Copia de seguridad 850

RMM 1249

Roles de usuario y derechos de la Programación cibernética 476

Roles necesarios 165

Runbooks en Microsoft Azure 1149

Ruta de desinstalación 1418

S

Scale Computing 518

Scripts en dispositivo de arranque 990

Scripts personalizados 991

Scripts predefinidos 990

Se adapta al intervalo de tiempo 570

Se necesitan puertos TCP para realizar copias de seguridad y replicaciones de equipos virtuales VMware. 39

Secuencia de comandos cibernética 474

Secuencias de comandos 478

Seguimiento de bloques modificados (CBT) 602, 960

Seguimiento de geolocalización 1495

Seguridad 1447

Seguridad a nivel de archivo 715

Selección de archivos de Google Drive 921

Selección de archivos de OneDrive 869

Selección de archivos de unidades compartidas 926

Selección de buzones de correo 853

Selección de carpetas públicas 856

Selección de equipos 880

Selección de la configuración de ESXi 546

© Acronis International GmbH, 2003-2025

Selección de los buzones de correo de Exchange Server 808

Selección de los datos de SharePoint Online 875

Selección de todo el equipo 538

Selección de un nivel de administración 374

Seleccionar archivos o carpetas 542

Seleccionar bases de datos de SQL 797

Seleccionar buzones de correo de Gmail 916

Seleccionar buzones de correo de Microsoft 365 905

Seleccionar datos de Exchange Server 798

Seleccionar discos o volúmenes 538

Seleccionar el proveedor de instantáneas 649

Seleccionar los datos que se incluirán en la copia de seguridad 538

Seleccionar un destino 547

Seleccionar un estado del sistema 545

Servicio de instantáneas de volumen (VSS) 648

Servicio de instantáneas de volumen (VSS) para equipos virtuales 650

servicios de Cyber Protection instalados en su entorno 219

Servicios instalados en macOS 219

Servicios instalados en Windows 219

Servidores de nube 1060

Servidores de recuperación en Microsoft Azure 1121

Servidores de recuperación en modo de conmutación por error 1157

Servidores DNS 1116

Servidores principales 1157

Si escoge crear el equipo virtual en un servidor de virtualización 277

Si escoge guardar el equipo virtual como un conjunto de archivos 276

Sintaxis 1271

Sistemas de archivos compatibles 525

Sistemas operativos compatibles 1011, 1107

Sistemas operativos compatibles con escritorio remoto y asistencia 1445

Sistemas operativos compatibles para la protección antivirus y antimalware 1160

Sistemas operativos Windows compatibles 1207

Sistemas operativos y entornos compatibles para la copia de seguridad y la recuperación 499

Sistemas operativos y versiones compatibles 28

Solución de incidentes 1302

Solución de problemas 706

Solución de problemas de configuración de VPN de IPsec 1043-1044

Solución de problemas de permisos en macOS 109

Solucionar problemas en la conectividad Open VPN de sitio a sitio 1034

Solucionar todo un incidente 1302

Solucionar un incidente con falso positivo 1306

Soporte para agrupación de tarjetas NIC 1005

Soporte técnico para la migración de máquinas virtuales 969

Startup Recovery Manager 1007

Supervisión 288, 328

Supervisión basada en anomalías 1508

Supervisión de alertas 1555

© Acronis International GmbH, 2003-2025

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

Supervisión de cargas de trabajo mediante la transmisión de captura de pantalla 1481

Supervisión de líneas base 1355

Supervisión de líneas base de inquilinos 1355

Supervisión del estado del disco 336

Supervisión del estado y el rendimiento de las cargas de trabajo 1507

T

Tasa de compresión 605

Tiempo medio de reparación de incidentes de seguridad 333

Tipo de control 993

Tipos de análisis 1164

Tipos de copia de seguridad 559

Tipos de datos de muestra 1275

Tipos de equipos virtuales admitidos 274

Tipos de eventos 1274

Tipos de eventos y campos 1274

Tipos de filtro de archivo 607

Tipos de recurso 394

Tipos de supervisión 1507

Tipos y categorías de alertas 295

Toma de instantáneas de LVM 626

Trabajadores en Microsoft Azure 1155

Trabajar con cargas de trabajo agregadas 465

Trabajar con cargas de trabajo de CyberApp 465

Trabajar con cargas de trabajo gestionadas 1466

Trabajar con cargas de trabajo sin gestionar 1485

Trabajar con Disaster Recovery en Microsoft Azure 1109

Trabajar con el gráfico XDR 1341

Trabajar con flujos de trabajo automatizados 1330

Trabajar con funciones de protección avanzada 1215

Trabajar con registros 1058

Trabajar con repositorios de software y paquetes de software 1410

Trabajar en VMware vSphere 955

Trabajo con Disaster Recovery a Cyber Protect Cloud 1016

Trabajo con planes 221

Transferencia de sonido 1447

Transferir archivos 1472

Transferir archivos mediante Acronis Asistencia rápida 1487

Traslado de cargas de trabajo a otro inquilino 121

Truncamiento de registros 625

U

Ubicación de la carpeta Cuarentena en los equipos 1210

Ubicaciones admitidas para el procesamiento de datos fuera del host 264

Ubicaciones admitidas para la validación 264

Ubicaciones compatibles 272, 581

Universal Restore en Linux 709

Universal Restore en Windows 708

Uso compartido de pantalla de Apple 1447

Uso de comodines para definir exclusiones 382, 1203

© Acronis International GmbH, 2003-2025

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

Uso de contraseñas con caracteres especiales o espacios en blanco 116

Uso de cuentas gMSA con el agente de Cyber Protection 69

Uso de la barra de herramientas en la ventana del Visor 1488

Uso de la consola de Cyber Protect a nivel de Todos los clientes 375

Uso de puntos de cálculo 1158

Uso de una cuenta de administrador de proyecto 152

Uso de una cuenta de administrador del sistema 149

Uso de Universal Restore 707

Uso de variables 599

Uso de variables para definir exclusiones 383

Uso del control de dispositivos 437

Uso del modo de aplicación adaptada para renovar una directiva de usuario 1227

Uso del Modo de observación para renovar una directiva de usuario 1226

Utilización de almacenamiento conectado localmente 964

V

Validación 264

Validación de copias de seguridad 725

Validación de la copia de seguridad 602, 712

Valores de filtro de archivos 608

Valores del campo acción 460

Variables de alertas de supervisión 1556

Velocidad de salida durante la copia de seguridad 637

Ventana de copia de seguridad y rendimiento 633

Ventana de copias de seguridad 634

Ver actividades de archivado de correos electrónicos 764

Ver alertas de archivado de correos electrónicos 764

Ver alertas de control de dispositivos 444

Ver cargas de trabajo gestionados por integraciones RMM 463

Ver datos de supervisión 1564

Ver el estado de la conmutación por error de prueba automatizada 1081, 1133

Ver la lista de parches disponibles 1398

Ver o cambiar la configuración del acceso 440

Ver qué incidentes no se han mitigado actualmente 1261

Verificar la autenticidad del archivo con Notary Service 698, 930

Versiones compatibles 890

Versiones compatibles de Microsoft Exchange Server 510

Versiones compatibles de Microsoft SQL Server 509

Versiones de la secuencia de comandos 486

Versiones de MariaDB admitidas 511

Versiones de Microsoft SharePoint compatibles 510

Versiones de MySQL admitidas 511

Versiones de Oracle Database compatibles 511

Versiones de SAP HANA compatibles 511

Versiones de Windows compatibles 1411

Viendo el último usuario que ha iniciado sesión 467

© Acronis International GmbH, 2003-2025

Vinculación de cargas de trabajo a usuarios específicos 467

Virtuozzo Hybrid Infrastructure 523

Virtuozzo Hybrid Server 522

Vista de detalles sobre servidores e la nube 1070

Vista de la información sobre los dispositivos detectados 200

Vista previa de correos electrónicos 787

Visualización de archivos de copia de seguridad que contienen datos forenses 619

Visualización de detalles de atasco 731

Visualización de detalles sobre elementos de la lista blanca 1212

Visualización de errores de integración de XDR 1346

Visualización de la ubicación de un dispositivo 1496

Visualización del estado de georreplicación 1576

Visualización del estado de la copia de seguridad en vSphere Client 971

Visualización del estado de protección de una carga de trabajo de Microsoft 365 por servicio 849

Visualización del hardware de un solo dispositivo 1371

Visualización del historial de ejecuciones 1105

Visualización del inventario de software de un solo dispositivo 1378

Visualización del registro de alertas de supervisión 1563

Visualización del resultado de distribución 967

Visualización del uso del almacenamiento inmutable 1574

Visualización fácil de entender de la historia del ataque 1252

Visualización y actualización de ubicaciones de copia de seguridad en la nube pública 747

Visualización y actualización de un agente para Azure desplegado 169

Visualización y comprensión de los resultados de la consulta 1267

Visualizar las cargas de trabajo de clientes específicos 376

VMware (Broadcom) 512

Volume Shadow Copy Service VSS para equipos virtuales 960

Volver a configurar la dirección IP 1053

Volver a generar la configuración 1049

VPN de sitio a sitio de Azure 1117

Vulnerabilidades existentes 343

W

Widget de dispositivos detectados 342

Widget de sesiones remotas 351

Widgets de Advanced Data Loss Prevention en el panel de control Información general 1240

Widgets de alertas 328

Widgets de conmutación por error 1127

Widgets de desinstalación de software 349

Widgets de Endpoint Detection and Response (EDR) 331

Widgets de evaluación de vulnerabilidades 342

Widgets de instalación de parches 343

Widgets de instalación de software 348

Widgets de inventario de hardware 350

© Acronis International GmbH, 2003-2025

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

Widgets de inventario de software 347

Widgets de software 347

Widgets de supervisión 1565

Widgets sobre el estado del disco 337

Windows 540

© Acronis International GmbH, 2003-2025